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 instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

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

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

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

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

© 2017 Cisco Systems, Inc. All rights reserved.
CONTENTS

Preface xv

Overview xv

Audience xv

Guide Conventions xv

Related Documentation xvii

Cisco Unified IP Phone 8900 Series Documentation xvii

Cisco Unified IP Phone 9900 Series Documentation xvii

Cisco Unified Communications Manager Documentation xvii

Cisco Business Edition 3000 Documentation xvii

Cisco Business Edition 6000 Documentation xvii

Documentation, Support, and Security Guidelines xviii

Cisco Product Security Overview xviii

PART I

About the Cisco Unified IP Phone 1

CHAPTER 1

Technical Details 3

Physical and Operating Environment Specifications 3

Cable Specifications 4

Network and Computer Port Pinouts 5

Network Port Connector 5

Computer Port Connector 5

Phone Power Requirements 6

Power Outage 7

Power Reduction 8

Power Negotiation over LLDP 8

Network Protocols 9

VLAN Interaction 13
PART II
Cisco Unified IP Phone Installation 57

CHAPTER 4
Cisco Unified IP Phone Installation 59
  Verify the Network Setup 59
  Enable Autoregistration for Phones 60
  Install Cisco Unified IP Phone 61
  Set Up Phone from Setup Menus 63
    Apply a Phone Password 64
    Text and Menu Entry from Phone 65
  Set Up Wireless LAN 65
    Set Up Wireless LAN on Cisco Unified Communications Manager 66
    Set Up Wireless LAN on Cisco Unified IP Phone 67
  Configure Network Settings 70
    Set Up IPv4 73
    Set Up IPv6 76
    Set Domain Name Field 79
    Set Admin VLAN ID Field 79
    Set PC VLAN Field 79
    Set SW Port Setup Field 80
    Set PC Port Setup Field 80
    Set Wireless Field 80
    Set Wireless Sign In Access Field 80
    Set SSID Field 81
    Set Security Mode Field 81
    Set 802.11 Mode Field 82
    Set DHCP Enabled Field 82
    Set IP Address Field 82
    Set Subnet Mask Field 83
    Set Default Router Field 83
    Set DNS Server Fields 83
    Set Alternate TFTP Field 83
    Set TFTP Server 1 Field 84
    Set TFTP Server 2 Field 84
    Set Up Phone To Use DHCP 84
Set Up Phone To Not Use DHCP 85
Phone Startup Process 85
Configure Phone Services for Users 86

CHAPTER 5
Cisco Unified Communications Manager Phone Setup 87
Set Up Cisco Unified IP Phone 87
Determine the Phone MAC Address 90
Phone Addition Methods 91
   Add Phones Individually 91
   Add Phones Using BAT Phone Template 91
Add Users to Cisco Unified Communications Manager 92
   Add a User from an External LDAP Directory 92
   Add User Directly to Cisco Unified Communications Manager 93
Add User to End User Group 94
Associate Phones with Users 94
Survivable Remote Site Telephony 95
Set Up Cisco Unified Communications Manager Features 97

CHAPTER 6
Self Care Portal Management 99
Self Care Portal Overview 99
Set Up User Access to the Self Care Portal 99
Customize the Self Care Portal Display 100

PART III
Hardware and Accessory Installation 101

CHAPTER 7
Cisco Unified IP Phone Accessories 103
Accessory Support 103
Connect Footstand 104
Secure the Phone with a Cable Lock 105
External Speakers and Microphone 106
Headsets 106
   Audio Quality 107
   Analog Headsets 107
      Enable Wideband on Analog Headsets 107
      Enable the Wideband for Analog Headsets 108
Wired Headsets 108
  Connect Wired Headset 108
  Disable a Wired Headset 108
USB Headsets 109
  Enable USB Headset 109
  Disable a USB Headset 109
Wireless Headsets 110
Bluetooth Wireless Headsets 110
  Enable a Bluetooth Wireless Headset 111
  Remove a Bluetooth Device from the Phone 112

CHAPTER 8  Cisco Unified IP Color Key Expansion Modules 113
Cisco Unified IP Color KEM Setup Overview 113
KEM Power Information 114
Connect Single KEM to Cisco Unified IP Phone 114
Connect Two or More KEMs to Phone Using KEM Spine Connector 115
Set Up Key Expansion Module in Cisco Unified Communications Manager Administration 116
Access Key Expansion Module setup 117
Upgrade Key Expansion Module 118
Remove All Key Expansion Modules 118
Troubleshoot the Key Expansion Module 118

CHAPTER 9  Cisco Unified Video Camera Installation 121
Cisco Unified Video Camera Overview 121
Set Up Cisco Unified Video Camera 121
Perform Camera Postinstallation Checks 122
Camera Settings 122
  Adjust View Area Setting 122
  Adjust Brightness Setting 123
  Adjust Auto Transmit Setting 123

CHAPTER 10  Wall Mounts 125
Wall Mount Options 125
Lockable Wall Mount Components for Phone 126
Install Bracket 126
PART IV
Cisco Unified IP Phone Administration 157

CHAPTER 11
Cisco Unified IP Phone Security 159

Supported Security Features 160

Supported TLS and Ciphers 163

Set Up Locally Significant Certificate 164

Phone Call Security 164

Secure Conference Call Identification 165

Secure Phone Call Identification 166

Provide Encryption for Barge 167

WLAN Security 167

802.1X Authentication 171

Access 802.1X Authentication 172

802.1X Authentication Options 172

Set Device Authentication Field 173

CHAPTER 12
Cisco Unified IP Phone Customization 175

Custom Phone Rings 175

Set Up Custom Phone Ring 175

Custom Ring File Formats 176

Custom Background Images 177

Set Up Custom Background Image 177
CHAPTER 13
Phone Features and Setup

- Custom Background File Formats 178
- Set Up Wideband Codec 179
- Set Up Idle Display 180

Phone Features and Setup Overview 182
Cisco IP Phone User Support 183
Telephony Features 183
Feature Buttons and Softkeys 206
Create Feature Control Policy 208
  - Feature Control Policy Default Values 209
Disable Speakerphone 210
Schedule Power Save for Cisco IP Phone 210
Schedule Power Save Plus (EnergyWise) on Cisco IP Phone 212
Set up AS-SIP 215
Enable Agent Greeting 217
Set Up the DF Bit 217
Set Up Do Not Disturb 218
Set Up Monitoring and Recording 218
Set Up Power Negotiation for LLDP 219
Set Up RTCP Control 220
Set Up Simplified New Call Window 220
Set Up Automatic Port Synchronization 220
Set Up Bluetooth Profiles 221
Set Up SSH Access 221
Set Up Call Forward Notification 222
Client Matter Codes and Forced Authorization Codes 223
Enable BLF for Call Lists 223
Set Up Dual Bank Information 224
Set Up Incoming Call Toast Timer 224
Set Up Peer Firmware Sharing 225
Set Up Remote Port Configuration 226
Set Headset Sidetone Control 226
Enable Device Invoked Recording 227
Set Up Enable Video On/Off 228
Set Up Dial Tone from Release Button 228

Park Monitoring 229
  Set Up Park Monitoring Timers 229
  Set Park Monitoring Parameters for Directory Numbers 230
  Set Up Park Monitoring for Hunt Lists 231

Enable Actionable Incoming Call Alert 231

Enable the Call History Display Enhancement 232

Enable Call History for Shared Line 233

Set Up the Default Line Filter 233

Set Up Custom Line Filter 233

Phone Button Templates 234
  Modify Phone Button Template 234
  Assign Phone Button Template for All Calls 235
  Set Up PAB or Speed Dial as IP Phone Service 235
  Modify Phone Button Template for PAB or Fast Dial 236

Control Phone Web Page Access 237

Enable Softkey Policy Control 237

Set Up a Softkey Template 238

Set Up Separate Audio and Video Mute 241

Set Up RTP/sRTP Port Range 241

Set Up TLS Resumption Timer 242

Set Up the Audio and Video Port Range 242

Set Up Cisco IP Manager Assistant 244

Enable Privacy Settings 246

Set Up Audio EQ 247

Set the Label for a Line 247

---

CHAPTER 14

Corporate and Personal Directory Setup 249

Corporate Directory Setup 249

Personal Directory Setup 249

User Personal Directory Entries Setup 250
  Download Cisco IP Phone Address Book Synchronizer 250
  Cisco IP Phone Address Book Synchronizer Deployment 250
    Install Synchronizer 251
    Set Up Synchronizer 251
CHAPTER 17  Troubleshooting  301

General Troubleshooting Information  301

Startup Problems  303

Cisco IP Phone Does Not Go Through the Normal Startup Process  303
Cisco IP Phone Does Not Register with Cisco Unified Communications Manager  304
Phone Displays Error Messages  304

Phone Cannot Connect to TFTP Server or to Cisco Unified Communications Manager  304
Phone Cannot Connect to TFTP Server  304
Phone Cannot Connect to Server  305
Phone Cannot Connect Using DNS  305

Cisco Unified Communications Manager and TFTP Services Are Not Running  305
Configuration File Corruption  306
Cisco Unified Communications Manager Phone Registration  306
Cisco IP Phone Cannot Obtain IP Address  306

Phone Reset Problems  306

Phone Resets Due to Intermittent Network Outages  307
Phone Resets Due to DHCP Setting Errors  307
Phone Resets Due to Incorrect Static IP Address  307
Phone Resets During Heavy Network Usage  307
Phone Resets Due to Intentional Reset  308
Phone Resets Due to DNS or Other Connectivity Issues  308
Phone Does Not Power Up  308
Phone Cannot Connect to LAN  309
Cisco IP Phone Security Problems  309
CTL File Problems  309
Authentication Error, Phone Cannot Authenticate CTL File 309
Phone Cannot Authenticate CTL File 309
CTL File Authenticates but Other Configuration Files Do Not Authenticate 310
ITL File Authenticates but Other Configuration Files Do Not Authenticate 310
TFTP Authorization Fails 310
Phone Does Not Register 310
Signed Configuration Files Are Not Requested 311
802.1X Authentication Problems 311
  802.1X Enabled on Phone but Phone Does Not Authenticate 312
  802.1X Not Enabled 312
Factory Reset of Phone Has Deleted 802.1X Shared Secret 313
Camera, Audio, and Video Problems 313
  No Video 313
  Phone Display Is Wavy 314
  Video Freezes 314
  Video Is Too Dark 314
  Video Is Poor Quality or Grainy 315
  Video Is Blocky or Distorted 315
  Video Is Slow Moving or Jittery 315
  Audio/Video Is Not Synchronized 316
  No Audio 316
  No Speech Path 316
  Choppy Speech 317
  Poor Audio Quality with Calls that Route Outside Cisco Unified Communications Manager 317
  Video Distorted or Pixilated 317
VXC VPN Troubleshooting 318
  Phone Does Not Set Up VXC VPN Tunnel 318
  Phone Does Not Connect with VXC VPN 318
General Telephone Call Problems 319
  VPN-Connected Phone Does Not Log Calls 319
  Phone Call Cannot Be Established 319
  Phone Does Not Recognize DTMF Digits or Digits Are Delayed 320
Troubleshooting Procedures 320
  Set Up Remote Phone 320
Check TFTP Settings 321
Determine DNS or Connectivity Issues 321
Check DHCP Settings 322
Create New Phone Configuration File 322
Identify 802.1X Authentication Problems 323
Verify DNS Settings 323
Start Service 324
Control Debug Information from Cisco Unified Communications Manager 324

Additional Troubleshooting Information 325

CHAPTER 18

Maintenance 327
Phone Reset Options 327
Reset the Phone to the Factory Settings from the Keypad 328
Perform Factory Reset from Phone Menu 328
Perform Network Configuration Reset 329
Perform User and Network Configuration Reset 329
Remove CTL File 329
Quality Report Tool 330
Voice Quality Monitoring 330
Voice Quality Troubleshooting Tips 330
Video Metrics 331
Cisco Unified IP Phone Cleaning 332

CHAPTER 19

International User Support 333
Unified Communications Manager Endpoints Locale Installer 333
International Call Logging Support 333
Language Limitation 334
Overview

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

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

Audience

Network engineers, system administrators, and telecom engineers should review this guide to learn the steps that are required to set up Cisco 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:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boldface font</td>
<td>Commands and keywords are in boldface.</td>
</tr>
</tbody>
</table>
**Guide Conventions**

<table>
<thead>
<tr>
<th><strong>Convention</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><em>italic</em> font</td>
<td>Arguments for which you supply values are in <em>italics</em>.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td><em>screen</em> font</td>
<td>Terminal sessions and information the system displays are in <em>screen</em> font.</td>
</tr>
<tr>
<td>input font</td>
<td>Information you must enter is in input font.</td>
</tr>
<tr>
<td><em>italic screen</em> font</td>
<td>Arguments for which you supply values are in <em>italic screen</em> font.</td>
</tr>
<tr>
<td>^</td>
<td>The symbol ^ represents the key labeled Control - for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
</tbody>
</table>

---

**Note**

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

**Caution**

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

Warnings use the following convention:

---

**Attention**

**IMPORTANT SAFETY INSTRUCTIONS**

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

SAVE THESE INSTRUCTIONS
Related Documentation

Use the following sections to obtain related information.

Cisco Unified IP Phone 8900 Series Documentation

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


Cisco Unified IP Phone 9900 Series Documentation

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


Cisco Unified Communications Manager Documentation

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


Cisco Business Edition 3000 Documentation

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


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:

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:


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 http://www.bis.doc.gov/policiesandregulations/ear/index.htm.
PART

About the Cisco Unified IP Phone

- Technical Details, page 3
- Cisco Unified IP Phone Descriptions, page 21
- VoIP Wireless Network Setup for Cisco Unified IP Phone 9971, page 43
Technical Details

- Physical and Operating Environment Specifications, page 3
- Cable Specifications, page 4
- Phone Power Requirements, page 6
- Network Protocols, page 9
- VLAN Interaction, page 13
- Cisco Unified Communications Manager Interaction, page 14
- Cisco Unified Communications Manager Express Interaction, page 14
- Voice Messaging System Interaction, page 15
- Phone Startup Overview, page 15
- External Devices, page 17
- USB Port Information, page 18
- Phone Configuration Files, page 18
- Network Bandwidth, page 19
- Phone Behavior During Times of Network Congestion, page 19

Physical and Operating Environment Specifications

The following table shows the physical and operating environment specifications for the Cisco Unified IP Phone 8961, 9951, and 9971.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value or range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating temperature</td>
<td>32° to 104°F (0° to 40°C)</td>
</tr>
<tr>
<td>Operating relative humidity</td>
<td>10% to 95% (noncondensing)</td>
</tr>
<tr>
<td>Specification</td>
<td>Value or range</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>Storage temperature</td>
<td>14°C to 140°F (–10°C to 60°C)</td>
</tr>
<tr>
<td>Height</td>
<td>9.2 in. (23.4 cm)</td>
</tr>
<tr>
<td>Width</td>
<td>10.33 in. (26.25 cm)</td>
</tr>
<tr>
<td>Depth</td>
<td>1.56 in. (3.97 cm)</td>
</tr>
<tr>
<td>Weight</td>
<td>3.5 lb. (1.6 kg)</td>
</tr>
<tr>
<td></td>
<td>Handset: Slimline (5 oz., 140g) or Standard (6 oz., 170g)</td>
</tr>
<tr>
<td>Power</td>
<td>100-240 VAC, 50-60 Hz, 0.5 A when using the AC adapter</td>
</tr>
<tr>
<td></td>
<td>48 VDC, 0.2 A when using the in-line power over the network cable</td>
</tr>
<tr>
<td>Power consumed by the camera</td>
<td>290mA (1.45W) (excludes the power consumed by the phone)</td>
</tr>
<tr>
<td>(Applicable to Cisco Unified IP Phone 9951 and 9971)</td>
<td></td>
</tr>
<tr>
<td>Cables</td>
<td>Category 3/5/5e/6 for 10-Mbps cables with 4 pairs</td>
</tr>
<tr>
<td></td>
<td>Category 5/5e/6 for 100-Mbps cables with 4 pairs</td>
</tr>
<tr>
<td></td>
<td>Category 5e/6 for 1000-Mbps cables with 4 pairs</td>
</tr>
<tr>
<td></td>
<td>Note: Cables have 4 pairs of wires for a total of 8 conductors.</td>
</tr>
<tr>
<td>Distance requirements</td>
<td>As supported by the Ethernet Specification, the maximum cable length between each Cisco Unified IP Phone and the switch is assumed to be 330 feet (100 meters).</td>
</tr>
</tbody>
</table>

**Note**
For power information regarding the Cisco Unified IP Key Color Expansion Module, see KEM Power Information, on page 114.

### Cable Specifications

The following information lists the cable specifications:

- RJ-9 jack (4-conductor) for handset and headset connection
- RJ-45 jack for the LAN 10/100/1000BaseT connection (10/100/1000 Network port on the Cisco Unified IP Phone 8961, 9951, and 9971)
- RJ-45 jack for a second 10/100/1000BaseT compliant connection (10/100/1000 Computer port on the Cisco Unified IP Phone 8961, 9951, and 9971)
• 3.5 mm jack for microphone and speaker connection (for Cisco Unified IP Phone 9951 and 9971 only)
• 48-volt power connector

**Network and Computer Port Pinouts**

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

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

**Network Port Connector**

The following table describes the network port connector pinouts.

*Table 2: Network Port Connector Pinouts*

<table>
<thead>
<tr>
<th>Pin Number</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BI_DA+</td>
</tr>
<tr>
<td>2</td>
<td>BI_DA-</td>
</tr>
<tr>
<td>3</td>
<td>BI_DB+</td>
</tr>
<tr>
<td>4</td>
<td>BI_DC+</td>
</tr>
<tr>
<td>5</td>
<td>BI_DC-</td>
</tr>
<tr>
<td>6</td>
<td>BI_DB-</td>
</tr>
<tr>
<td>7</td>
<td>BI_DD+</td>
</tr>
<tr>
<td>8</td>
<td>BI_DD-</td>
</tr>
</tbody>
</table>

*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 3: Computer (Access) Port Connector Pinouts*

<table>
<thead>
<tr>
<th>Pin Number</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BI_DB+</td>
</tr>
</tbody>
</table>
Function

<table>
<thead>
<tr>
<th>Pin Number</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>BI_DB-</td>
</tr>
<tr>
<td>3</td>
<td>BI_DA+</td>
</tr>
<tr>
<td>4</td>
<td>BI_DD+</td>
</tr>
<tr>
<td>5</td>
<td>BI_DD-</td>
</tr>
<tr>
<td>6</td>
<td>BI_DA-</td>
</tr>
<tr>
<td>7</td>
<td>BI_DC+</td>
</tr>
<tr>
<td>8</td>
<td>BI_DC-</td>
</tr>
</tbody>
</table>

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

---

*Note*

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

When connecting the phone to a Cisco switch which supports NG-PoE+, and both CDP and LLDP are enabled on the switch, disable the LLDP protocol on the phone from the Cisco Unified Communications Manager Administration.

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

**Table 4: Guidelines for Cisco Unified IP Phone 8961, 9951, and 9971 Power**

<table>
<thead>
<tr>
<th>Power Type</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>External power: Provided through the CP-PWR-CUBE-4= external power supply</td>
<td>The Cisco Unified IP Phone 8961, 9951, and 9971 uses the CP-PWR-CUBE-4 power supply.</td>
</tr>
<tr>
<td><em>Note</em></td>
<td>You must use the CP-PWR-CUBE-4 when you deploy the Cisco Unified IP Phone 9971 on a wireless network.</td>
</tr>
</tbody>
</table>
### Power Type

<table>
<thead>
<tr>
<th>Power Type</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>External power—Provided through the Cisco Unified IP Phone Power Injector.</td>
<td>The Cisco Unified IP Phone Power Injector may be used with any Cisco Unified IP Phone. Functioning as a midspan device, the injector delivers inline power to the attached phone. The Cisco Unified IP Phone Power Injector connects between a switch port and the IP Phone, and supports a maximum cable length of 100m between the unpowered switch and the IP phone.</td>
</tr>
</tbody>
</table>
| PoE power—Provided by a switch through the Ethernet cable attached to the phone. | Cisco Unified IP Phone 8961, 9951, and 9971 supports IEEE 802.3af Class 3 power on signal pairs and spare pairs.  
Cisco Unified IP Phone 8961, 9951, and 9971 supports IEEE 802.3at for external add-on devices.  
To ensure uninterruptible operation of the phone, make sure that the switch has a backup power supply.  
Make sure that the CatOS or IOS version that runs on your switch supports your intended phone deployment. See the documentation for your switch for operating system version information.  
Support for NG-PoE+: The Cisco Unified IP Phone 8961, 9951, and 9971 can draw more power than IEEE 802.3at, as long as there is NG-PoE+ switch support. |

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

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

<table>
<thead>
<tr>
<th>Document Topics</th>
<th>URL</th>
</tr>
</thead>
</table>

### 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
When 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.

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

**Power Save Plus (EnergyWise)**

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

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

**Power Negotiation over LLDP**

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

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

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

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

---

**Note**

When CDP and Power Negotiation are disabled, the phone can power the accessories up to 15.4W.
Cisco Unified IP Phones support several industry-standard and Cisco network protocols required for voice communication. The following table provides an overview of the network protocols that the Cisco Unified IP Phone 8961, 9951, and 9971 support.

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

<table>
<thead>
<tr>
<th>Network protocol</th>
<th>Purpose</th>
<th>Usage notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bluetooth</td>
<td>Bluetooth is a wireless personal area network (WPAN) protocol that specifies how devices communicate over short distances.</td>
<td>Cisco Unified IP Phones 9951 and 9971 support Bluetooth 2.1.</td>
</tr>
<tr>
<td>Bootstrap Protocol (BootP)</td>
<td>BootP enables a network device, such as the Cisco Unified IP Phone, to discover certain startup information, such as the IP address.</td>
<td>—</td>
</tr>
<tr>
<td>Cisco Audio Session Tunnel (CAST)</td>
<td>The CAST protocol allows Cisco Unified IP Phones and associated applications to discover and communicate with the remote IP Phones without requiring changes to the traditional signaling components, such as Cisco Unified Communications Manager (CM) and gateways.</td>
<td>The Cisco Unified IP Phone uses CAST as an interface between CUVA and Cisco Unified Communications Manager using the Cisco Unified IP Phone as a SIP proxy.</td>
</tr>
<tr>
<td>Cisco Discovery Protocol (CDP)</td>
<td>CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment. Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.</td>
<td>The Cisco Unified IP Phone uses CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.</td>
</tr>
<tr>
<td>Cisco Peer-to-Peer Distribution Protocol (CPPDP)</td>
<td>CPPDP is a Cisco proprietary protocol used to form a peer-to-peer hierarchy of devices. This hierarchy is used to distribute firmware files from peer devices to their neighboring devices.</td>
<td>CPPDP is used by the Peer Firmware Sharing feature.</td>
</tr>
<tr>
<td>Network protocol</td>
<td>Purpose</td>
<td>Usage notes</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Dynamic Host Configuration Protocol (DHCP)</td>
<td>DHCP dynamically allocates and assigns an IP address to network devices. DHCP enables you to connect an IP phone into the network and the phone to become operational without the need to manually assign an IP address or to configure additional network parameters.</td>
<td>DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, gateway, and a TFTP server on each phone locally. Cisco recommends that you use DHCP custom option 150. With this method, you configure the TFTP server IP address as the option value. For additional supported DHCP configurations, see the “Dynamic Host Configuration Protocol” chapter and the “Cisco TFTP” chapter in the Cisco Unified Communications Manager System Guide. <strong>Note</strong> If you cannot use option 150, you may try using DHCP option 66.</td>
</tr>
<tr>
<td>Hypertext Transfer Protocol (HTTP)</td>
<td>HTTP is the standard way of transferring information and moving documents across the Internet and the web.</td>
<td>Cisco Unified IP Phones use HTTP for XML services and for troubleshooting purposes.</td>
</tr>
<tr>
<td>Hypertext Transfer Protocol Secure (HTTPS)</td>
<td>Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of servers.</td>
<td>Web applications with both HTTP and HTTPS support have two URLs configured. Cisco Unified IP Phones that support HTTPS choose the HTTPS URL.</td>
</tr>
<tr>
<td>IEEE 802.1X</td>
<td>The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.</td>
<td>The Cisco Unified IP Phone implements the IEEE 802.1X standard by providing support for the following authentication methods: EAP-FAST, EAP-TLS, and EAP-MD5. When 802.1X authentication is enabled on the phone, you should disable the PC port and voice VLAN.</td>
</tr>
<tr>
<td>IEEE 802.11a/b/g</td>
<td>The IEEE 802.11 standard specifies how devices communication over a wireless local area network (WLAN). 802.11a operates at the 5 GHz band and 802.11b and 802.11g operate at the 2.4 GHz band. (Cisco Unified IP Phone 9971 only) The 802.11 interface is a deployment option for cases when Ethernet cabling is unavailable or undesirable.</td>
<td></td>
</tr>
<tr>
<td>Network protocol</td>
<td>Purpose</td>
<td>Usage notes</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Internet Protocol (IP)</td>
<td>IP is a messaging protocol that addresses and sends packets across the network.</td>
<td>To communicate using IP, network devices must have an assigned IP address, subnet, and gateway. IP addresses, subnets, and gateway identifications are automatically assigned if you are using the Cisco Unified IP Phone with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each phone locally. The Cisco Unified IP Phones support IPv6 addresses. For more information, see Cisco Unified Communications Manager Features and Services Guide, &quot;Internet Protocol Version 6 (IPv6)&quot;) chapter.</td>
</tr>
<tr>
<td>Link Layer Discovery Protocol (LLDP)</td>
<td>LLDP is a standardized network discovery protocol (similar to CDP) that is supported on some Cisco and third-party devices.</td>
<td>The Cisco Unified IP Phone supports LLDP on the PC port.</td>
</tr>
<tr>
<td>Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)</td>
<td>LLDP-MED is an extension of the LLDP standard for voice products.</td>
<td>The Cisco Unified IP Phone supports LLDP-MED on the SW port to communicate information such as:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Voice VLAN configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Device discovery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Power management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inventory management</td>
</tr>
<tr>
<td>Real-Time Transport Protocol (RTP)</td>
<td>RTP is a standard protocol for transporting real-time data, such as interactive voice and video, over data networks.</td>
<td>Cisco Unified IP Phones use the RTP protocol to send and receive real-time voice traffic from other phones and gateways.</td>
</tr>
<tr>
<td>Network protocol</td>
<td>Purpose</td>
<td>Usage notes</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Real-Time Control Protocol (RTCP)</td>
<td>RTCP works in conjunction with RTP to provide QoS data (such as jitter, latency, and round-trip delay) on RTP streams.</td>
<td>RTCP for audio calls is disabled by default. RTCP for video calls (including both audio streams and video streams in the video call) is enabled by default. You can enable or disable RTCP on individual phones from the Cisco Unified Communications Manager Administration.</td>
</tr>
<tr>
<td>Session Description Protocol (SDP)</td>
<td>SDP is the portion of the SIP protocol that determines which parameters are available during a connection between two endpoints. Conferences are established by using only the SDP capabilities that all endpoints in the conference support.</td>
<td>SDP capabilities, such as codec types, DTMF detection, and comfort noise, are normally configured on a global basis by Cisco Unified Communications Manager or Media Gateway in operation. Some SIP endpoints may allow configuration of these parameters on the endpoint itself.</td>
</tr>
<tr>
<td>Session Initiation Protocol (SIP)</td>
<td>SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP is an ASCII-based application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints.</td>
<td>Like other VoIP protocols, SIP addresses the functions of signaling and session management within a packet telephony network. Signaling allows transportation of call information across network boundaries. Session management provides the ability to control the attributes of an end-to-end call. Cisco Unified IP Phones support the SIP protocol when the phones are operating in IPv6 address, IPv4 address, or dual-stack mode.</td>
</tr>
<tr>
<td>Transmission Control Protocol (TCP)</td>
<td>TCP is a connection-oriented transport protocol.</td>
<td>Cisco Unified IP Phones use TCP to connect to Cisco Unified Communications Manager and to access XML services.</td>
</tr>
<tr>
<td>Transport Layer Security (TLS)</td>
<td>TLS is a standard protocol for securing and authenticating communications.</td>
<td>Upon security implementation, Cisco Unified IP Phones use the TLS protocol when securely registering with Cisco Unified Communications Manager.</td>
</tr>
</tbody>
</table>
### Network protocol

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

---

**Related Topics**

- 802.1X Authentication, on page 171
- Configure Network Settings, on page 70
- Phone Startup Process, on page 85
- VLAN Interaction, on page 13
- Cisco Unified Communications Manager Interaction, on page 14
- Cisco Unified Communications Manager Express Interaction, on page 14
- Set Up the Audio and Video Port Range, on page 242

---

**VLAN Interaction**

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

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

- The current VLANs might be configured on an IP subnet basis. However, additional IP addresses might not be available to assign to the phone so as to use different traffic they 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:

Related Topics
Network Protocols, on page 9

Cisco Unified Communications Manager Interaction
Cisco Unified Communications Manager is an open, industry-standard call processing system. Cisco Unified Communications Manager software sets up and tears down calls between phones, integrating traditional PBX functionality with the corporate IP network. Cisco Unified Communications Manager manages the components of the IP telephony system, such as the phones, the access gateways, and the resources necessary for features such as call conferencing and route planning. Cisco Unified Communications Manager also provides:
• Firmware for phones
• Certificate Trust List (CTL) and Identity Trust List (ITL) files using the TFTP service
• Phone registration
• Call preservation, so that a media session continues if signaling is lost between the primary Communications Manager and a phone

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

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

Related Topics
Network Protocols, on page 9

Cisco Unified Communications Manager Express Interaction
When the Cisco IP Phone works with the Cisco Unified Communications Manager Express (Unified CME), the phones must go into CME mode.
When a user invokes the conference feature, the tag allows the phone to use either a local or network hardware conference bridge.

The Cisco IP Phones do not support the following actions:

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

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

Related Topics

Network Protocols, on page 9

Voice Messaging System Interaction

Cisco Unified Communications Manager lets you integrate with different voice messaging systems, including the Cisco Unity voice messaging system. Because you can integrate with a variety of systems, you must provide users with information about how to use your specific system.

You should provide the following information to each user:

• How to access the voice messaging system account.
  Make sure that you have used Cisco Unified Communications Manager to configure the Messages button on the Cisco Unified IP Phone.
• Initial password for accessing the voice messaging system.
  Make sure that you have configured a default voice messaging system password for all users.
• How the phone indicates that voice messages are waiting.
  Make sure that you have used Cisco Unified Communications Manager to set up a message waiting indicator (MWI) method.

Phone Startup Overview

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

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

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

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

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Key Management Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>None</td>
<td>Any device can authenticate to the access point. For added security, static WEP encryption might optionally be used.</td>
</tr>
<tr>
<td>Shared Key</td>
<td>None</td>
<td>The phone encrypts the challenge text by using the WEP key and the access point must verify the WEP key that was used to encrypt the challenge text before network access is available.</td>
</tr>
<tr>
<td>LEAP or EAP-FAST</td>
<td>None</td>
<td>The RADIUS server authenticates the username and password before network access is available.</td>
</tr>
<tr>
<td>Auto (AKM)</td>
<td>WPA, WPA2, or CCKM</td>
<td>The phone looks for an access point with one of the key management options enabled. The username and password are authenticated by the RADIUS server before network access is available.</td>
</tr>
<tr>
<td>Auto (AKM)</td>
<td>WPA-Pre-shared key, WPA2-Pre-shared key</td>
<td>The phone looks for an access point that has one of the key management options enabled. Authentication uses the configured WPA-Pre-shared key or WPA2-Pre-shared key</td>
</tr>
</tbody>
</table>

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

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

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

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

For more information, see the Cisco Unified Communications Manager Security Guide, “Configuring the Cisco CTL Client” chapter.
8 Request the ITL file. The phone requests the ITL file after it requests the CTL file. The ITL file contains the certificates of the entities that the phone can trust. The certificates are used to authenticate a secure connection with the servers or to authenticate a digital signature signed by the servers. Cisco Unified Communications Manager 8.5 and later supports the ITL file.

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

---

**Note**

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

---

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

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

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

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

---

**Note**

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

---

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

**USB Port Information**

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

**Note**

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

**Phone Configuration Files**

Configuration files for a phone are stored on the TFTP server and define parameters for connecting to Cisco Unified Communications Manager. In general, any time you make a change in Cisco Unified Communications Manager that requires the phone to be reset, a change is automatically made to the phone configuration file. Configuration files also contain information about which image load the phone should be running. If this image load differs from the one currently loaded on a phone, the phone contacts the TFTP server to request the required load files.

If you configure security-related settings in Cisco Unified Communications Manager Administration, the phone configuration file will contain sensitive information. To ensure the privacy of a configuration file, you must configure it for encryption. For more information, see the documentation for your particular Cisco Unified Communications Manager release. A phone requests a configuration file whenever it resets and registers with Cisco Unified Communications Manager.

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

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

When using secure video over VPN and VXC/VPN, the maximum supported bandwidth is 320 kbps.
When the phone calls Cisco TelePresence, the maximum bandwidth is 320 kbps.

Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect Cisco IP Phone voice and video quality, and in some cases, can cause a call to drop. Sources of network degradation can include, but are not limited to, the following activities:

- Administrative tasks, such as an internal port scan or security scan
- Attacks that occur on your network, such as a Denial of Service attack
Cisco Unified IP Phone Descriptions

- Cisco Unified IP Phone 8961, 9951, and 9971 Overview, page 21
- Cisco Unified IP Phone 8961, page 22
- Cisco Unified IP Phone 9951, page 28
- Cisco Unified IP Phone 9971, page 34
- Terminology Differences, page 40

Cisco Unified IP Phone 8961, 9951, and 9971 Overview

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

The Cisco Unified IP Phones have the following features:

- 24-bit color phone screen (Cisco Unified IP Phone 9971 has touchscreen support)
- Programmable feature buttons that support up to 5 lines (6 lines for the Cisco Unified IP Phone 9971) or that can be programmed for other features
- Full video capabilities (Cisco Unified IP Phones 9951 and 9971 only)
- Gigabit ethernet connectivity
- Support for an external microphone and speakers
- Bluetooth support for wireless headsets (Cisco Unified IP Phones 9951 and 9971 only)
- Network connectivity by Wi-Fi (Cisco Unified IP Phone 9971 only)
- USB ports:
  - two USB ports for Cisco Unified IP Phones 9951 and 9971
  - one USB port for Cisco Unified IP Phone 8961
A Cisco Unified IP Phone, like other network devices, must be configured and managed. These phones encode G.711 a-law, G.711 mu-law, G.722, G.729a, G.729ab, iLBC, and iSAC codecs, and decode G.711 a-law, G.711 mu-law, G.722, G.729, G.729a, G.729b, G.729ab, iLBC, and iSAC codecs.

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

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

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

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

Finally, because the Cisco Unified IP Phone is a network device, you can obtain detailed status information from it directly. This information can assist you with troubleshooting any problems users might encounter when using their IP phones. You can also obtain statistics about a current call or firmware versions on the phone.

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

**Cisco Unified IP Phone 8961**

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

**Phone Connections for Cisco Unified IP Phone 8961**

Connect your phone to the corporate IP telephony network, using the following diagram.
<table>
<thead>
<tr>
<th></th>
<th>Description</th>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DC adapter port (DC48V)</td>
<td>5</td>
<td>Computer port (10/100/1000 PC) connection</td>
</tr>
<tr>
<td>2</td>
<td>AC-to-DC power supply (optional)</td>
<td>6</td>
<td>Handset connection</td>
</tr>
<tr>
<td>3</td>
<td>AC power wall plug (optional)</td>
<td>7</td>
<td>Analog headset connection (headset optional)</td>
</tr>
<tr>
<td>4</td>
<td>Network port (10/100/1000 SW) with IEEE 802.3af and 802.3at power enabled</td>
<td>8</td>
<td>Anti-theft security lock connector (lock optional)</td>
</tr>
</tbody>
</table>

The following diagram shows the phone from the side.
| 1 | USB port | 2 | Accessory connector; for example, to connect a Cisco Unified IP Color Key Expansion Module |

**Note**

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

**Buttons and Hardware**

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

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

- **Session buttons (right side):** Use to perform tasks such as answering a call, resuming a held call, or (when not being used for an active call) initiating phone functions such as displaying missed calls. Each call on your phone is associated with a session button.
shows information about your phone, including directory number, call information (for example, caller ID, icons for an active call or call on hold) and available softkeys.
Each button corresponds with an active call or a call function. When you press the button, the action depends on the state of the phone:

- **Active calls**: Causes the phone to take the default action for an active call. For example, if you press the session button for a ringing call, the call is answered and if you press the button on a held call, the call resumes. Session information, such as caller ID and call duration, appears on the phone screen next to the session button.

- **Call functions**: When a session button is not being used for an active call, it can be used to initiate functions on the phone, as indicated by the adjacent phone screen icons. For example, press the session button to display missed calls, take the phone off hook, or dial your voicemail system (with a Voicemail icon).

Color LEDs reflect the call state. LEDs can **flash** (blink on and off rapidly), **pulse** (alternately dim and brighten), or appear solid (glow without interruption).

- **Flashing amber**: Ringing call. Press this button to answer the call.

- **Solid green**: May be a connected call or an outgoing call that is not yet connected. If the call is connected, press this button to display the call details or the participants of a conference call. If the call is not yet connected, press this button to end the call.

- **Pulsing green**: Held call. Press this button to resume the held call.

- **Solid red**: Shared line is in use remotely. Press this button to barge into call (if Barge is enabled).

- **Pulsing red**: Shared line call put on hold remotely. Press this button to resume the held call.

The positions of the session buttons and feature buttons can be reversed on phones that use a locale with a right-to-left reading orientation, such as Hebrew and Arabic.

<table>
<thead>
<tr>
<th>2</th>
<th>Session buttons</th>
<th>Allow you to access the softkey options (for the selected call or menu item) displayed on your phone screen.</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Softkey buttons</td>
<td>Allow you to access the softkey options (for the selected call or menu item) displayed on your phone screen.</td>
</tr>
<tr>
<td>4</td>
<td>Back button</td>
<td>Returns to the previous screen or menu.</td>
</tr>
<tr>
<td>5</td>
<td>Release button</td>
<td>Ends a connected call or session.</td>
</tr>
<tr>
<td></td>
<td>Navigation pad and Select button</td>
<td>The four-way Navigation pad allows you to scroll through menus, highlight items, and move within a text input field. The Select button (center of the Navigation pad) allows you to select a highlighted item. The Select button is lit (white) when the phone is in Power Save or Power Save Plus mode. Press the Select button to override Power Save and Power Save Plus mode.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>7</td>
<td>Conference button</td>
<td>Creates a conference call.</td>
</tr>
<tr>
<td>8</td>
<td>Hold button</td>
<td>Places a connected call on hold and toggles between an active and held call.</td>
</tr>
<tr>
<td>9</td>
<td>Transfer button</td>
<td>Transfers a call.</td>
</tr>
<tr>
<td>10</td>
<td>Keypad</td>
<td>Allows you to dial phone numbers, enter letters, and choose menu items by entering the item number.</td>
</tr>
<tr>
<td>11</td>
<td>Speakerphone button</td>
<td>Selects the speakerphone as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green. The speakerphone audio path does not change until you select a new default audio path (for example, by picking up the handset). If external speakers are connected, the Speakerphone button selects them as the default audio path.</td>
</tr>
<tr>
<td>12</td>
<td>Mute button</td>
<td>Toggles the microphone on or off during a call. When the microphone is muted, the button is lit red. When muted, you can hear the other parties on the call, but they cannot hear you.</td>
</tr>
<tr>
<td>13</td>
<td>Headset button</td>
<td>Selects the headset as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green. A headset icon in the phone screen header line indicates that the headset is the default audio path. This audio path does not change until you select a new default audio path (for example, by picking up the handset).</td>
</tr>
<tr>
<td>Number</td>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>14</td>
<td>Volume button</td>
<td>Controls the handset, headset, and speakerphone volume (off hook) and the ringer volume (on hook). Silences the ringer on the phone if an incoming call is ringing.</td>
</tr>
<tr>
<td>15</td>
<td>Messages button</td>
<td>Autodials your voicemail system (varies by system).</td>
</tr>
<tr>
<td>16</td>
<td>Applications button</td>
<td>Opens/closes the Applications menu. Depending on how your system administrator sets up the phone, use it to access applications such as call history, preferences, and phone information.</td>
</tr>
<tr>
<td>17</td>
<td>Contacts button</td>
<td>Opens/closes the Contacts menu. Depending on how your system administrator sets up the phone, use it to access personal directory, corporate directory, or call history.</td>
</tr>
<tr>
<td>18</td>
<td>Phone display</td>
<td>Can be positioned to your preferred viewing angle.</td>
</tr>
</tbody>
</table>
| 19     | Programmable feature buttons (also called feature buttons) | Each button corresponds with a phone line, speed dial, or calling feature. Press a phone line button to display the active calls for that line. If you have multiple lines, you may have an All Calls button that displays a consolidated list of all calls from all lines (oldest at the top). If you do not see the All Calls button, your system administrator may have set up the primary line to automatically display all calls. For information on your setup, contact your system administrator. Color LEDs indicate the line state:  
  - Amber: Ringing call on this line  
  - Green: Active or held call on this line  
  - Red: Shared line in use remotely  
The positions of the session buttons and feature buttons can be reversed on phones that use a locale with a right-to-left reading orientation, such as Hebrew and Arabic. |
| 20     | Handset with light strip | The handset light strip lights up to indicate a ringing call (flashing red) or a new voice message (steady red). |

**Cisco Unified IP Phone 9951**

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

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

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

The following picture shows the side of the phone.
<table>
<thead>
<tr>
<th></th>
<th>USB port</th>
<th>3 Speaker port for output to optional external speakers</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Accessory connector; for example, for connecting a Cisco Unified IP Phone Expansion Module</td>
<td>4 Microphone port for input from optional external microphone</td>
</tr>
</tbody>
</table>

**Note**

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

**Buttons and Hardware**

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

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

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

Shows information about your phone, including directory number, call information (for example, caller ID, icons for an active call or call on hold) and available softkeys.
<table>
<thead>
<tr>
<th></th>
<th>Session buttons</th>
<th>Each button corresponds with an active call or a call function. When you press the button, the action depends on the state of the phone:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Active calls: Press the button to take the default action for an active call. For example, press the session button for a ringing call to answer the call and press the button on a held call to resume the call. Session information, such as caller ID and call duration, appears on the phone screen next to the session button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Call functions: When a session button is not being used for an active call, it can be used to initiate functions on the phone, as indicated by the adjacent phone screen icons. For example, press the session button to display missed calls, take the phone off hook, or dial your voicemail system (with a Voicemail icon).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Color LEDs reflect the call state. LEDs can flash (blink on and off rapidly), pulse (alternately dim and brighten), or appear solid (glow without interruption).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Flashing amber ✅: Ringing call. Press this button to answer the call.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Solid green ✅: May be a connected call or an outgoing call that is not yet connected. If the call is connected, press this button to display the call details or the participants of a conference call. If the call is not yet connected, press this button to end the call.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Pulsing green ✅: Held call. Press this button to resume the held call.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Solid red ✅: Shared line in use remotely. Press this button to barge into the call (if Barge is enabled).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Pulsing red ✅: Shared line call put on hold remotely. Press this button to resume the held call.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The positions of the session buttons and feature buttons can be reversed on phones that use a locale with a right-to-left reading orientation, such as Hebrew and Arabic.</td>
</tr>
<tr>
<td>3</td>
<td>Softkey buttons</td>
<td>Allow you to access the softkey options (for the selected call or menu item) displayed on your phone screen.</td>
</tr>
<tr>
<td>4</td>
<td>Back button</td>
<td>Returns to the previous screen or menu.</td>
</tr>
<tr>
<td>5</td>
<td>Release button</td>
<td>Ends a connected call or session.</td>
</tr>
<tr>
<td></td>
<td>Navigation pad and Select button</td>
<td>The four-way Navigation pad allows you to scroll through menus, highlight items, and move within a text input field. The Select button (center of the Navigation pad) allows you to select a highlighted item. The Select button is lit (white) when the phone is in Power Save or Power Save Plus mode. Press the Select button to override Power Save and Power Save Plus mode.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>7</td>
<td>Conference button</td>
<td>Creates a conference call.</td>
</tr>
<tr>
<td>8</td>
<td>Hold button</td>
<td>Places a connected call on hold and toggles between an ongoing and held call.</td>
</tr>
<tr>
<td>9</td>
<td>Transfer button</td>
<td>Transfers a call.</td>
</tr>
<tr>
<td>10</td>
<td>Keypad</td>
<td>Allows you to dial phone numbers, enter letters, and choose menu items by entering the item number.</td>
</tr>
<tr>
<td>11</td>
<td>Speakerphone button</td>
<td>Selects the speakerphone as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green. The speakerphone audio path does not change until you select a new default audio path (for example, by picking up the handset). If external speakers are connected, the Speakerphone button selects them as the default audio path.</td>
</tr>
<tr>
<td>12</td>
<td>Mute button</td>
<td>Toggles the microphone on or off during a call. When the microphone is muted, the button is lit red. When muted, you can hear the other parties on the call, but they cannot hear you.</td>
</tr>
<tr>
<td>13</td>
<td>Headset button</td>
<td>Selects the headset as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green. A headset icon in the phone screen header line indicates the headset is the default audio path. This audio path does not change until you select a new default audio path (for example, by picking up the handset).</td>
</tr>
<tr>
<td></td>
<td>Component</td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
|14 | Volume button                    | Controls the handset, headset, and speakerphone volume (off hook) and the ringer volume (on hook).  
Silences the ringer on the phone if an incoming call is ringing. |
|15 | Messages button                  | Autodials your voicemail system (varies by system).                         |
|16 | Applications button              | Opens/closes the Applications menu. Depending on how your system administrator sets up the phone, use it to access applications such as call history, preferences, and phone information. |
|17 | Contacts button                  | Opens/closes the Contacts menu. Depending on how your system administrator sets up the phone, use it to access personal directory, corporate directory, or call history. |
|18 | Phone display                    | Can be positioned to your preferred viewing angle.                           |
|19 | Programmable feature buttons     | Each button corresponds to a phone line, speed dial, and calling feature.  
Press a button for a phone line to display the active calls for that line.  
If you have multiple lines, you may have an All Calls button that displays a consolidated list of all calls from all lines (oldest at the top). If you do not see the All Calls button, your system administrator may have set up the primary line to automatically display all calls. For information on your set up, contact your system administrator.  
Color LEDs indicate the line state:  
  - Amber: Ringing call on this line  
  - Green: Active or held call on this line  
  - Red: Shared line in-use remotely  
The position of the programmable feature buttons can be reversed with the position of the session buttons on phones that use a locale with a right-to-left reading orientation, such as Hebrew and Arabic. |
|20 | Handset with light strip         | The handset light strip lights up to indicate a ringing call (flashing red) or a new voice message (steady red). |

**Cisco Unified IP Phone 9971**

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

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

1. DC adapter port (DC48V)
2. AC-to-DC power supply (optional for the network port connection but required for a Wi-Fi connection)
3. AC power wall plug (optional)
4. Network port (10/100/1000 SW) with IEEE 802.3af and 802.3at power enabled
5. Computer port (10/100/1000 PC) connection
6. Handset connection
7. Analog headset connection (optional)
8. USB port
9. Anti-theft security lock connector (lock optional)
10. Camera pin holes (for Cisco Unified Video Camera)
11. Secure Digital I/O (SDIO) slot (not used for this release)

The following picture shows the side of the phone.
### Buttons and Hardware

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

- Use the feature buttons (on the left) to view calls on a line or access features such as Speed Dial or All Calls.
- Use the call session buttons (on the right) to perform tasks such as making a call, answering a call, or resuming a held call. Each call on your phone is associated with a session button.

---

**Note** Each USB port supports the connection of up to five supported and nonsupported devices. Each device connected to the phone is included in the maximum device count. For example, your phone can support five USB devices (such as three Cisco Unified IP Color Key Expansion modules, one hub, and one other standard USB device) on the side port and five additional standard USB devices on the back port. Many third-party USB products count as multiple USB devices, for example, a device containing USB hub and headset can count as two USB devices. For more information, see the USB device documentation.
<p>|   | Phone screen | Shows information about your phone, including directory number, call information (for example, caller ID, icons for an active call or call on hold) and available softkeys. Phone screen items, such as menu options and softkeys, are touch-sensitive. |</p>
<table>
<thead>
<tr>
<th></th>
<th>Session buttons</th>
<th>Each button corresponds with an active call or a call function. When you press the button, the action depends on the state of the phone:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Active calls: Press the button to take the default action for an active call. For example, press the session button for a ringing call to answer the call and press the button on a held call to resume the call. Session information, such as caller ID and call duration, appears on the phone screen next to the session button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Call functions: When a session button is not being used for an active call, it can be used to initiate functions on the phone, as indicated by the adjacent phone screen icons. For example, press the session button to display missed calls, take the phone off hook, or dial your voicemail system (with a Voicemail icon).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Color LEDs reflect the call state. LEDs can flash (blink on and off rapidly), pulse (alternately dim and brighten), or appear solid (glow without interruption).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Flashing amber: Ringing call. Press this button to answer the call.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Solid green: May be a connected call or an outgoing call that is not yet connected. If the call is connected, press this button to display the call details or the participants of a conference call. If the call is not yet connected, press this button to end the call.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Pulsing green: Held call. Press this button to resume the held call.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Solid red: Shared line in use remotely. Press this button to barge into the call (if Barge is enabled).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Pulsing red: Shared line call put on hold remotely. Press this button to resume the held call.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The positions of the session buttons and feature buttons can be reversed on phones that use a locale with a right-to-left reading orientation, such as Hebrew and Arabic.</td>
</tr>
<tr>
<td>3</td>
<td>Back button</td>
<td>Returns to the previous screen or menu.</td>
</tr>
<tr>
<td>4</td>
<td>Release button</td>
<td>Ends a connected call or session.</td>
</tr>
<tr>
<td></td>
<td>Button Description</td>
<td>Function</td>
</tr>
<tr>
<td>---</td>
<td>-------------------</td>
<td>----------</td>
</tr>
<tr>
<td>5</td>
<td>Navigation pad and Select button</td>
<td>The four-way Navigation pad allows you to scroll through menus, highlight items, and move within a text input field. The Select button (center of the Navigation pad) allows you to select a highlighted item, disable the phone screen for cleaning, or enable the phone screen if it is in power-save mode. The Select button is lit (white) when the phone is in Power Save or Power Save Plus mode. Press the Select button to override Power Save and Power Save Plus mode.</td>
</tr>
<tr>
<td>6</td>
<td>Conference button</td>
<td>Creates a conference call.</td>
</tr>
<tr>
<td>7</td>
<td>Hold button</td>
<td>Places a connected call on hold and toggles between an active and held call.</td>
</tr>
<tr>
<td>8</td>
<td>Transfer button</td>
<td>Transfers a call.</td>
</tr>
<tr>
<td>9</td>
<td>Keypad</td>
<td>Allows you to dial phone numbers, enter letters, and choose menu items by entering the item number.</td>
</tr>
<tr>
<td>10</td>
<td>Speakerphone button</td>
<td>Selects the speakerphone as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green. The speakerphone audio path does not change until you select a new default audio path (for example, by picking up the handset). If external speakers are connected, the Speakerphone button selects them as the default audio path.</td>
</tr>
<tr>
<td>11</td>
<td>Mute button</td>
<td>Toggles the microphone on or off during a call. When the microphone is muted, the button is lit red. When muted, you can hear the other parties on the call, but they cannot hear you.</td>
</tr>
<tr>
<td>12</td>
<td>Headset button</td>
<td>Selects the wired or wireless headset as the default audio path and initiates a new call, picks up an incoming call, or ends a call. During a call, the button is lit green. A headset icon in the phone screen header line indicates the headset is the default audio path. This audio path does not change until a new default audio path is selected (for example, by picking up the handset).</td>
</tr>
</tbody>
</table>
13 Volume button

Controls the handset, headset, and speakerphone volume (off hook) and the ringer volume (on hook).
Silences the ringer on the phone if an incoming call is ringing.

14 Messages button

Autodials your voicemail system (varies by system).

15 Applications button

Opens/closes the Applications menu. Depending on how your system administrator sets up the phone, use it to access applications such as call history, preferences, and phone information.

16 Contacts button

Opens/closes the Contacts menu. Depending on how your system administrator sets up the phone, use it to access personal directory, corporate directory, or call history.

17 Phone display

Can be positioned to your preferred viewing angle.

18 Programmable feature buttons (also called feature buttons)

Correspond to phone lines, speed dials, and calling features.
Press a button for a phone line to display the active calls for that line.
If you have multiple lines, you may have an All Calls button that displays a consolidated list of all calls from all lines (oldest at the top). If you do not see the All Calls button, your system administrator may have set up the primary line to automatically display all calls. For information on your set up, contact your system administrator.
Color LEDs indicate the line state:

- Amber: Ringing call on this line
- Green: Active or held call on this line
- Red: Shared line in-use remotely

The positions of the session buttons and feature buttons can be reversed on phones that use a locale with a right-to-left reading orientation, such as Hebrew and Arabic.

19 Handset with light strip

The handset light strip lights up to indicate a ringing call (flashing red) or a new voice message (steady red).

Terminology Differences

The following table highlights some of the differences in terminology found in the Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager (SIP), the Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager (SIP), and the Cisco Unified Communications Manager Administration Guide.
<table>
<thead>
<tr>
<th>User Guide</th>
<th>Administration Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line Status</td>
<td>Busy Lamp Field (BLF)</td>
</tr>
<tr>
<td>Message Indicators</td>
<td>Message Waiting Indicator (MWI) or Message Waiting Lamp</td>
</tr>
<tr>
<td>Programmable Feature Button</td>
<td>Programmable Button or Programmable Line Key (PLK)</td>
</tr>
<tr>
<td>Simplified New Call Window</td>
<td>Simplified New Call Bubble</td>
</tr>
<tr>
<td>Voicemail System</td>
<td>Voice Messaging System</td>
</tr>
</tbody>
</table>

Table 6: Terminology Differences
VoIP Wireless Network Setup for Cisco Unified IP Phone 9971

- VoIP Wireless Network Overview, page 43
- VoIP Wireless Network Components, page 43
- 802.11 Standards for WLAN Communications, page 50

VoIP Wireless Network Overview

This chapter provides an overview of the interaction between a wireless-capable Cisco Unified IP Phone 9971 and other key components of a VoIP network in a wireless local area network (WLAN) corporate environment. When you deploy a Cisco Unified IP Phone on a wireless LAN, you must use Cisco Unified Communications Manager Release 7.1(3) or later and the SIP protocol.

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

The Cisco Unified IP Phone 9971 supports Cisco Centralized Key Management (CCKM), a centralized key management protocol, and provides a cache of session credentials on the wireless domain server (WDS) with 802.1x+WEP or WPA(TKIP) only. APs must register to the WDS for fast roaming to work. CCKM is also supported on the Cisco Unified Wireless LAN Controller alone. CCKM is not supported with WPA2 or WPA(AES). For details about CCKM, see the Cisco Fast Secure Roaming Application Note at: http://www.cisco.com/en/US/products/hw/wireless/ps4570/prod_technical_reference09186a00801c5223.html.


VoIP Wireless Network Components

The Cisco Unified IP Phone 9971 depends upon and interacts with wireless access points (AP) that have the correct QoS and key Cisco IP telephony components, including Cisco Unified Communications Manager.
Administration, to provide wireless voice communication. Cisco Access Points can run in standalone or unified mode. Unified mode requires the Cisco Unified Wireless LAN Controller.

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

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

*Figure 1: WLAN with Wireless IP Phones*

Cisco Unified Wireless AP Requirements

APs are critical components in a WLAN because they provide the wireless links or "hot spots" to the network. When a Cisco Unified IP Phone powers on, it searches for and becomes associated with an access point (AP) if the phone wireless access is set to On. The Cisco Unified IP Phone scans for APs with SSIDs and encryption types that it recognizes. The phone builds and maintains a list of eligible APs and uses the following variables to determine the best AP:

- Received Signal Strength Indicator (RSSI): Signal strength of available APs within the RF coverage area. The phone attempts to associate with the AP with the highest RSSI value and lowest channel usage values (QBSS) that possess matching SSID and encryption types.

- Traffic Specification (T Spec): Calculation of call limits and WLAN load balancing. The T Spec value of each voice stream allows the system to allocate bandwidth to voice devices on a first-come, first-served basis.

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

*Note* In a non-controller-based wireless network, we recommend that you statically configure channels for each AP. If your wireless network uses a controller, use the Auto-RF feature for minimal voice disruption.
For more information about AP channel and domain relationships, see Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide at this location:

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

Cisco requires that APs that support voice communications use Cisco IOS Release 12.3(8)JA or later. Cisco IOS software provides features for managing voice traffic. In some WLANs, each AP has a wired connection to an Ethernet switch, such as a Cisco Catalyst 3750, that is configured on a LAN. The switch provides access to gateways and the Cisco Unified Communications Manager server to support wireless IP telephony.

The wireless Cisco Unified IP Phone 9971 is supported on both the Cisco autonomous and unified solutions support the following access points:

Minimum and recommended versions are:

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

- Cisco Unified Wireless LAN Controller
  - Minimum = 5.1.163.0 or later
  - Recommended = 5.2.193.0 or later

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

Table 7: Supported APs and Modes

<table>
<thead>
<tr>
<th>AP Models</th>
<th>802.11b</th>
<th>802.11g</th>
<th>802.11a</th>
<th>Autonomus Mode</th>
<th>Unified Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Aironet 500 Series</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Aironet 1100 Series</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Aironet 1130 AG Series</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Aironet 1140 Series</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Aironet 1200 Series</td>
<td>Yes</td>
<td>Yes</td>
<td>Optional</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Aironet 1230 AG Series</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Aironet 1240 AG Series</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Aironet 1250 Series</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Aironet 1300 Series</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Cisco Unified IP Phones use the same APs as wireless data devices. However, voice traffic over a WLAN requires different equipment configurations and layouts than a WLAN that is used exclusively for data traffic. Data transmission can tolerate a higher level of RF noise, packet loss, and channel contention than voice transmission. Packet loss during voice transmission can cause choppy or broken audio and can make the phone call inaudible. Packet errors can also cause blocky or frozen video.

Because the Cisco Unified IP Phone 9971 is a desktop (not mobile) phone, changes in the local environment can cause phones to roam between access points and can affect the voice and video performance. In contrast, data users remain in one place or occasionally move to another location. The ability to roam while maintaining a call is one of the advantages of wireless voice, so RF coverage needs to include stairwells, elevators, quiet corners outside conference rooms, and passageways.

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

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

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

### AP Authentication and Encryption Options

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

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

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

- When you use WPA pre-shared key or WPA2 pre-shared key, the pre-shared key must be statically set on the phone. These keys must match the keys that are on the AP.

- When you use Auto (AKM), encryption options are automatically configured for WPA, WPA2, WPA Pre-shared key, WPA2 Pre-shared key, or CCKM.

- In AKM mode, the phone authenticates with LEAP if the phone is configured with WPA, WPA2, or CCKM key management, or if 802.1x is used.

- The Cisco Unified IP Phone does not support auto EAP negotiation; to use EAP-FAST mode, you must specify it.

The following table provides a list of authentication and encryption schemes that are configured on the Cisco Aironet APs that the Cisco Unified IP Phone supports. The table shows the network configuration option for the phone that corresponds to the AP configuration.

### Table 8: Authentication and Encryption Schemes

<table>
<thead>
<tr>
<th>Cisco AP configuration</th>
<th>Cisco Unified IP Phone configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication</strong></td>
<td><strong>Key management</strong></td>
</tr>
<tr>
<td>Open</td>
<td>None</td>
</tr>
<tr>
<td>Open (Static WEP)</td>
<td>WEP</td>
</tr>
<tr>
<td>Shared key (Static WEP)</td>
<td>WEP</td>
</tr>
<tr>
<td>LEAP 802.1x</td>
<td>Optional CCKM</td>
</tr>
<tr>
<td>LEAP WPA</td>
<td>WPA with optional CCKM</td>
</tr>
<tr>
<td>LEAP WPA2</td>
<td>WPA2</td>
</tr>
<tr>
<td>EAP-FAST 802.1x</td>
<td>Optional CCKM</td>
</tr>
<tr>
<td>EAP-FAST with WPA</td>
<td>WPA</td>
</tr>
<tr>
<td>EAP-FAST with WPA2</td>
<td>WPA2</td>
</tr>
<tr>
<td>WPA-PSK</td>
<td>WPA-PSK</td>
</tr>
</tbody>
</table>

**Key management**

- Common encryption
- Open
- WEP
- Shared key (Static WEP)
- Optional CCKM
- WPA with optional CCKM
- WPA2
- WPA-PSK

**Authentication**

- LEAP or Auto (AKM)
- LEAP or Auto (AKM)
- LEAP or Auto (AKM)
- EAP-FAST
- EAP-FAST
### Wireless Voice Quality Considerations

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

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

- **2.4 GHz**: Many devices that use 2.4 GHz can potentially interfere with the 802.11b/g connection. Interference can produce a Denial of Service (DoS) scenario, possibly preventing successful 802.11 transmissions.

- **5 GHz**: This range divides into several sections called Unlicensed National Information Infrastructure (UNII) bands, each of which has four channels. The channels are spaced at 20 MHz to provide nonoverlapping channels and more channels than 2.4 GHz provides.

The recommended channels for 802.11b and 802.11g in North America are 1, 6, and 11.

**Note**

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

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

### Wireless Voice QoS Requirements

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

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

<table>
<thead>
<tr>
<th>Cisco AP configuration</th>
<th>Cisco Unified IP Phone configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPA2-PSK</td>
<td>WAP2-PSK</td>
</tr>
<tr>
<td>AES</td>
<td>Auto (AKM)</td>
</tr>
</tbody>
</table>


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

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

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

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

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

Figure 2: Voice Traffic in a Wireless Network

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

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

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

Note

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

To improve reliability of voice transmissions in a nondeterministic environment, the Cisco Unified IP Phone supports the IEEE 802.11e industry standard and is Wi-Fi Multimedia (WMM) capable. WMM enables differentiated services for voice, video, best effort data and other traffic. However, in order for these differentiated services to provide sufficient QoS for voice packets, only a certain amount of voice bandwidth can be serviced or admitted on a channel at one time. If the network can handle "N" voice calls with reserved bandwidth, when the amount of voice traffic is increased beyond this limit (to N+1 calls), the quality of all calls suffers.
To help address the problems of VoIP stability and roaming, an initial Call Admission Control (CAC) scheme is required. With CAC, QoS is maintained in a network overload scenario by ensuring that the number of active voice calls does not exceed the configured limits on the AP. The Cisco Unified IP Phone can integrate layer 2 TSpec admission control with layer 3 Cisco Unified Communications Manager admission control (RSVP). During times of network congestion, calling or called parties receive a fast busy indication. The system maintains a small bandwidth reserve so wireless phone clients can roam into a neighboring AP, even when the AP is at full capacity. After reaching the voice bandwidth limit, the next call is load-balanced to a neighboring AP without affecting the quality of the existing calls on the channel.

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

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


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

Supported Antennas

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


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

802.11 Standards for WLAN Communications

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

- 802.11a: Uses the 5 GHz band that provides more channels and improved data rates by using OFDM technology. Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) support this standard.

- 802.11b: Specifies the radio frequency (RF) of 2.4 Ghz for both transmitting and receiving data at lower data rates (1, 2, 5.5, 11 Mbps).
• 802.11d: Enables access points to advertise their currently supported radio channels and transmit power levels. The 802.11d enabled client then uses that information to determine the channels and powers to use. The Cisco Unified IP Phone 9971 requires World mode (802.11d) to determine which channels are legally allowed for any given country. For supported channels, see the following table. Ensure that 802.11d is properly configured on the Cisco IOS Access Points or Cisco Unified Wireless LAN Controller.

• 802.11e: Quality of Service (QoS).

• 802.11g: Uses the same unlicensed 2.4 Ghz band as 802.11b, but extends the data rates to provide greater performance by using Orthogonal Frequency Division Multiplexing (OFDM) technology. OFDM is a physical-layer encoding technology for transmitting signals by using RF.

• 802.11h: 5 GHz spectrum and transmit power management.

• 802.11i: Security.

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Band Range</th>
<th>Available Channels</th>
<th>5 GHz Channel Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP-9971-K9</td>
<td>2.412 – 2.484 GHz</td>
<td>13 (14 in Japan)</td>
<td>UNII-2</td>
</tr>
<tr>
<td></td>
<td>5.180 – 5.240 GHz</td>
<td>4</td>
<td>UNII-2</td>
</tr>
<tr>
<td></td>
<td>5.260 – 5.320 GHz</td>
<td>4</td>
<td>UNII-2 Extended</td>
</tr>
<tr>
<td></td>
<td>5.500 – 5.700 GHz</td>
<td>11</td>
<td>UNII-3</td>
</tr>
<tr>
<td></td>
<td>5.745 – 5.805 GHz</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

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

Related Topics
World Mode (802.11d), on page 51

World Mode (802.11d)

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

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

Because all countries support these frequencies, you can attempt to scan these channels regardless of World mode (802.11d) support. For the countries that support 2.4GHz, see Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide at this location: http://www.cisco.com/en/US/products/ps10453/products_implementation_design_guides_list.html

Enable World mode (802.11d) for the corresponding country where the access point is located. World mode is enabled automatically for the Cisco Unified Wireless LAN Controller.
You must enable World mode for Cisco Autonomous Access Points by using the following commands:

- Interface dot11radio X
- world-mode dot11d country US both

The Cisco Unified IP Phone 9971 supports the following countries:

<table>
<thead>
<tr>
<th>Country 1</th>
<th>Country 2</th>
<th>Country 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Argentina (AR)</td>
<td>India (IN)</td>
<td>Poland (PL)</td>
</tr>
<tr>
<td>Australia (AU)</td>
<td>Indonesia (ID)</td>
<td>Portugal (PT)</td>
</tr>
<tr>
<td>Austria (AT)</td>
<td>Ireland (IE)</td>
<td>Puerto Rico (PR)</td>
</tr>
<tr>
<td>Belgium (BE)</td>
<td>Israel (IL)</td>
<td>Romania (RO)</td>
</tr>
<tr>
<td>Brazil (BR)</td>
<td>Italy (IT)</td>
<td>Russian Federation (RU)</td>
</tr>
<tr>
<td>Bulgaria (BG)</td>
<td>Japan (JP)</td>
<td>Saudi Arabia (SA)</td>
</tr>
<tr>
<td>Canada (CA)</td>
<td>Korea (KR / KP)</td>
<td>Singapore (SG)</td>
</tr>
<tr>
<td>Chile (CL)</td>
<td>Latvia (LV)</td>
<td>Slovakia (SK)</td>
</tr>
<tr>
<td>Colombia (CO)</td>
<td>Liechtenstein (LI)</td>
<td>Slovenia (SI)</td>
</tr>
<tr>
<td>Costa Rica (CR)</td>
<td>Lithuania (LT)</td>
<td>South Africa (ZA)</td>
</tr>
<tr>
<td>Cyprus (CY)</td>
<td>Luxembourg (LU)</td>
<td>Spain (ES)</td>
</tr>
<tr>
<td>Czech Republic (CZ)</td>
<td>Malaysia (MY)</td>
<td>Sweden (SE)</td>
</tr>
<tr>
<td>Denmark (DK)</td>
<td>Malta (MT)</td>
<td>Switzerland (CH)</td>
</tr>
<tr>
<td>Estonia (EE)</td>
<td>Mexico (MX)</td>
<td>Taiwan (TW)</td>
</tr>
<tr>
<td>Finland (FI)</td>
<td>Monaco (MC)</td>
<td>Thailand (TH)</td>
</tr>
<tr>
<td>France (FR)</td>
<td>Netherlands (NL)</td>
<td>Turkey (TR)</td>
</tr>
<tr>
<td>Germany (DE)</td>
<td>New Zealand (NZ)</td>
<td>Ukraine (UA)</td>
</tr>
<tr>
<td>Gibraltar (GI)</td>
<td>Norway (NO)</td>
<td>United Arab Emirates (AE)</td>
</tr>
<tr>
<td>Greece (GR)</td>
<td>Oman (OM)</td>
<td>United Kingdom (GB)</td>
</tr>
<tr>
<td>Hong Kong (HK)</td>
<td>Panama (PA)</td>
<td>United States (US)</td>
</tr>
<tr>
<td>Hungary (HU)</td>
<td>Peru (PE)</td>
<td>Venezuela (VE)</td>
</tr>
<tr>
<td>Iceland (IS)</td>
<td>Philippines (PH)</td>
<td>Vietnam (VN)</td>
</tr>
</tbody>
</table>
802.11 Data Rates, Transmit Power, Ranges, and Decibel Tolerances

The following table lists the transmit (Tx) power capacities, data rates, ranges in feet and meters, and decibels that the receiver tolerates for the 802.11 standards.

Table 9: Tx Power, Data Rates, Ranges, and Decibels by Standard

<table>
<thead>
<tr>
<th>Standard</th>
<th>Maximum Tx Power (See Note 1)</th>
<th>Data Rate (See Note 2)</th>
<th>Range</th>
<th>Receiver Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>16 dBm</td>
<td>6 Mbps</td>
<td>604 ft (184 m)</td>
<td>-91 dBm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9 Mbps</td>
<td>604 ft (184 m)</td>
<td>-90 dBm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12 Mbps</td>
<td>551 ft (168 m)</td>
<td>-88 dBm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>18 Mbps</td>
<td>545 ft (166 m)</td>
<td>-86 dBm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>24 Mbps</td>
<td>512 ft (156 m)</td>
<td>-82 dBm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>36 Mbps</td>
<td>420 ft (128 m)</td>
<td>-80 dBm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>48 Mbps</td>
<td>322 ft (98 m)</td>
<td>-77 dBm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>54 Mbps</td>
<td>289 ft (88 m)</td>
<td>-75 dBm</td>
</tr>
<tr>
<td>802.11g</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>16 dBm</td>
<td>6 Mbps</td>
<td>709 ft (216 m)</td>
<td>-91 dBm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9 Mbps</td>
<td>650 ft (198 m)</td>
<td>-90 dBm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12 Mbps</td>
<td>623 ft (190 m)</td>
<td>-87 dBm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>18 Mbps</td>
<td>623 ft (190 m)</td>
<td>-86 dBm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>24 Mbps</td>
<td>623 ft (190 m)</td>
<td>-82 dBm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>36 Mbps</td>
<td>495 ft (151 m)</td>
<td>-80 dBm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>48 Mbps</td>
<td>413 ft (126 m)</td>
<td>-77 dBm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>54 Mbps</td>
<td>394 ft (120 m)</td>
<td>-76 dBm</td>
</tr>
<tr>
<td>802.11b</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Receiver Sensitivity

<table>
<thead>
<tr>
<th>Standard</th>
<th>Maximum Tx Power (See Note 1)</th>
<th>Data Rate (See Note 2)</th>
<th>Range</th>
<th>Receiver Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>17 dBm</td>
<td>1 Mbps</td>
<td>1,010 ft (308 m)</td>
<td>-96 dBm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Mbps</td>
<td>951 ft (290 m)</td>
<td>-85 dBm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.5 Mbps</td>
<td>919 ft (280 m)</td>
<td>-90 dBm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 Mbps</td>
<td>902 ft (275 m)</td>
<td>-87 dBm</td>
</tr>
</tbody>
</table>

**Note**

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

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

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

### Wireless Modulation Technologies

Wireless communications use the following modulation technologies for signaling:

**Direct-Sequence Spread Spectrum (DSSS)**

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

**Orthogonal Frequency Division Multiplexing (OFDM)**

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

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

**Table 10: Data Rates, Number of Channels, and Modulation Technologies by IEEE Standard**

<table>
<thead>
<tr>
<th>Item</th>
<th>802.11b</th>
<th>802.11g</th>
<th>802.11a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data rates</td>
<td>1, 2, 5.5, 11 Mbps</td>
<td>6, 9, 12, 18, 24, 36, 48, 54 Mbps</td>
<td>6, 9, 12, 18, 24, 36, 48, 54 Mbps</td>
</tr>
<tr>
<td>Item</td>
<td>802.11b</td>
<td>802.11g</td>
<td>802.11a</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Nonoverlapping</td>
<td>3 (Japan uses 4)</td>
<td>3</td>
<td>Up to 23</td>
</tr>
<tr>
<td>channels</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless modulation</td>
<td>DSSS</td>
<td>OFDM</td>
<td>OFDM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
PART II

Cisco Unified IP Phone Installation

- Cisco Unified IP Phone Installation, page 59
- Cisco Unified Communications Manager Phone Setup, page 87
- Self Care Portal Management, page 99
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.

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

Procedure

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

• VoIP is configured on your Cisco routers and gateways.
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. 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** Select the required server and then check Autoregister.

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

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

**Step 4** Click Save.

**Related Topics**

Phone Addition Methods, on page 91

**Install Cisco Unified IP Phone**

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

**Note**

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


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

If you used autoregistration, you need to update the specific configuration information for the phone such as associating the phone with a user, changing the button table, or directory number.
Before you install a phone, even if it is new, upgrade the phone to the current firmware image. Before using external devices, read External Devices, on page 17 for safety and performance information.

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

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

Procedure

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

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

For more information, see Phone Power Requirements, on page 6.

Step 2 Connect the handset to the headset port. With a wall-mounted phone, you might need to adjust the handset rest to ensure that the receiver cannot slip out of the cradle. See Adjust the Handset Rest, on page 154.

Step 3 (Optional) Connect a headset to the headset port. You can add a headset later if you do not connect one now. For more information, see Headsets, on page 106.

Step 4 Connect a wireless headset (for the Cisco Unified IP Phone 9951 and 9971 only). You can add a wireless headset later if you do not want to connect one now. For more information, see your wireless headset documentation.

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

Step 6 (Optional) Connect a straight-through Ethernet cable from another network device, such as a desktop computer, to the computer port on the Cisco Unified IP Phone. You can connect another network device later if you do not connect one now.
You can use Category 3, 5, or 5e cabling for 10 Mbps connections; Category 5 or 5e for 100 Mbps connections; and Category 5e for 1000 Mbps connections.

Step 7 Monitor the phone startup process. This step adds primary and secondary directory numbers and features that are associated with directory numbers to the phone, and verifies that the phone is configured properly. For more information, see Phone Startup Process, on page 85.

Step 8 If you choose to deploy the Cisco Unified IP Phone 9971 on a wireless network, skip to Step 9.
If you are configuring the Ethernet network settings on the phone for an IP network, you can set up an IP address for the phone either by using DHCP or by manually entering an IP address. For more information, see Configure Network Settings, on page 70, Set Up Phone To Use DHCP, on page 84, and Set Up Phone To Not Use DHCP, on page 85.
Step 9 (Cisco Unified IP Phone 9971 only) If you choose to deploy the Cisco Unified IP Phone 9971 on the wireless network, you must perform the following:

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

Note The wireless LAN on the phone does not activate when Ethernet cables are connected on the phone. For more information, see VoIP Wireless Network Setup for Cisco Unified IP Phone 9971, on page 43.

Step 10 Make calls with the Cisco Unified IP Phone to verify that the phone and features work correctly. See the Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager.

Step 11 Provide information to end users about how to use their phones and how to configure their phone options. This step ensures that users have adequate information to successfully use their Cisco Unified IP Phones. For more information, see Cisco IP Phone User Support, on page 183

Step 12 Adjust the footstand. For more information, see Connect Footstand, on page 104.

Step 13 Secure the phone with a cable lock. For more information, see Secure the Phone with a Cable Lock, on page 105.

Related Topics
Set Up Remote Phone, on page 320

Set Up Phone from Setup Menus

The Cisco Unified IP Phone includes the following configuration menus:

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

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

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

- Security Setup: Provides options for viewing and configuring security settings such as security mode, the trust list and 802.1X authentication.
Before you can change option settings on the Network Setup menu, you must unlock options for editing.

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

- **Enabled**: Allows access to the Settings menu.
- **Disabled**: Prevents access to the Settings menu.
- **Restricted**: Allows access to the User Preferences menu and allows volume changes to be saved. Prevents access to other options on the Settings menu.

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

**Procedure**

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

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

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

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

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

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

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

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

**Apply a Phone Password**

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

**Procedure**

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

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

**Step 3** Apply the password to the common phone profile that the phone uses.
Text and Menu Entry from Phone

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

• Use the arrows on the navigation pad to highlight the field that you wish to edit, then press Select in the navigation pad to activate the field. After the field is activated, you can enter values.
• Use the keys on the keypad to enter numbers and letters.
• To enter letters by using the keypad, use a corresponding number key. Press the key one or more times to display a particular letter. For example, press the 2 key once for "a," twice quickly for "b," and three times quickly for "c." After you pause, the cursor automatically advances to allow you to enter the next letter.
• Press the arrow softkey ⬅ if you make a mistake. This softkey deletes the character to the left of the cursor.
• Press Cancel before pressing Save to discard any changes that you made.
• To enter an IP address, you enter values into four segments already divided for you. When you have finished entering the leftmost digits before the first period, use the right arrow key to move to the next segment. The period that follows the leftmost digits is automatically inserted.
• To enter a colon for an IPv6 address, press * on the keypad.

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

Set Up Wireless LAN

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

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

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


The Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide includes the following configuration information:

• Wireless network configuration
Set Up Wireless LAN on Cisco Unified Communications Manager

In Cisco Unified Communications Manager Administration, you must enable a parameter called "Wi-Fi" for the wireless Cisco Unified IP Phone 9971.

Note

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

Procedure

Step 1 To enable the wireless LAN on a specific phone perform the following steps:
   a) Select Device > Phone.
   b) Locate the required phone.
   c) Select the enable setting for the Wi-Fi parameter in the Product Specific Configuration Layout section
   d) Check the Override Common Settings check box

Step 2 To enable wireless LAN for a group of phones,
   a) Select Device > Device Settings > Common Phone Profile.
   b) Select the enable setting for the Wi-Fi parameter
   c) Check the Override Common Settings check box
   d) Associate the phones with that common phone profile using Device > Phone.

Step 3 To enable wireless LAN for all WLAN-capable phones in your network,
   a) Select System > Enterprise Phone Configuration.
   b) Select the enable setting for the Wi-Fi parameter.
   c) Check the Override Common Settings check box.
Set Up Wireless LAN on Cisco Unified IP Phone

Before the Cisco Unified IP Phone 9971 can connect to the WLAN, you must configure the network profile for the phone with the appropriate WLAN settings. You can use the Network Setup menu on the phone to access the Wireless Setup submenu and set up the WLAN configuration.

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

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

Procedure

Step 1
Press Applications.

Step 2
Select Administrator Settings > Network Setup > Wireless Setup.

Step 3
Set up the wireless configuration as described in the following table.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless</td>
<td>Turns the wireless radio on Cisco Unified IP Phone on or off. Valid values specify:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• On: Turns the wireless radio on the phone on.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Off: Turns the wireless radio on the phone off.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: On</td>
<td>See Set Wireless Field, on page 80.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>To Change</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• On: The Wireless Sign In Access window displays. Turning this value on allows you to sign in or change your Wireless user ID and password on the main Applications menu. Otherwise, to change your sign-in information, navigate down to the Security menu level and select either the LEAP or EAP-FAST methods, both of which require sign-in credentials.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Off: The Wireless Sign In Access window does not display.</td>
<td></td>
</tr>
<tr>
<td>Default: Off</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv4 Setup</td>
<td>In the IPv4 Setup configuration submenu, you can do the following:</td>
<td>Scroll to IPv4 Setup and press Select.</td>
</tr>
<tr>
<td></td>
<td>• Enable or disable the phone to use the IP address that the DHCP server assigns.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Manually set the IP Address, Subnet Mask, Default Routers, DNS Server, and Alternate TFTP servers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For more information about the IPv4 address fields, see <em>Set Up IPv4</em>, on page 73.</td>
<td></td>
</tr>
<tr>
<td>IPv6 Setup</td>
<td>In the IPv6 Setup configuration submenu, you can do the following:</td>
<td>Scroll to IPv6 Setup and press Select.</td>
</tr>
<tr>
<td></td>
<td>• Enable or disable the phone to use the IPv6 address that the DHCP server assigns.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Manually set the IPv6 Address, Prefix Length, Default Routers, DNS Server, and Alternate TFTP servers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For more information about the IPv6 address fields, see <em>Set Up IPv6</em>, on page 76.</td>
<td></td>
</tr>
<tr>
<td>MAC Address</td>
<td>Unique Media Access Control (MAC) address of the phone.</td>
<td>Display only. Cannot configure.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>To Change</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Name of the Domain Name System (DNS) domain in which the phone resides.</td>
<td>See Set Domain Name Field, on page 79.</td>
</tr>
<tr>
<td>SSID</td>
<td>Specifies the Service Set Identifier, a unique identifier for accessing wireless access points.</td>
<td>See Set SSID Field, on page 81.</td>
</tr>
<tr>
<td>Security Mode</td>
<td>The type of authentication that the phone uses to access the WLAN. Valid values specify:</td>
<td>See Set Security Mode Field, on page 81.</td>
</tr>
<tr>
<td></td>
<td>• Open: Access to all access points (APs) without encryption.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Open with WEP: Open 802.11 authentication but uses Wired Equivalent Privacy (WEP) for encrypting the data. Specifies access to all APs and authentication through WEP keys at the local AP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Shared Key: Shared key authentication using WEP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LEAP: Lightweight Extensible Authentication Protocol authentication exchanges a username and cryptographically secure password with a RADIUS server in the network. LEAP is a Cisco proprietary version of EAP. LEAP supports WPA and WPA2.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EAP-FAST: Extensible Authentication Protocol Flexible Authentication via Secure Tunneling exchanges a username and cryptographically secure password with a RADIUS server in the network where a PAC (Protected Access Credential) establishes a secure tunnel for authentication. EAP-FAST supports WPA and WPA2.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AKM: Selects the 802.11 authentication mechanism automatically from the configuration information that the access point exhibits. WPA-PSK or WPA versions 1 or 2 can be used if they are configured for this mode.</td>
<td></td>
</tr>
</tbody>
</table>
Configure Network Settings

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

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

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

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

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

---

### Configure Network Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11 Mode</td>
<td>Specifies the wireless signal standard that is used in the WLAN. Valid values specify:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Auto: Default value. Gives precedence to 5.0 Ghz if available.</td>
<td>See Set 802.11 Mode Field, on page 82.</td>
</tr>
<tr>
<td></td>
<td>- 802.11a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 802.11b/g</td>
<td></td>
</tr>
</tbody>
</table>

Note: Consider the following when you select AKM:

- AKM uses LEAP for 802.1x when WPA, WPA2, or CCKM is in use.
- AKM selects the encryption method by giving precedence to the strongest key management type and then the strongest cipher.
- CCKM is not supported with WPA2.
Table 11: Ethernet Setup Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Setup</td>
<td>In the IPv4 Setup configuration submenu, you can do the following:</td>
<td>Scroll to IPv4 Setup and press Select. See Set Up IPv4, on page 73.</td>
</tr>
<tr>
<td></td>
<td>• Enable or disable the phone to use the IP address that the DHCP server assigns.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Manually set the IP Address, Subnet Mask, Default Routers, DNS Server, and Alternate TFTP servers.</td>
<td></td>
</tr>
<tr>
<td>MAC Address</td>
<td>Unique Media Access Control (MAC) address of the phone.</td>
<td>Display only. Cannot configure.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Name of the Domain Name System (DNS) domain in which the phone resides.</td>
<td>See Set Domain Name Field, on page 79.</td>
</tr>
<tr>
<td>Operational VLAN ID</td>
<td>Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch of which the phone is a member.</td>
<td>Display only. Cannot configure. The phone obtains the Operational VLAN ID via Cisco Discovery Protocol (CDP) or Link Level Discovery Protocol Media Endpoint Discovery (LLDP-MED). This information comes from the switch to which the phone is attached. To assign a VLAN ID manually, use the Admin VLAN ID option.</td>
</tr>
<tr>
<td>Admin. VLAN ID</td>
<td>Auxiliary VLAN of which the phone is a member.</td>
<td>See Set Admin VLAN ID Field, on page 79.</td>
</tr>
<tr>
<td></td>
<td>Used only if the phone does not receive an auxiliary VLAN from the switch; otherwise, this value is ignored.</td>
<td></td>
</tr>
<tr>
<td>PC VLAN</td>
<td>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.</td>
<td>See Set PC VLAN Field, on page 79.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>To Change</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SW Port Setup</td>
<td>Speed and duplex of the network port. Valid values specify:</td>
<td>See Set SW Port Setup Field, on page 80.</td>
</tr>
<tr>
<td></td>
<td>• Auto Negotiate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1000 Full: 1000-BaseT/full duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 100 Half: 100-BaseT/half duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 100 Full: 100-BaseT/full duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 10 Half: 10-BaseT/half duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 10 Full: 10-BaseT/full duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the phone is connected to a switch, configure the port on the switch to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the same speed/duplex as the phone, or configure both to autonegotiate.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you change the setting of this option, you must change the SW Port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuration option to the same setting.</td>
<td></td>
</tr>
<tr>
<td>PC Port Setup</td>
<td>Speed and duplex of the Computer (access) port. Valid values:</td>
<td>See Set PC Port Setup Field, on page 80.</td>
</tr>
<tr>
<td></td>
<td>• Auto Negotiate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1000 Full: 1000-BaseT/full duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 100 Half: 100-BaseT/half duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 100 Full: 100-BaseT/full duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 10 Half: 10-BaseT/half duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 10 Full: 10-BaseT/full duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the phone is connected to a switch, configure the port on the switch to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the same speed/duplex as the phone, or configure both to autonegotiate.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you change the setting of this option, you must change the SW Port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuration option to the same setting.</td>
<td></td>
</tr>
</tbody>
</table>

**Note** If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to autonegotiate.

To configure the setting on multiple phones simultaneously, enable Remote Port Configuration in the Enterprise Phone Configuration window (**System > Enterprise Phone Configuration**).

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.
**Procedure**

**Step 1**
Press Applications 📲.

**Step 2**
To access the Network Settings menu, select Administrator Settings > Network Settings

**Related Topics**
- Network Protocols, on page 9
- Status Messages Fields, on page 265

**Set Up IPv4**

The following table describes the IPv4 Setup menu options.

*Table 12: IPv4 Setup Menu Options*

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Enabled</td>
<td>Indicates whether the phone has DHCP enabled or disabled.</td>
<td>See Set DHCP Enabled Field, on page 82.</td>
</tr>
<tr>
<td></td>
<td>When DHCP is enabled, the DHCP server assigns the phone an IP address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When DHCP is disabled, the administrator must manually assign an IP address to the phone.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For more information, see Set Up Phone To Use DHCP, on page 84 and Set Up Phone To Not Use DHCP, on page 85.</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>Internet Protocol (IP) address of the phone.</td>
<td>See Set IP Address Field, on page 82.</td>
</tr>
<tr>
<td></td>
<td>If you assign an IP address with this option, you must also assign a subnet mask and default router.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>See the Subnet Mask and Default Router options in this table.</td>
<td></td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Subnet mask used by the phone.</td>
<td>See Set Subnet Mask Field, on page 83.</td>
</tr>
<tr>
<td>Default Router</td>
<td>Default router used by the phone.</td>
<td>See Set Default Router Field, on page 83.</td>
</tr>
<tr>
<td>DNS Server 1</td>
<td>Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2 and 3) that the phone uses.</td>
<td>See Set DNS Server Fields, on page 83.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>To change</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Alternate TFTP</td>
<td>Indicates whether the phone is using an alternate TFTP server.</td>
<td>See Set Alternate TFTP Field, on page 83.</td>
</tr>
<tr>
<td>TFTP Server 1</td>
<td>Primary Trivial File Transfer Protocol (TFTP) server that the phone uses. If you are not using DHCP in your network and you want to change this server, you must use the TFTP Server 1 option. If you set the Alternate TFTP option to yes, you must enter a nonzero value for the TFTP Server 1 option. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL or ITL file on the phone, you must unlock the file before you can save changes to the TFTP Server 1 option. In this case, the phone deletes the file when you save changes to the TFTP Server 1 option. A new CTL or ITL file downloads from the new TFTP Server 1 address. When the phone looks for the TFTP server, the phone gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for the TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for the TFTP server in this order: 1 Any manually assigned IPv6 TFTP servers 2 Any manually assigned IPv4 TFTP servers 3 DHCPv6 assigned TFTP servers 4 DHCP assigned TFTP servers.</td>
<td>See Set TFTP Server 1 Field, on page 84.</td>
</tr>
</tbody>
</table>

**Note** For information about the CTL and ITL files, see the *Cisco Unified Communications Manager Security Guide*. 

---

*Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 10.0*
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
</table>
| TFTP Server 2  | Optional backup TFTP server that the phone uses if the primary TFTP server is unavailable. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL or ITL file on the phone, you must unlock either of the files before you can save changes to the TFTP Server 2 option. In this case, the phone deletes either of the files when you save changes to the TFTP Server 2 option. A new CTL or ITL file downloads from the new TFTP Server 2 address. When the phone looks for the TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for the TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for the TFTP server in the following order:  
1 Manually assigned IPv6 TFTP servers  
2 Manually assigned IPv4 TFTP servers  
3 DHCPv6 assigned TFTP servers  
4 DHCP assigned TFTP servers | See Set TFTP Server 2 Field, on page 84. If you forget to unlock the CTL or ITL file, you can change the TFTP Server 2 address in either file, then erase them by pressing Erase from the Security Configuration menu. A new CTL or ITL file downloads from the new TFTP Server 2 address. |
| BOOTP Server   | Indicates whether the phone received the IP address from a BOOTP server rather than from a DHCP server. | Display only.                                                                 |
| DHCP Address Released | Releases the IP address that DHCP assigned. | This field is editable if DHCP is enabled. If you wish to remove the phone from the VLAN and release the IP address for reassignment, set this option to Yes and press Apply. |

Note For information about the CTL or ITL file, see Cisco Unified Communications Manager Security Guide.
Procedure

Step 1
Press Applications.

Step 2
To access the Network Settings menu, select Administrator Settings > Network Settings.

Step 3
To access the IPv4 settings menu, perform one of the following actions:

- For Cisco Unified IP Phones 8961 and 9951: navigate to the IPv4 options from Ethernet Setup > IPv4 Setup.
- For Cisco Unified IP Phone 9971 with Wi-Fi disabled on the Cisco Unified Communications Manager: navigate to the Ethernet IPv4 options from Ethernet Setup > IPv4 Setup.
- For Cisco Unified IP Phone 9971 with Wi-Fi enabled on the Cisco Unified Communications Manager: navigate to Wireless Setup > IPv4 Setup.

Set Up IPv6

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

IPv6 addresses must be in one of the following formats:

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

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

- IP Addressing Mode
- IP Addressing Mode Preference for Signalling

If IPv6 is enabled in the Unified cluster, the default setting for IP addressing mode is IPv4 and IPv6 (dual-stack). In this addressing mode, the phone will acquire and use one IPv4 address and one IPv6 address. It can use the IPv4 and the IPv6 address as required for media. The phone uses either the IPv4 or IPv6 address for call control signalling to Unified CM.

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

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

You set up IPv6 from one of the following menus:

- On all phones: Ethernet Settings > IPv6 Setup
For the Cisco Unified IP Phone 9971, when WiFi is enabled: **Wireless Settings > IPv6 Setup**

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

*Table 13: IPv6 Setup Menu Options*

<table>
<thead>
<tr>
<th>Option</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPv6 Enabled</td>
<td>Yes</td>
<td>Indicates the method that the phone uses to get the IPv6 address. When DHCPv6 is enabled, the phone gets the IPv6 address using the DHCPv6 server of Stateless address autoconfiguration (SLAAC). When DHCPv6 is disabled, the administrator must assign all the IPv6 settings. <strong>Note</strong> Unlike DHCPv4, even DHCPv6 is disabled the phone can still generate a SLAAC address if autoconfigure is enabled.</td>
</tr>
</tbody>
</table>
| IPv6 Address          | ::            | Displays the current IPv6 address of the phone or allows the user to enter a new IPv6 address. Two address formats are supported:  
  • Compressed format to collapse a single run of consecutive zero groups into a single group represented by a double colon.  
  
  If the IP address is assigned with this option, you must also assign the IPv6 prefix length and the default router. |
| IPv6 Prefix Length    | 0             | Displays the current prefix length for the subnet or allows the user to enter a new prefix length.  
  The subnet prefix length is a decimal value from 1-128. |
| IPv6 Default Router   | ::            | Displays the default router used by the phone or allows the user to enter a new IPv6 default router. |
| IPv6 DNS Server 1     | ::            | Displays the primary DNSv6 server used by the phone or allows the user to enter a new server. |
| IPv6 DNS Server 2     | ::            | Displays the secondary DNSv6 server used by the phone or allows the user to set a new secondary DNSv6 server. |
| IPv6 Alternate TFTP   | No            | Allows the user to enable the use of an alternate (secondary) IPv6 TFTP server. |
| IPv6 TFTP Server 1    | ::            | Displays the primary IPv6 TFTP server used by the phone or allows the user to set a new primary TFTP server. |
### Configure Network Settings

**Option** | **Default Value** | **Description**
--- | --- | ---
IPv6 TFTP Server 2 | :: | (Optional) Displays the secondary IPv6 TFTP server used if the primary IPv6 TFTP server is unavailable or allows the user to set a new secondary TFTP server.
IPv6 Address Released | No | Allows the user to release IPv6-related information.

**Procedure**

**Step 1** Press Applications.

**Step 2** To access the Network Settings menu, select Administrator Settings > Network Settings.

**Step 3** To access the IPv6 settings menu, perform one of the following actions:

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

**Step 4** To enter IPv6 addresses,

a) Click in an input field.

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

The following table describes the address formats.

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

- To enter a colon (:) in the address, press the asterisk (*) on the keypad.
- To enter hexadecimal digits a, b, and c, press 2 on the keypad, scroll to select the required digit, and press Enter.
- To enter hexadecimal digits d, e, and f, press 3 on the keypad, scroll to select the required digit, and press Enter.
- After you enter each part of the address, you press Apply or Revert.
Step 5  Change toggle fields using these steps:
   a) If an option is set to No, press Yes to enable it. If the option is set to Yes, press No to disable it.
   b) Press Apply to save your change, or Revert to discard it.

Set Domain Name Field

Procedure

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

Set Admin VLAN ID Field

Procedure

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

Set PC VLAN Field

Procedure

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

Procedure

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

Set PC Port Setup Field

Procedure

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

Set Wireless Field

Procedure

Step 1 Scroll to the Wireless option, and use the toggle switch to change the setting between on and off. Valid values specify:
   • On: Turns the wireless radio on the phone on.
   • Off: Turns the wireless radio on the phone off.

Default: On

Step 2 Press Apply.

Set Wireless Sign In Access Field

Procedure

Step 1 Scroll to the Wireless Sign In option, and use the toggle switch to change the setting between on and off.
• On: The Wireless Sign In Access window is displayed. Turning this value on allows you to sign in or change your wireless user ID and password on the main Applications menu. Otherwise, to change your sign-in information, navigate to the Security Mode option under Wi-Fi client setup menu and select either EAP-FAST, PEAP-GTC, PEAP-MSCHAPv2 methods, all of which require sign-in credentials.

• Off: The Wireless Sign In Access window is not displayed.

Default: Off

Step 2
Press Apply.

Set SSID Field

Procedure

Step 1
Scroll to the SSID option, press Select, and enter an SSID.

Step 2
Press Apply.

Set Security Mode Field

Procedure

Step 1
Scroll to the Security Mode option, and highlight the desired value. Valid values specify:

• None: Access to all access points (APs) without encryption.

• WEP: Open 802.11 authentication that uses Wired Equivalent Privacy (WEP) to encrypt the data. Specifies access to all APs and authentication through WEP keys at the local AP.

• PSK: Shared key authentication uses AES or TKIP encryption.

• EAP-FAST: Extensible Authentication Protocol Flexible Authentication via Secure Tunneling exchanges a username and cryptographically secure password with a RADIUS server in the network where a PAC (Protected Access Credential) establishes a secure tunnel for authentication. EAP-FAST supports WPA and WPA2.

• PEAP(MSCHAPV2): Protected Extensible Authentication Protocol authentication exchanges a username and cryptographically secure password with a RADIUS server in the network. PEAP is a Cisco proprietary version of EAP. PEAP supports WPA and WPA2.

Step 2
Click Apply.
Set 802.11 Mode Field

**Procedure**

**Step 1** Scroll to the 802.11 Mode option, and select the desired value.

Valid values specify:

- Auto: Default value.
- 2.4 GHz
- 5 GHz

You can modify the 802.11 mode field only if the phone does not have a wireless LAN profile configured or the phone is configured with allowed wireless LAN profile.

**Step 2** Click **Save**.

**Step 3** Click **Apply**.

Set DHCP Enabled Field

**Procedure**

**Step 1** Scroll to the DHCP Enabled option.

**Step 2** Press **No** to disable DHCP, or press **Yes** to enable DHCP.

Set IP Address Field

**Procedure**

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

**Step 2** Scroll to the IP Address option, press **Select**, and enter a new IP Address.

**Step 3** Press **Apply**.
Set Subnet Mask Field

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Set the DHCP Enabled option to <strong>No</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Scroll to the Subnet Mask option, press <strong>Select</strong>, and enter a new subnet mask.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Press <strong>Apply</strong>.</td>
</tr>
</tbody>
</table>

Set Default Router Field

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Set the DHCP Enabled option to <strong>No</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Scroll to the appropriate Default Router option, press <strong>Select</strong>, and enter a new router IP address.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Press <strong>Apply</strong>.</td>
</tr>
</tbody>
</table>

Set DNS Server Fields

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Set the DHCP Enabled option to <strong>No</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Scroll to the appropriate DNS Server option, press <strong>Select</strong>, and enter a new DNS server IP address.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Press <strong>Apply</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>If multiple DNS Servers can be configured, repeat Steps 2 and 3 as needed to assign backup DNS servers.</td>
</tr>
</tbody>
</table>

Set Alternate TFTP Field

You must enter the Alternate TFTP and TFTP server fields when you configure an off-premises phone for SSL VPN to ASA using a built-in client.
### Set TFTP Server 1 Field

You must enter the Alternate TFTP server and TFTP Service 1 field when you configure an off-premises phone for SSL VPN to ASA using a built-in client.

**Procedure**

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

### Set TFTP Server 2 Field

**Procedure**

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

### Set Up Phone To Use DHCP

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

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

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

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

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

Step 4 Press Apply.

Set Up Phone To Not Use DHCP

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

Procedure

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

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

a) Set DHCP Enabled to No.

b) Enter the static IP address for phone.

c) Enter the subnet mask.

d) Enter the default router IP addresses.

e) Set Alternate TFTP Server to Yes, and enter the IP address for TFTP Server 1.

Step 3 Press Apply.

Phone Startup Process

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

1 The Feature and Sessions buttons flash amber and then green in sequence during the various stages of bootup as the phone checks the hardware.

2 The main screen displays Registering to Cisco Unified Communications Manager.

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

Related Topics

Startup Problems, on page 303
Configure Phone Services for Users

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

Before a user can access any service:

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

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

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

Procedure

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

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

See Self Care Portal Management, on page 99 for a summary of the information that you must provide to end users.
Cisco Unified Communications Manager Phone Setup

- Set Up Cisco Unified IP Phone, page 87
- Determine the Phone MAC Address, page 90
- Phone Addition Methods, page 91
- Add Users to Cisco Unified Communications Manager, page 92
- Add User to End User Group, page 94
- Associate Phones with Users, page 94
- Survivable Remote Site Telephony, page 95
- Set Up Cisco Unified Communications Manager Features, page 97

Set Up Cisco Unified IP Phone

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

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

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

Procedure

Step 1 Gather the following information about the phone:

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

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

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

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

Step 3 Customize phone button templates (if required) by changing the number of line buttons, speed-dial buttons or service URL buttons. Select Device > Device Settings > Phone Button Template to create and update the templates. You can add a Privacy, All Calls, or Mobility button to meet user needs.

For more information, see the "Phone button template setup" chapter in the Cisco Unified Communications Manager Administration Guide and Phone Button Templates, on page 234.

Step 4 Define the Device Pools. Select System > Device Pool. Device Pools define common characteristics for devices, such as region, date/time group, softkey template, and MLPP information. For information on Device Pool setup, see the "Device pool setup" chapter in the Cisco Unified Communications Manager Administration Guide.

Step 5 Define the Common Phone Profile. Select Device > Device settings > Common Phone Profile. Common phone profiles provide data that the Cisco TFTP server requires, as well as common phone settings, such as Do Not Disturb and feature control options. For more information, see the "Common phone profile setup" chapter in the Cisco Unified Communications Manager Administration Guide.

Step 6 Define a Calling Search Space. In Cisco Unified Communications Manager Administration, click Call Routing > Class of Control > Calling Search Space. A Calling Search Space is a collection of partitions that are searched to determine how a dialed number is routed. The calling search space for the device and the calling search space for the directory number are used together. The directory number CSS takes precedence over the device CSS. For more information, see the "Calling search space setup" chapter in the Cisco Unified Communications Manager Administration Guide.

Step 7 Configure a security profile for the device type and protocol. Select System > Security > Phone Security Profile. For more information, see the "Phone security profile setup" chapter in the Cisco Unified Communications Manager Security Guide.

Step 8 Add and configure the phone by completing the required fields in the Phone Configuration window. An asterisk (*) next to the field name indicates a required field; for example, MAC address and device pool. This step adds the device with the default settings to the Cisco Unified Communications Manager database.
For more information, see the "Cisco Unified IP Phone Configuration" chapter in the Cisco Unified Communications Manager Administration Guide.

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

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

**Step 9** Add and configure directory numbers (lines) on the phone by completing the required fields in the Directory Number Configuration window. An asterisk (*) next to the field name indicates a required field; for example, directory number and presence group. This step adds primary and secondary directory numbers and features associated with directory numbers to the phone.

For more information, see the "Directory Number Configuration" chapter in the Cisco Unified Communications Manager Administration Guide.

**Step 10** Configure speed-dial buttons and assign speed-dial numbers.

Users can change speed-dial settings on their phones by using Cisco Unified Communications Self Care Portal.

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

**Step 11** Configure Cisco Unified IP Phone services and assign services (optional) to provide IP Phone services.

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

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

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

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

**Step 12** Assign services to programmable buttons (optional) to provide access to an IP Phone service or URL.

For more information, see the "Adding a Service URL Button" section of the "Cisco Unified IP Phone Configuration" chapter in the Cisco Unified Communications Manager Administration Guide.

**Step 13** Add user information by configuring required fields. An asterisk (*) next to the field name indicates a required field; for example, User ID and last name. This step adds user information to the global directory for Cisco Unified Communications Manager.

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

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

Note: If your company uses a Lightweight Directory Access Protocol (LDAP) directory to store information about users, you can install and configure Cisco Unified Communications to use your existing LDAP directory.
If you want to add both the phone and user to the Cisco Unified Communications Manager database at the same time, see the "User/Phone Add Configurations" chapter in the *Cisco Unified Communications Manager Administration Guide*.

**Step 14** Associate a user to a user group. This step assigns users a common list of roles and permissions that apply to all users in a user group. Administrators can manage user groups, roles, and permissions to control the level of access (and, therefore, the level of security) for system users. For example, you must add users to the standard Cisco CCM End Users group so users can access Cisco Unified Communications Manager Self Care Portal.

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

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

**Step 15** Associate a user with a phone (optional). This step provides users with control over their phone such as forwarding calls or adding speed-dial numbers or services.

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

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

**Step 16** If you are not already in the End User Configuration window, choose User Management > End User to perform some final configuration tasks. Use the Search fields and Find to locate the user (for example, John Doe), then click on the user ID to get to the End User Configuration window for the user.

**Step 17** In the Directory Number Associations area of the screen, set the primary extension from the drop-down list.

**Step 18** In the Mobility Information area, check the Enable Mobility box.

**Step 19** In the Permissions Information area, use the User Group buttons to add this user to any user groups. For example, you may want to add the user to a group that is defined as a Standard CCM End User Group.

**Step 20** To view all configured user groups, choose User Management > User Group.

**Step 21** In the Extension Mobility area, check the Enable Extension Mobility Cross Cluster box if the user is allowed for Extension Mobility Cross Cluster service.

**Step 22** Select Save.

---

### Determine the Phone MAC Address

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

Adding phones either individually or using BAT requires you to identify the MAC address for the phone. For more information, see Determine the Phone MAC Address, on page 90.

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

Related Topics

Enable Autoregistration for Phones, on page 60

Add Phones Individually

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

Procedure

1. In Cisco Unified Communications Manager Administration, choose Device > Phone.
2. Click Add New.
3. Select the phone type.
4. Select Next.
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.
6. Select Save.

Add Phones Using BAT Phone Template

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

To add phones using BAT only (not in conjunction with TAPS), you must obtain the appropriate MAC address for each phone.
For more information about using BAT, see the documentation for your particular Cisco Unified Communications Manager release.

**Procedure**

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

**Step 2** Click **Add New**.

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

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

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

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

---

**Add Users to Cisco Unified Communications Manager**

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

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

**Procedure**

**Step 1** To add users individually, see Add User Directly to Cisco Unified Communications Manager, on page 93.

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

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

---

**Add a User from an External LDAP Directory**

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

- **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 User to End User Group

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

Procedure

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

Associate Phones with Users

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

Procedure

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

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

---

**Survivable Remote Site Telephony**

Survivable Remote Site Telephony (SRST) ensures that basic phone functions remain accessible when WAN connectivity is lost. 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.

**Note**

SRST does not support IPv6.


The following table describes the availability of features during failover.

**Table 14: SRST feature support**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Call</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>End Call</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Redial</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Answer</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Hold</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Resume</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Conference</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Conference to Active Calls (Join)</td>
<td>No</td>
<td>The Active Calls softkey does not display.</td>
</tr>
<tr>
<td>Conference List</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Transfer</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Transfer to Active Calls (Direct Transfer)</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Supported</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Auto Answer</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Call Waiting</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Caller ID</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Audible Message Waiting Indicator</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>All Calls Programmable Line Key</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Answer Programmable Line Key</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Unified Session Presentation</td>
<td>Yes</td>
<td>Conference is the only feature supported due to other feature limitations.</td>
</tr>
<tr>
<td>Voicemail</td>
<td>Yes</td>
<td>Voicemail will not be synchronized with other users in the Cisco Unified Communications Manager cluster.</td>
</tr>
<tr>
<td>Call Forward All</td>
<td>Yes</td>
<td>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.</td>
</tr>
<tr>
<td>Speed Dial</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Service IRL Programmable Line Key</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>To Voicemail (iDivert)</td>
<td>No</td>
<td>The iDivert softkey does not display.</td>
</tr>
<tr>
<td>Line Filters</td>
<td>Partial</td>
<td>Lines are supported but cannot be shared.</td>
</tr>
<tr>
<td>Park Monitoring</td>
<td>No</td>
<td>The Park softkey does not display.</td>
</tr>
<tr>
<td>Barge</td>
<td>No</td>
<td>User sees the message That feature is not currently available.</td>
</tr>
<tr>
<td>Feature</td>
<td>Supported</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Directed Call Park</td>
<td>No</td>
<td>The softkey does not display.</td>
</tr>
<tr>
<td>BLF</td>
<td>Partial</td>
<td>BLF feature key works like Speed Dial keys.</td>
</tr>
<tr>
<td>Hold Reversion</td>
<td>No</td>
<td>Calls remain on hold indefinitely.</td>
</tr>
<tr>
<td>Remote Hold</td>
<td>No</td>
<td>Calls appear as Local Hold calls.</td>
</tr>
<tr>
<td>Meet Me</td>
<td>No</td>
<td>The Meet Me softkey does not display.</td>
</tr>
<tr>
<td>PickUp</td>
<td>No</td>
<td>The softkey causes no action.</td>
</tr>
<tr>
<td>Group PickUp</td>
<td>No</td>
<td>The softkey causes no action.</td>
</tr>
<tr>
<td>Other PickUp</td>
<td>No</td>
<td>The softkey causes no action.</td>
</tr>
<tr>
<td>Malicious Call ID</td>
<td>No</td>
<td>The softkey causes no action.</td>
</tr>
<tr>
<td>QRT</td>
<td>No</td>
<td>The softkey causes no action.</td>
</tr>
<tr>
<td>Hunt Group</td>
<td>No</td>
<td>The softkey causes no action.</td>
</tr>
<tr>
<td>Intercom</td>
<td>No</td>
<td>The softkey causes no action.</td>
</tr>
<tr>
<td>Mobility</td>
<td>No</td>
<td>The softkey causes no action.</td>
</tr>
<tr>
<td>Privacy</td>
<td>No</td>
<td>The softkey causes no action.</td>
</tr>
<tr>
<td>Call Back</td>
<td>No</td>
<td>The Call Back softkey does not display.</td>
</tr>
<tr>
<td>Video</td>
<td>Yes</td>
<td>Video conference is not supported.</td>
</tr>
<tr>
<td>Shared Line</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>BLF Speed Dial</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**Set Up Cisco Unified Communications Manager Features**

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

**Procedure**

**Step 1** In Cisco Unified Communications Manager Administration, choose one of the following windows:
• Device > Phone (Phone Configuration window) Product Specific Configuration portion of window

• Device > Device Settings > Common Phone Profile (Common Phone Profile Configuration window)

• System > Enterprise Phone Configuration (Enterprise Phone Configuration window)

Step 2  Click the ? button in Cisco Unified Communications Manager Administration for descriptions of the parameters.

Step 3  When you set the parameters, check the Override Common Settings check box for each setting that you wish to update.
If you do not check this box, the corresponding parameter setting does not take effect.

If you set the parameters in the three configuration windows, the setting takes precedence in the following order:

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

Related Topics

Set Up Cisco Unified Video Camera, on page 121
CHAPTER 6

Self Care Portal Management

- Self Care Portal Overview, page 99
- Set Up User Access to the Self Care Portal, page 99
- Customize the Self Care Portal Display, page 100

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:
  http://<server_name:portnumber>/ucmuser/, where server_name is the host on which the web server is installed and portnumber is the port number on that host.
- A user ID and default password to access the application.
- An overview of the tasks that users can accomplish with the portal.

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

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

Set Up User Access to the Self Care Portal

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

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

**Step 2** Search for the user.

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

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

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

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

---

**Customize the Self Care Portal Display**

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

- Show Ring Settings
- Show Line Label Settings

**Note**

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

---

**Procedure**

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

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

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

**Step 4** Select **Save**.
PART III

Hardware and Accessory Installation

- Cisco Unified IP Phone Accessories, page 103
- Cisco Unified IP Color Key Expansion Modules, page 113
- Cisco Unified Video Camera Installation, page 121
- Wall Mounts, page 125
## Cisco Unified IP Phone Accessories

- Accessory Support, page 103
- Connect Footstand, page 104
- Secure the Phone with a Cable Lock, page 105
- External Speakers and Microphone, page 106
- Headsets, page 106

### Accessory Support

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

**Table 15: Accessory Support for the Cisco Unified IP Phone 8961, 9951, and 9971**

<table>
<thead>
<tr>
<th>Accessory</th>
<th>Type</th>
<th>Cisco Unified IP Phone 8961</th>
<th>Cisco Unified IP Phone 9951</th>
<th>Cisco Unified IP Phone 9971</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Accessory</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Unified IP Color Key Expansion Module: See Cisco Unified IP Color Key Expansion Modules, on page 113.</td>
<td>Add-on module</td>
<td>1</td>
<td>Up to 2</td>
<td>Up to 3</td>
</tr>
<tr>
<td>Cisco Unified Video Camera: See Cisco Unified Video Camera Installation, on page 121.</td>
<td>Add-on module</td>
<td>-</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

**Third-Party accessories**
<table>
<thead>
<tr>
<th>Accessory</th>
<th>Type</th>
<th>Cisco Unified IP Phone 8961</th>
<th>Cisco Unified IP Phone 9951</th>
<th>Cisco Unified IP Phone 9971</th>
</tr>
</thead>
<tbody>
<tr>
<td>Headsets: See Headsets, on page 106. This section includes information about each headset type.</td>
<td>Analog</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Analog Wideband</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Bluetooth</td>
<td>-</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>USB (wired or wireless)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Microphone: See External Speakers and Microphone, on page 106.</td>
<td>External PC</td>
<td>-</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Speakers: See External Speakers and Microphone, on page 106.</td>
<td>External PC</td>
<td>-</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

### Connect Footstand

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

Step 1  Insert the curved connectors into the lower slots.
Step 2  Lift the footstand until the connectors snap into the upper slots.

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

Secure the Phone with a Cable Lock

You can secure your phone with a laptop cable lock up to 20 mm wide.
Procedure

Step 1  Take the looped end of the cable lock and wrap it around the object to which you want to secure your phone.
Step 2  Pass the lock through the looped end of the cable.
Step 3  Unlock the cable lock.
Step 4  Press and hold the locking button to align the locking teeth.
Step 5  Insert the cable lock into the lock slot of your phone and release the locking button.
Step 6  Lock the cable lock.

External Speakers and Microphone

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

Note

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

Headsets

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

Headsets connect to your phone using either the USB or the auxiliary port. Depending upon your headset model, you have to adjust your phone's audio settings for the best audio experience, including the headset sidetone setting.

After you apply a new sidetone setting, wait one minute and then reboot the phone for the setting to be stored in flash.

The phone reduces some background noise that a headset microphone detects. You can use a noise canceling headset to further reduce the background noise and improve the overall audio quality.

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

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

We recommend that customers test headsets in the intended environment to determine performance before making a purchasing decision to deploy on a large scale.

Audio Quality

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

For additional information, see http://www.cisco.com/c/en/us/products/unified-communications/uc_endpoints_accessories.html

Analog Headsets

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

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

Enable Wideband on Analog Headsets

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

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

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

Procedure

| Step 1 | On the Cisco IP Phone, press Applications. |
| Step 2 | Select Accessories. |
| Step 3 | Highlight the analog headset, then press Setup. |
| Step 4 | Press On to turn on the wideband. Press Off to turn off the wideband. |
Enable the Wideband for Analog Headsets

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

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

If the screen doesn't display an On or Off softkey, follow these steps to ensure that you can enable wideband on an analog headset:

**Procedure**

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

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

**Step 3** Click the Device Name that you want. The Phone Configuration window is displayed.

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

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

**Step 6** Click Save.

Wired Headsets

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

**Connect Wired Headset**

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

**Procedure**

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

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

**Disable a Wired Headset**

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

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

**Step 2**
In the Find and List Phones window, enter the search criteria for the phone and click **Find**.

**Step 3**
Click the Device Name that you want. The Phone Configuration window is displayed.

**Step 4**
In the Product Specific Configuration Layout portion of the Phone Configuration window, select **Disable Speakerphone and Headset**.

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

### USB Headsets

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

#### Enable USB Headset

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

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

### Procedure

**Step 1**
Enable the USB headset in one of the following windows:

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

**Step 2**
Check the corresponding Override Common Settings parameter in the configuration window.

#### Disable a USB Headset

To disable the USB headset, disable the USB port that you enabled in Cisco Unified Communications Manager Administration. Also, you can select another type of headset in the Accessories window on the phone, thus disabling the previously enabled headset.
**Procedure**

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

**Step 2** Locate the phone you want to modify, and go to the Phone Configuration window for that phone.

**Step 3** In the Phone Configuration window, uncheck **Override Common Settings**.

**Step 4** Save your changes.

---

**Wireless Headsets**

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

The Cisco website provides information about wireless headsets that work with your IP phone. Go to the following URL:


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

---

**Bluetooth Wireless Headsets**

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

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

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

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

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

The Bluetooth icon 📡 indicates whether a device is connected.

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

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

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

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

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

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

- Answer a call
- End a call
- Change the headset volume for a call
- Redial
- Caller ID
- Reject
- Divert
- Hold and Accept
- Release and Accept

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

**Important**

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

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

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

**Enable a Bluetooth Wireless Headset**

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

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

Remove a Bluetooth Device from the Phone

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

Procedure

Step 1  Press Applications.
Step 2  Select Accessories.
Step 3  Highlight the device that you want to remove and press Delete.
Cisco Unified IP Color Key Expansion Modules

- Cisco Unified IP Color KEM Setup Overview, page 113
- KEM Power Information, page 114
- Connect Single KEM to Cisco Unified IP Phone, page 114
- Connect Two or More KEMs to Phone Using KEM Spine Connector, page 115
- Set Up Key Expansion Module in Cisco Unified Communications Manager Administration, page 116
- Access Key Expansion Module setup, page 117
- Upgrade Key Expansion Module, page 118
- Remove All Key Expansion Modules, page 118
- Troubleshoot the Key Expansion Module, page 118

Cisco Unified IP Color KEM Setup Overview

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

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

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

For information about installing a wall mount kit for a phone that includes a Cisco Unified IP Color Key Expansion Module, see related links.
Table 16: Cisco Unified IP Phones and Supported KEMs

<table>
<thead>
<tr>
<th>Cisco Unified IP Phone model</th>
<th>Supported KEMs</th>
</tr>
</thead>
<tbody>
<tr>
<td>9971</td>
<td>3 KEMs with 108 lines or buttons</td>
</tr>
<tr>
<td>9951</td>
<td>2 KEMs with 72 lines or buttons</td>
</tr>
<tr>
<td>8961</td>
<td>1 KEM with 36 lines or buttons</td>
</tr>
</tbody>
</table>

Related Topics
Wall Mounts, on page 125

KEM Power Information

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

**Power consumption**

48V DC, 5W per KEM

**Power scheme**

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

Connect Single KEM to Cisco Unified IP Phone

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

Step 1  Position the phone so that the front of the phone is facing up.
Step 2  Connect one end of the KEM spine connector to the accessory connector on the Cisco Unified IP Phone.
Step 3  Connect the other end of the KEM spine connector to the KEM as shown in the following figure.

Figure 3: Connecting the KEM Spine Connector to the Cisco Unified IP Phone and KEM

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

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

Connect Two or More KEMs to Phone Using KEM Spine Connector

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

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

**Step 2** Connect one end of the KEM spine connector to the accessory connector on the Cisco Unified IP Phone and the other end of the spine connector to a KEM, as seen in Connect Single KEM to Cisco Unified IP Phone, on page 114. The first KEM is now connected to the Cisco Unified IP Phone.

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

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

*Figure 4: Cisco Unified IP Phone with Three KEMs Attached*

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

---

**Set Up Key Expansion Module in Cisco Unified Communications Manager Administration**

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

**Procedure**

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

**Step 2** Select and enter your search criteria and click **Find**. The Find and List Phones window appears with a list of phones that match your search criteria.
Step 3  Click the IP phone that you want to configure for the Cisco Unified IP Color Key Expansion Module. The Phone Configuration window appears.

Step 4  Scroll down to the Expansion Module Information section on the right pane of the Phone Configuration window, and choose the appropriate expansion module (or "none") for the Module 1, Module 2 and Module 3 fields, in that order.

For the Module Load Name, enter the custom software for the appropriate expansion module, if applicable.
The value that you enter overrides the default value for the current model. Ensure that the firmware load matches the module load. If the Module Load Name is left blank, the default load (the load bundled with the phone load) is installed.

For the number of supported KEMs per phone model, see Cisco Unified IP Color KEM Setup Overview, on page 113.

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

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

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

Step 7  Click Save.

---

### Access Key Expansion Module setup

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

When multiple KEMs are attached, they are numbered according to the order in which they connect to the phone. For example (see Connect Two or More KEMs to Phone Using KEM Spine Connector, on page 115):

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

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

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

### Procedure

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

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

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Power on the KEM, press <strong>Page 1</strong>, and do not release the key. When the LCD turns white, continue pressing <strong>Page 1</strong> for at least one second.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Release <strong>Page 1</strong>; LEDs should turn red. Immediately press <strong>Page 2</strong> and continue pressing <strong>Page 2</strong> for at least one second.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Release <strong>Page 2</strong>; all LEDs should turn amber.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Press Lines 5, 14, 1, 18, 10, and 9 in sequence. The LCD should turn blue, and the spinning loader icon displays in the center. The KEM starts to upgrade.</td>
</tr>
</tbody>
</table>

Remove All Key Expansion Modules

If you are removing one or more KEMs but still leaving one or more KEMs attached to the phone, see Connect Single KEM to Cisco Unified IP Phone, on page 114 or Connect Two or More KEMs to Phone Using KEM Spine Connector, on page 115 for instructions on how to connect the KEMs and phone based on how many KEMs remain. Also, go to Cisco Unified Communications Manager Administration and update the phone configuration file accordingly.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Detach all existing KEMs from the phone.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In Cisco Unified Communications Manager Administration, update the phone configuration file accordingly.</td>
</tr>
</tbody>
</table>

Troubleshoot the Key Expansion Module

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Open a CLI.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Enter the following command to enter debug mode: <code>debugsh</code></td>
</tr>
</tbody>
</table>
Step 3  Enter ? to see all available commands and options.
Step 4  Use the applicable commands and options to find the desired KEM information.
Step 5  To exit debug mode, press Ctrl-C.
Troubleshoot the Key Expansion Module
Cisco Unified Video Camera Installation

- Cisco Unified Video Camera Overview, page 121
- Set Up Cisco Unified Video Camera, page 121
- Perform Camera Postinstallation Checks, page 122
- Camera Settings, page 122

Cisco Unified Video Camera Overview

The Cisco Unified IP Phone 9951 and 9971 supports the add-on Cisco Unified Video Camera accessory. The Cisco Unified Video Camera connects to your Cisco Unified IP Phone and allows you to make a point-to-point video call with another Cisco Unified IP Phone with a Cisco Unified Video Camera attached. If a Cisco Unified Video Camera is not attached to the phone, the phone can only receive one-way video.

Note

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

Set Up Cisco Unified Video Camera

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

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

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

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

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

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

**Step 3** Click **Save**.

**Related Topics**

Set Up Cisco Unified Communications Manager Features, on page 97

**Perform Camera Postinstallation Checks**

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

**Procedure**

**Step 1** Wait until the *camera ready* message appears.

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

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

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

**Note** For information about adjusting camera settings on the phone, see the *Cisco Unified Video Camera Quick Start Guide* at this location: [http://www.cisco.com/en/US/products/ps10655/products_user_guide_list.html](http://www.cisco.com/en/US/products/ps10655/products_user_guide_list.html)

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

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

**Camera Settings**

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

**Adjust View Area Setting**

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

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

**Adjust Brightness Setting**

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

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

To adjust the Brightness setting, follow these steps:

**Procedure**

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

**Adjust Auto Transmit Setting**

The Auto Transmit setting allows you to control the streaming of videos for both inbound and outbound calls. When Auto Transmit is on (default setting), the camera streams video automatically during calls. When Auto Transmit is off, video for each call is automatically muted (however, your phone still receives video). To resume video transmission in this case, press the **Unmute Video** softkey. To turn the Auto Transmit setting on or off, follow these steps:
Procedure

Step 1  On the Cisco Unified IP Phone, press Applications.
Step 2  Select Accessories.
Step 3  Highlight Cisco Unified Camera.
Step 4  Press Setup.
Step 5  Move the Auto Transmit slider bar to On or Off.
CHAPTER 10

Wall Mounts

- Wall Mount Options, page 125
- Lockable Wall Mount Components for Phone, page 126
- Lockable Wall Mount Components for Phone with Key Expansion Module, page 131
- Non-Lockable Wall Mount Components for Phone, page 136
- Non-Lockable Wall Mount Components for Phone with Key Expansion Module, page 145
- Adjust the Handset Rest, page 154

Wall Mount Options

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

The following wall mount options are available:

- Cisco Unified IP Phone 8961, 9951, and 9971 Wall Mount Kit: A lockable wall mount kit for the Cisco Unified IP Phone 8961, 9951, and 9971.

- Cisco Unified IP Phone 8961, 9951, and 9971 Wall Mount Kit for Phone with Key Expansion module: A lockable wall mount kit for the Cisco Unified IP Phone 8961, 9951, and 9971 with one Key Expansion Module.

- ADA Non-Lockable Wall Mount Kit for 8961 Series and 9900 Series IP Phones: Installed on the Cisco Unified IP Phone 8961, 9951, and 9971.

- ADA Non-Lockable Wall Mount Kit for 8961 Series and 9900 Series IP Phones plus a single Key Expansion Module: Installed on the Cisco Unified IP Phone 8961, 9951, and 9971 with one Key Expansion Module.
Lockable Wall Mount Components for Phone

This section describes how to install a wall mount for the Cisco Unified IP Phone 8961, 9951, and 9971.

Figure 5: Wall Mount Kit for Single Phone Assembly

The package includes these items:

- One phone bracket
- One wall bracket
- Four #10-12x1-inch Phillips-head screws with 4 anchors
- One sheet metal screw (not shown)
- Two #4-40x1/4-inch machine screws
- One 6-inch Ethernet cable
- One key if the bracket includes the optional lock

Install Bracket

Before You Begin

You need these tools to install the bracket:

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

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

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

a) Use the level to ensure that the bracket is level, then use a pencil to mark the screw holes.

b) Using a #2 Phillips-head screwdriver, carefully center the anchor over the pencil mark and press the anchor into the wall.

c) Screw the anchor clockwise into the wall until it is seated flush.
d) Use the included screws and a #2 Phillips-head screwdriver to attach the bracket to the wall.

Figure 6: Mount Wall Bracket

Step 2  Attach the phone bracket to the IP Phone.
   a) Detach the handset cord (and headset cord, if there is a headset), power cord, and any other attached cords from the base of the phone.
   b) Remove the label covers that conceal the screw holes.
   c) Attach the phone bracket by inserting the tabs into the mounting tabs on the phone. The phone ports should be accessible through the holes in the bracket.
d) Secure the phone bracket to the IP phone with the machine screws.
e) Thread the handset cord (and headset cord, if using one). Reattach the cords and seat them in the clips that are incorporated into the phone body.

**Figure 7: Attach Phone Bracket**

Step 3  Attach the Ethernet cable to the 10/100/1000 SW network port and wall jack. If you are connecting a network device (such as a computer) to the phone, attach the cable to the 10/100/1000 Computer (PC access) port.
If you are using an external power supply, plug the power cord into the phone and dress the cord by clipping it into the clips that are incorporated into the phone body next to the PC port.

**Figure 8: Attach Cables**

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

Figure 9: Attach Phone to Wall Bracket

Step 5  Use the locking key to lock the phone to the wall bracket.
Step 6  Proceed to Adjust the Handset Rest, on page 154.

Lockable Wall Mount Components for Phone with Key Expansion Module

This section describes how to install a wall mount for the Cisco Unified IP Phone 8961, 9951, and 9971 that connects to the Key Expansion Module.

Figure 10: Wall Mount Kit for Phone with Key Expansion Module
The package includes these items:

- One phone bracket
- One wall bracket
- Four #10-12x1-inch Phillips-head screws with 4 anchors
- One sheet metal screw
- Three #4-40x1/4-inch machine screws
- One 6-inch Ethernet cable
- One key if the bracket includes the optional lock

### Install Bracket for Phone with KEM

**Note**

Be sure to connect to connect the Cisco Unified IP Phone to the Key Expansion Module before installing the phone bracket.

**Before You Begin**

You need these tools to install the bracket:

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

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

**Procedure**

**Step 1**

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

a) Use a level to ensure the bracket is level, then use a pencil to mark the screw holes.

b) Using a #2 Phillips-head screwdriver, carefully center the anchor over the pencil mark and press the anchor into the wall.

c) Screw the anchor clockwise into the wall until it is seated flush.
d) Use the included screws and a #2 Phillips-head screwdriver to attach the bracket to the wall.

*Figure 11: Mount Wall Bracket*

**Step 2**  
Attach the phone bracket to the IP phone and key expansion assembly.

a) Detach the handset cord (and headset cord, if there is a headset), power cord, and any other attached cords from the base of the phone.

b) Remove the label covers that are conceal the screw holes.
c) Attach the phone bracket by inserting the tabs into the mounting tabs on the phone. The phone ports should be accessible through the holes in the bracket.
d) Secure the phone bracket to the IP phone with the machine screws.
e) Thread the handset cord (and headset cord, if using one). Reattach the cords and seat them in the clips that are incorporated into the phone body.

Figure 12: Attach Phone Bracket

Step 3 Attach the Ethernet cable to the 10/100/1000 SW network port and wall jack. If you are connecting a network device (such as a computer) to the phone, attach the cable to the 10/100/1000 Computer (PC access) port.
If you are using an external power supply, plug the power cord into the phone and dress the cord by clipping it into the clips that are incorporated into the phone body next to the PC port.

*Figure 13: Attach Cables*

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

*Figure 14: Attach Phone to Wall Bracket*

**Step 5** Use the locking key to lock the phone to the wall bracket.

**Step 6** Proceed to *Adjust the Handset Rest, on page 154*

---

**Non-Lockable Wall Mount Components for Phone**

This section describes how to install the ADA Non-Lockable Wall Mount Kit for 8961 Series and 9900 Series IP Phones on a Cisco Unified IP Phone 8961, 9951, and 9971 when the phone is not connected to a Key Expansion Module.
The following figure shows the wall mount kit installed on the phone.

*Figure 15: Back View of ADA Non-Lockable Wall Mount Kit Installed on Phone*

![Back View of ADA Non-Lockable Wall Mount Kit Installed on Phone](image)

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

*Figure 16: Side View of ADA Non-Lockable Wall Mount Kit Installed on Phone*

![Side View of ADA Non-Lockable Wall Mount Kit Installed on Phone](image)
The following figure shows the components of the ADA Non-Lockable Wall Mount Kit for 8961 Series and 9900 Series IP Phones.

**Figure 17: Components**

The package contains the following items:
- One phone bracket
- One wall bracket
- Four #8-18 x 1.25-inch Phillips-head screws with four anchors
- Two #4-40 x 0.31-inch machine screws
- One 6-inch Ethernet cable

**Install Non-Lockable Wall Mount Kit for Phone**

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

**Before You Begin**

You need these tools to install the bracket:
- #1 and #2 Phillips-head screwdrivers
- Level
- Pencil

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

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

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

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

*Figure 18: Bracket Installation*

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

a) Detach the handset cord (and headset cord, if there is a headset), power cord, and any other attached cords from the base of the phone.

b) Remove the label covers that conceal the screw holes.

c) Attach the phone bracket by inserting the tabs into the mounting tabs on the back of the phone. The phone ports should be accessible through the holes in the bracket.

d) Secure the phone bracket to the IP phone with the machine screws, using the #1 Phillips-head screwdriver.

e) Thread the handset cord (and headset cord, if using one). Reattach the cords and seat them in the clips that are incorporated into the phone body.
The following figure shows how the bracket attaches to the phone.

*Figure 19: Attach Phone Bracket*

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

a) Attach the Ethernet cable to the 10/100/1000 SW network port and wall jack.

b) (Optional) If you are connecting a network device (such as a computer) to the phone, attach the cable to the 10/100/1000 Computer (PC access) port.

c) (Optional) If you are using an external power supply, plug the power cord into the phone and dress the cord by clipping it into the clips that are incorporated into the phone body next to the PC port.

d) (Optional) If the cables terminate inside the wall bracket, connect the cables to the jacks.
The following figure shows the cables.

*Figure 20: Attach Cables*

![Cable Diagram]

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

*Figure 21: Attach Phone to Wall Bracket*

**Step 5** Press the phone firmly into the wall bracket and slide the phone down. The tabs in the bracket click into position.

**Step 6** Proceed to Adjust the Handset Rest, on page 154.
Remove Phone from Non-Lockable Wall Mount

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

*Figure 22: Tab Location*

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

**Before You Begin**

You require 2 screwdrivers or metal rods.
Procedure

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

Figure 23: Disengage Tabs

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

Non-Lockable Wall Mount Components for Phone with Key Expansion Module

This section describes how to install the ADA Non-Lockable Wall Mount Kit for 8961 Series and 9900 Series IP Phones with Key Expansion Module on a Cisco Unified IP Phone 8961, 9951, and 9971 when the phone is connected to a Key Expansion Module.
The following figures show the wall mount kit installed on the phone.

*Figure 24: Back View of ADA Non-Lockable Wall Mount Kit Installed on Phone with Key Expansion Module*

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

*Figure 25: Side View of ADA Non-Lockable Wall Mount Kit Installed on Phone with Key Expansion Module*
The following figure shows the components of the ADA Non-Lockable Wall Mount Kit for the Cisco Unified IP Phone 8961, 9951, and 9971 with a Key Expansion Module.

**Figure 26: Components**

The package contains the following items:

- One phone bracket
- One wall bracket
- Six #8-18 x 1.25-inch Phillips-head screws with six anchors
- Three #4-40 x 0.31-inch machine screws
- One 6-inch Ethernet cable

**Install Non-Lockable Wall Mount Kit for Phone with Key Expansion Module**

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

**Before You Begin**

You need these tools to install the bracket:

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

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

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

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

a) Hold the bracket on the wall. See the following figure for the orientation of the wall bracket.
b) Use the level to ensure that the bracket is level and use a pencil to mark the screw holes.
c) Using a #2 Phillips-head screwdriver, carefully center the anchor over the pencil mark and press the anchor into the wall.
d) Screw the anchor clockwise into the wall until it is seated flush.
e) Use the included screws and a #2 Phillips-head screwdriver to attach the bracket to the wall.
The following figure shows the steps for installing the bracket.

**Figure 27: Bracket Installation**

![Bracket Installation Diagram]

**Step 2** Attach the phone bracket to the IP phone and key expansion assembly.

a) Detach the handset cord (and headset cord, if there is a headset), power cord, and any other attached cords from the base of the phone.

b) Remove the label covers that are conceal the screw holes.

c) Attach the phone bracket by inserting the tabs into the mounting tabs on the back of the phone. The phone ports should be accessible through the holes in the bracket.

d) Secure the phone bracket to the IP phone with the machine screws using a #1 Philips-head screwdriver.

e) Thread the handset cord (and headset cord, if using one). Reattach the cords and seat them in the clips that are incorporated into the phone body. The headset and handset connectors should be accessible from outside the wall mount bracket.
The following figure shows the steps to attach the phone bracket.

**Figure 28: Attach Phone Bracket**

![Diagram of phone bracket with labeled screw holes and slot for mounting tabs.]

**Step 3** Attach the cords.

a) Attach the Ethernet cable to the 10/100/1000 SW network port and wall jack.

b) (Optional) If you are connecting a network device (such as a computer) to the phone, attach the cable to the 10/100/1000 Computer (PC access) port.

c) (Optional) If you are using an external power supply, plug the power cord into the phone and dress the cord by clipping it into the clips that are incorporated into the phone body next to the PC port.

d) (Optional) If the cables terminate inside the wall bracket, connect the cables to the jacks.
The following figure shows the cables.

**Figure 29: Attach Cables**

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

*Figure 30: Attach Phone to Wall Bracket*

**Step 5** Proceed to Adjust the Handset Rest, on page 154.
Remove Phone and Key Expansion Module from Non-Lockable Wall Mount

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

*Figure 31: Tab Location*

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

**Before You Begin**

You require two screwdrivers or metal rods.
Procedure

**Step 1** Push the screwdrivers into the left and right holes in the phone mounting plate until you feel resistance.

**Step 2** Press firmly inwards (towards the phone) to disengage the tabs, lift up on the phone to release the phone from the wall bracket, and then pull the phone towards you.

*Figure 32: Disengage Tabs*

---

**Adjust the Handset Rest**

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

**Step 1** Remove the handset from the cradle and pull the plastic tab from the handset rest.

**Step 2** Rotate the tab 180 degrees.

**Step 3** Hold the tab between two fingers, with the corner notches facing you.

**Step 4** Line up the tab with the slot in the cradle and press the tab evenly into the slot. An extension protrudes from the top of the rotated tab.

**Step 5** Return the handset to the handset rest.
Adjust the Handset Rest
Part IV

Cisco Unified IP Phone Administration

- Cisco Unified IP Phone Security, page 159
- Cisco Unified IP Phone Customization, page 175
- Phone Features and Setup, page 181
- Corporate and Personal Directory Setup, page 249
- Cisco VXC VPN, page 253
CHAPTER 11

Cisco Unified IP Phone Security

- View Current Security Features on Phone, page 159
- View Security Profiles, page 159
- Supported Security Features, page 160

View Current Security Features on Phone

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

Procedure

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

View Security Profiles

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

Procedure

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

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

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

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

Note

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

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

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

A Locally Significant Certificate (LSC) installs on phones after you perform the necessary tasks that are associated with the Certificate Authority Proxy Function (CAPF). You can use Cisco Unified Communications Manager Administration to configure an LSC, as described in the Cisco Unified Communications Manager Security Guide. Alternatively, you can initiate the installation of an LSC from the Security Setup menu on the phone. This menu also lets you update or remove an LSC.

The Cisco Unified IP Phone 8961, 9951, and 9971 uses the phone security profile, which defines whether the device is nonsecure or secure. For information about applying the security profile to the phone, see the Cisco Unified Communications Manager Security Guide.

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

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

For information about current security settings on a phone, press and choose Administrator Settings > Security Setup.
## Table 17: Overview of Security Features

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

- **CAPF (Certificate Authority Proxy Function)**
  Implements parts of the certificate generation procedure that are too processing-intensive for the phone, and interacts with the phone for key generation and certificate installation. The CAPF can be configured to request certificates from customer-specified certificate authorities on behalf of the phone, or it can be configured to generate certificates locally.

- **Security profile**
  Defines whether the phone is nonsecure, authenticated, encrypted, or protected. Other entries in this table describe security features. For more information about these features, about Cisco Unified Communications Manager, and about Cisco Unified IP Phone security, see the *Cisco Unified Communications Manager Security Guide*.

- **Encrypted configuration files**
  Lets you ensure the privacy of phone configuration files.

- **Optional web server disabling for a phone**
  For security purposes, you can prevent access to the web pages for a phone (which display a variety of operational statistics for the phone) and User Options web pages. For more information, see Control Phone Web Page Access, on page 237.

- **Phone hardening**
  Additional security options, which you control from Cisco Unified Communications Manager Administration:
  - Disabling PC port
  - Disabling Gratuitous ARP (GARP)
  - Disabling PC Voice VLAN access
  - Disabling access to the Setting menus, or providing restricted access that allows access to the Preferences menu and saving volume changes only
  - Disabling access to web pages for a phone
  - Disabling Bluetooth Accessory Port

- **802.1X Authentication**
  The Cisco Unified IP Phone can use 802.1X authentication to request and gain access to the network. See 802.1X Authentication, on page 171 for more information.

- **Secure SIP Failover for SRST**
  After you configure a Survivable Remote Site Telephony (SRST) reference for security and then reset the dependent devices in Cisco Unified Communications Manager Administration, the TFTP server adds the SRST certificate to the phone cnf.xml file and sends the file to the phone. A secure phone then uses a TLS connection to interact with the SRST-enabled router.

- **Signaling encryption**
  Ensures that all SIP signaling messages that are sent between the device and the Cisco Unified Communications Manager server are encrypted.

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

The following table describes the options in the Security Setup menu.
Table 18: Security Setup Menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Mode</td>
<td>Displays the security mode that is set for the phone.</td>
<td>From Cisco Unified Communications Manager Administration, choose Device &gt; Phone. The setting appears in the Protocol Specific Information portion of the Phone Configuration window.</td>
</tr>
<tr>
<td>LSC</td>
<td>Indicates whether a locally significant certificate that is used for security features is installed on the phone (Yes) or is not installed on the phone (No).</td>
<td>For information about how to manage the LSC for your phone, see the &quot;Using the Certificate Authority Proxy Function&quot; chapter in the Cisco Unified Communications Manager Security Guide.</td>
</tr>
</tbody>
</table>
| Trust List     | The Trust List provides submenus for the CTL, ITL, and Signed Configuration files. The CTL File submenu displays the contents of the CTL file. The ITL File submenu displays the contents of the ITL file. The Trust List menu also displays the following information:  
  • CTL Signature: the SHA1 hash of the CTL file  
  • Unified CM/TFTPServer: the name of the Cisco Unified Communications Manager and TFTPServer that the phone uses. Displays a certificate icon if a certificate is installed for this server.  
  • CAPF Server: the name of the CAPF server that the phone uses. Displays a certificate icon if a certificate is installed for this server.  
  • SRST Router: the IP address of the trusted SRST router that the phone can use. Displays a certificate icon if a certificate is installed for this server. | For more information, see Set Up Locally Significant Certificate, on page 164. |
| 802.1X Authentication | Allows you to enable 802.1X authentication for this phone. | See 802.1X Authentication, on page 171. |

Supported TLS and Ciphers

TLS v1.0

Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Set Up Locally Significant Certificate

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.


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.

Phone Call Security

When security is implemented for a phone, you can identify secure phone calls by icons on the phone screen. You can also determine whether the connected phone is secure and protected if a security tone plays at the beginning of the call.
In a secure call, all call signaling and media streams are encrypted. A secure call offers a high level of security, providing integrity and privacy to the call. When a call in progress is encrypted, the call progress icon to the right of the call duration timer in the phone screen changes to the following icon: 🗝.

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

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

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

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

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

**Secure Conference Call Identification**

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

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

**Note**
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 19: Security Restrictions with Conference Calls**

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

**Secure Phone Call Identification**

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

A secured call is established using this process:

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

2. The phone displays the secure icon 🛡️ on the phone screen. This icon indicates that the phone is configured for secure calls, but this does not mean that the other connected phone is also secured.

3. The user hears a security tone if the call connects to another secured phone, indicating that both ends of the conversation are encrypted and secured. If the call connects to a nonsecure phone, the user does not hear the security tone.

**Note**

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

Only protected phones play these secure or nonsecure indication tones. Nonprotected phones never play tones. If the overall call status changes during the call, the indication tone changes and the protected phone plays the appropriate tone.
A protected phone plays a tone or not under these circumstances:

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

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

---

**Note**

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

---

**Provide Encryption for Barge**

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

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

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

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

---

**WLAN Security**

Because all WLAN devices that are within range can receive all other WLAN traffic, securing voice communications is critical in WLANs. To ensure that intruders do not manipulate or intercept voice traffic, the Cisco SAFE Security architecture supports the Cisco Unified IP Phone and Cisco Aironet APs. For more information about security in networks, see [http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html](http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html).

The Cisco Wireless IP telephony solution provides wireless network security that prevents unauthorized sign-ins and compromised communications by using the following authentication methods that the wireless Cisco Unified IP Phone 9971 supports:

- **Open Authentication**: Any wireless device can request authentication in an open system. The AP that receives the request may grant authentication to any requestor or only to requestors that are found on a list of users. Communication between the wireless device and AP could be nonencrypted or devices can use Wired Equivalent Privacy (WEP) keys to provide security. Devices that use WEP only attempt to authenticate with an AP that is using WEP.

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

Shared key authentication can be less secure than open authentication with WEP because someone can monitor the challenges. An intruder can calculate the WEP key by comparing the unencrypted and encrypted challenge text strings.

- **Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)**
  
  Authentication: This client server security architecture encrypts EAP transactions within a Transport Level Security (TLS) tunnel between the AP and the RADIUS server, such as the Cisco Access Control Server (ACS).

  The TLS tunnel uses Protected Access Credentials (PACs) for authentication between the client (phone) and the RADIUS server. The server sends an Authority ID (AID) to the client (phone), which in turn selects the appropriate PAC. The client (phone) returns a PAC-Opaque to the RADIUS server. The server decrypts the PAC with the master key. Both endpoints now contain the PAC key and a TLS tunnel is created. EAP-FAST supports automatic PAC provisioning, but you must enable it on the RADIUS server.

  **Note**  
  In the Cisco ACS, by default, the PAC expires in one week. If the phone has an expired PAC, authentication with the RADIUS server takes longer while the phone gets a new PAC. To avoid PAC provisioning delays, set the PAC expiration period to 90 days or longer on the ACS or RADIUS server.

- **Light Extensible Authentication Protocol (LEAP):** Cisco proprietary password-based mutual authentication scheme between the client (phone) and a RADIUS server. Cisco Unified IP Phone can use LEAP for authentication with the wireless network.

- **Auto (AKM):** Selects the 802.11 Authentication mechanism automatically from the configuration information that the AP, WPA-PSK, or WPA exhibits.

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

- **WPA/WPA2:** Uses RADIUS server information to generate unique keys for authentication. Because these keys are generated at the centralized RADIUS server, WPA/WPA2 provides more security than WPA preshared keys that are stored on the AP and phone.

- **Cisco Centralized Key Management (CCKM):** Uses RADIUS server and a wireless domain server (WDS) information to manage and authenticate keys. The WDS creates a cache of security credentials for CCKM-enabled client devices for fast and secure reauthentication.

With WPA/WPA2 and CCKM, encryption keys are not entered on the phone, but are automatically derived between the AP and phone. But the EAP username and password that are used for authentication must be entered on each phone.

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

To ensure that voice traffic is secure, the Cisco Unified IP Phone supports WEP, TKIP, and Advanced Encryption Standards (AES) for encryption. When these mechanisms are used for encryption, both the signalling SIP packets and voice Real-Time Transport Protocol (RTP) packets are encrypted between the AP and the Cisco Unified IP Phone.
WEP

With WEP use in the wireless network, authentication happens at the AP by using open or shared-key authentication. The WEP key that is setup on the phone must match the WEP key that is configured at the AP for successful connections. The Cisco Unified IP Phone supports WEP keys that use 40-bit encryption or a 128-bit encryption and remain static on the phone and AP.

EAP and CCKM authentication can use WEP keys for encryption. The RADIUS server manages the WEP key and passes a unique key to the AP after authentication for encrypting all voice packets; consequently, these WEP keys can change with each authentication.

TKIP

WPA and CCKM use TKIP encryption that has several improvements over WEP. TKIP provides per-packet key ciphering and longer initialization vectors (IVs) that strengthen encryption. In addition, a message integrity check (MIC) ensures that encrypted packets are not being altered. TKIP removes the predictability of WEP that helps intruders decipher the WEP key.

AES

An encryption method used for WPA2 authentication. This national standard for encryption uses a symmetrical algorithm that has the same key for encryption and decryption. AES uses Cipher Blocking Chain (CBC) encryption of 128 bits in size, which supports key sizes of 128, 192 and 256 bits, as a minimum. The Cisco Unified IP Phone supports a key size of 256 bits.

Note

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

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

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

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

• When you use Auto (AKM), encryption options are automatically configured for WPA, WPA2, WPA Pre-shared key, WPA2 Pre-shared key, or CCKM.

• In AKM mode, the phone authenticates with LEAP if the phone is configured with WPA, WPA2, or CCKM key management, or if 802.1x is used.

• The Cisco Unified IP Phone does not support auto EAP negotiation; to use EAP-FAST mode, you must specify it.

The following table provides a list of authentication and encryption schemes that are configured on the Cisco Aironet APs that the Cisco Unified IP Phone supports. The table shows the network configuration option for the phone that corresponds to the AP configuration.

Table 20: Authentication and Encryption Schemes

<table>
<thead>
<tr>
<th>Cisco AP Configuration</th>
<th>Cisco Unified IP Phone Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Key management</td>
</tr>
<tr>
<td>Open</td>
<td>Common encryption</td>
</tr>
<tr>
<td>Open (Static WEP)</td>
<td>None</td>
</tr>
<tr>
<td>Shared key (Static WEP)</td>
<td>WEP</td>
</tr>
<tr>
<td>LEAP 802.1x</td>
<td>Optional CCKM</td>
</tr>
<tr>
<td>LEAP WPA</td>
<td>WPA with optional CCKM</td>
</tr>
<tr>
<td>LEAP WPA2</td>
<td>WPA2</td>
</tr>
<tr>
<td>EAP-FAST 802.1x</td>
<td>Optional CCKM</td>
</tr>
<tr>
<td>EAP-FAST with WPA</td>
<td>WPA</td>
</tr>
<tr>
<td>EAP-FAST with WPA2</td>
<td>WPA2</td>
</tr>
<tr>
<td>WPA-PSK</td>
<td>WPA-PSK</td>
</tr>
</tbody>
</table>
Cisco Unified IP Phone
Configuration

<table>
<thead>
<tr>
<th>Cisco AP Configuration</th>
<th>Cisco Unified IP Phone Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPA2-PSK</td>
<td>Auto (AKM)</td>
</tr>
<tr>
<td>WAP2-PSK</td>
<td></td>
</tr>
<tr>
<td>AES</td>
<td></td>
</tr>
</tbody>
</table>


For more information about configuring authentication and encryption schemes on APs, see the [Cisco Aironet Configuration Guide](http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=278875243) for your model and release under the following URL:


### 802.1X Authentication

The Cisco IP Phones support 802.1X Authentication.

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

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

Support for 802.1X authentication requires several components:

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

You must perform the following actions to configure 802.1X.

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

  * Enabled: If you are using a switch that supports multidomain authentication, you can enable the PC port and connect a PC to it. In this case, Cisco IP Phones support proxy EAPOL-Logoff to
monitor the authentication exchanges between the switch and the attached PC. For more information about IEEE 802.1X support on the Cisco Catalyst switches, see the Cisco Catalyst switch configuration guides at:


* 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

Network Protocols, on page 9

Access 802.1X Authentication

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

Procedure

| Step 1 | Press Applications. |
| Step 2 | Choose Administrator Settings > Security Setup > 802.1X Authentication. |
| Step 3 | Configure the options as described in 802.1X Authentication Options, on page 172. |
| Step 4 | To exit this menu, press Exit. |

802.1X Authentication Options

The following table describes the 802.1X authentication options.
### Table 21: 802.1X Authentication Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>To change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Authentication</td>
<td>Determines whether 802.1X authentication is enabled:</td>
<td>See Set Device Authentication Field, on page 173.</td>
</tr>
<tr>
<td></td>
<td>• Enabled: Phone uses 802.1X authentication to request network access.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Disabled: Default setting. The phone uses CDP to acquire VLAN and network access.</td>
<td></td>
</tr>
<tr>
<td>Transaction Status</td>
<td>State: Displays the state of 802.1x authentication:</td>
<td>Display only. Cannot configure.</td>
</tr>
<tr>
<td></td>
<td>• Disconnected: Indicates that 802.1x authentication is not configured on the phone.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Authenticated: Indicates that the phone is authenticated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Held: Indicates that the authentication process is in progress.</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol: Displays the EAP method that is used for 802.1x authentication (can be EAP-FAST or EAP-TLS).</td>
<td></td>
</tr>
</tbody>
</table>

### Set Device Authentication Field

#### Procedure

**Step 1** Press Applications.

**Step 2** Choose Admin settings > Security setup > 802.1X Authentication

**Step 3** Set the Device Authentication option:

- Yes
- No

**Step 4** Press Apply.
Set EAP-MD5 Fields

Procedure

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

- Custom Phone Rings, page 175
- Custom Background Images, page 177
- Set Up Wideband Codec, page 179
- Set Up Idle Display, page 180

Custom Phone Rings

The Cisco IP Phone ships with two default ring types that are implemented in hardware: Chirp1 and Chirp2. Cisco Unified Communications Manager also provides a default set of additional phone ring sounds that are implemented in software as pulse code modulation (PCM) files. The PCM files, along with an XML file 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 documentation for your particular Cisco Unified Communications Manager release.

Set Up Custom Phone Ring

Procedure

Step 1
Create a PCM file for each custom ring (one ring per file). Ensure the PCM files comply with the format guidelines that are listed in the Custom Ring File Formats section.

Step 2
Upload the new PCM files that you created to the Cisco TFTP server for each Cisco Unified Communications Manager in your cluster.
Formore information, see the documentation for your particular Cisco Unified Communications Manager release.

**Step 3**
Use a text editor to edit the Ringlist.xml file.
See the "Custom Ring File Formats" section for information about how to format this file and for a sample Ringlist.xml file.

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

**Step 5**
To cache the new Ringlist.xml file:
- Stop and start the TFTP service by using Cisco Unified Serviceability
- Disable and reenable the "Enable Caching of Constant and Bin Files at Startup" TFTP service parameter, located in the Advanced Service Parameters area.

---

**Custom Ring File Formats**

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

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

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

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

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

The PCM files for the rings must meet the following requirements for proper playback on the phones:

- Raw PCM (no header)
- 8000 samples per second
- 8 bits per sample
- Mu-law compression
- Maximum ring size = 16080 samples
- Minimum ring size = 240 samples
- Number of samples in the ring = multiple of 240.
- Ring start and end at zero crossing.
To create PCM files for custom phone rings, use any standard audio editing package that supports these file format requirements.

**Custom Background Images**

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

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

---

**Attention**

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

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

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

---

**Set Up Custom Background Image**

**Procedure**

**Step 1**
Create two PNG files for each image (a full-size version and a thumbnail version). Ensure the PNG files comply with the format guidelines that are listed in Custom Background File Formats, on page 178.

**Step 2**
Upload the new PNG files that you created to the following subdirectory in the TFTP server for the Cisco Unified Communications Manager:
Desktops/640x480x24

**Note**
The file name and subdirectory parameters are case sensitive. Be sure to use the forward slash "/" when you specify the subdirectory path.

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

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

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

**Note**
We recommend that you store backup copies of custom image files in a different location. You can use these backup copies if the customized files are overwritten when you upgrade Cisco Unified Communications Manager.
**Step 4** Use a text editor to edit the List.xml file. See Custom Background File Formats, on page 178 for the file location, file, formatting requirements, and a sample file.

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

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

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

---

**Custom Background File Formats**

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

```
Desktops/640x480x24
```

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

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

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

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

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

**List.xml Example**

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

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

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

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

The PNG files for background images must meet the following requirements for proper display on the phone:
• Full size image - 640 pixels (width) X 480 pixels (height).
• Thumbnail image - 123 pixels (width) X 111 pixels (height).

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

Set Up Wideband Codec

By default, the G.722 codec is enabled for the Cisco Unified IP Phone 8961, 9951, and 9971. If Cisco Unified Communications Manager is configured to use G.722 and if the far endpoint supports G.722, the call connects using the G.722 codec in place of G.711.

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

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

Procedure

Step 1
To configure wideband support for all devices:
  a) From Cisco Unified Communications Manager Administration, choose System > Enterprise Parameters
  b) Set the Advertise G.722 Codec field
     The default value of this enterprise parameter is True, which means that all Cisco Unified IP Phone Models 9971 that register to this Cisco Unified Communications Manager advertise G.722 to Cisco Unified Communications Manager. If each endpoint in the attempted call supports G.722 in the capabilities set, Cisco Unified Communications Manager chooses that codec for the call whenever possible.

Step 2
To configure wideband support for a specific device:
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:


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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In Cisco Unified Communications Manager Administration, select Device &gt; Phone</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Idle field, enter the URL to the idle display XML Service.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Idle Timer field, enter the time that the idle phone waits before displaying the idle display XML service.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select Save.</td>
</tr>
</tbody>
</table>
Phone Features and Setup

- Phone Features and Setup Overview, page 182
- Cisco IP Phone User Support, page 183
- Telephony Features, page 183
- Feature Buttons and Softkeys, page 206
- Create Feature Control Policy, page 208
- Disable Speakerphone, page 210
- Schedule Power Save for Cisco IP Phone, page 210
- Schedule Power Save Plus (EnergyWise) on Cisco IP Phone, page 212
- Set up AS-SIP, page 215
- Enable Agent Greeting, page 217
- Set Up the DF Bit, page 217
- Set Up Do Not Disturb, page 218
- Set Up Monitoring and Recording, page 218
- Set Up Power Negotiation for LLDP, page 219
- Set Up RTCP Control, page 220
- Set Up Simplified New Call Window, page 220
- Set Up Automatic Port Synchronization, page 220
- Set Up Bluetooth Profiles, page 221
- Set Up SSH Access, page 221
- Set Up Call Forward Notification, page 222
- Client Matter Codes and Forced Authorization Codes, page 223
- Enable BLF for Call Lists, page 223
- Set Up Dual Bank Information, page 224
- Set Up Incoming Call Toast Timer, page 224
Phone Features and Setup Overview

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

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

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

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

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

Consider including the following types of information on this site:

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

Telephony Features

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

For information about using most of these features on the phone, see Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager. See Feature Buttons and Softkeys, on page 206 for a list of features that can be configured as programmable buttons, dedicated softkeys, and feature buttons.

Note: Cisco Unified Communications Manager Administration also provides several service parameters that you can use to configure various telephony functions. For more information about accessing and configuring service parameters, see Cisco Unified Communications Manager Administration Guide. For more information about the functions of a service, click on the name of the parameter or the question mark help button in the Service Parameter Configuration window.
### Table 22: Telephony Features for the Cisco Unified IP Phone

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actionable Incoming Call Alert</td>
<td>Controls whether the incoming call alert displays as a traditional pop-up alert or as an actionable alert.</td>
</tr>
<tr>
<td></td>
<td>See <a href="#">Enable Actionable Incoming Call Alert, on page 231</a>.</td>
</tr>
<tr>
<td>Agent Greeting</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>See:</td>
</tr>
<tr>
<td></td>
<td>• <a href="#">Enable Agent Greeting, on page 217</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="#">Cisco Unified Communications Manager Features and Services Guide</a>, “Barge and Privacy” chapter</td>
</tr>
<tr>
<td></td>
<td>• <a href="#">Cisco Unified Communications Manager System Guide</a>, &quot;Cisco Unified IP Phones” chapter</td>
</tr>
<tr>
<td>Alert Calls</td>
<td>Allows users to view a list of all phone numbers that users consider important and want to be notified of in chronological order.</td>
</tr>
<tr>
<td></td>
<td>See <a href="#">Cisco Unified Communications Manager Administration Guide</a>.</td>
</tr>
<tr>
<td>All Calls</td>
<td>Allows a user to view a list, sorted in chronological order (oldest first), of all active calls on all of the user phone lines.</td>
</tr>
<tr>
<td></td>
<td>See <a href="#">Assign Phone Button Template for All Calls, on page 235</a>.</td>
</tr>
<tr>
<td>All Calls, Shared Line, Calling and Called Display Interaction</td>
<td>Improves the user experience by presenting Barge, cBarge, and Conference calls as a single unified session.</td>
</tr>
<tr>
<td>All Calls on Primary Line</td>
<td>Allows the primary line to assume the All Calls functionality. Moving the All Calls functionality to the Primary Line frees up the feature key for other dedicated tasks.</td>
</tr>
<tr>
<td></td>
<td>See <a href="#">Cisco Unified Communications Manager Administration Guide</a>.</td>
</tr>
<tr>
<td>Anonymous Call Block</td>
<td>Allows a user to reject calls from anonymous callers.</td>
</tr>
<tr>
<td></td>
<td>See <a href="#">Cisco Unified Communications Manager Administration Guide</a>, &quot;SIP Profile Configuration&quot; chapter</td>
</tr>
<tr>
<td>Any Call Pickup</td>
<td>Allows users to pick up a redirected call via the CTI application, on any line in their call pickup group, regardless of how the call routed to the phone.</td>
</tr>
<tr>
<td></td>
<td>See <a href="#">Cisco Unified Communications Manager Features and Services Guide</a>, “Call Pickup” chapter</td>
</tr>
<tr>
<td>Answer (oldest call)</td>
<td>Allows a user to answer the oldest call that is available on all line appearances on the user phone, including Hold Reversion and Park Reversion calls that are in an altering state.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assisted Directed Call Park</td>
<td>Allows the user to direct-park a call by pressing only one button. See <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Configuring Directed Call Park” chapter.</td>
</tr>
<tr>
<td>Assured Services for SIP Lines</td>
<td>Offers users a highly secure call flow for Cisco IP Phones and third-party telephones with an option to place priority calls. For more information, see <em>Set up AS-SIP</em>, on page 215.</td>
</tr>
<tr>
<td>Audio-Only Lock Icon</td>
<td>Controls the display of the Security icons on the call. See the Cisco Unified Communications Manager documentation.</td>
</tr>
<tr>
<td>Audio Parameter Enhancement</td>
<td>Enables you to customize the audio parameters. These parameters control the quality of the audio that the users experience. For more information, see <em>Set Up Audio EQ</em>, on page 247.</td>
</tr>
<tr>
<td>AutoAnswer</td>
<td>Connects incoming calls automatically after a ring or two. AutoAnswer works with either the speakerphone or the headset. See <em>Cisco Unified Communications Manager Administration Guide</em>, “Directory Number Configuration” chapter.</td>
</tr>
<tr>
<td>Auto Dial</td>
<td>Allows the phone user to choose from matching numbers in the Placed Calls log while dialing. To place the call, the user can choose a number from the Auto Dial list or continue to enter digits manually.</td>
</tr>
<tr>
<td>Automatic Port Synchronization</td>
<td>When the Cisco Unified Communications Manager administrator uses the Remote Port Configuration feature to set the speed and duplex function of an IP Phone remotely, loss of packets can occur if one port is slower than the other. The Automatic Port Synchronization feature synchronizes the ports to the lower speed which eliminates packet loss. See <em>Set Up Automatic Port Synchronization</em>, on page 220.</td>
</tr>
<tr>
<td>Barge</td>
<td>Allows a user to join a nonprivate call on a shared phone line. The feature adds a user to a call and converts the call into a conference, allowing the user and other parties to access conference features. See:</td>
</tr>
<tr>
<td></td>
<td><em>Cisco Unified Communications Manager Administration Guide</em>, “Cisco Unified IP Phone Configuration” chapter</td>
</tr>
<tr>
<td></td>
<td><em>Cisco Unified Communications Manager System Guide</em>, “Cisco Unified IP Phone” chapter</td>
</tr>
<tr>
<td></td>
<td><em>Cisco Unified Communications Manager Features and Services Guide</em>, “Barge and Privacy” chapter</td>
</tr>
<tr>
<td></td>
<td><em>Cisco Unified Communications Manager Administration Guide</em>, “Feature Control Policy Configuration”</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Bluetooth Profiles                        | Allows you to select the Bluetooth profiles for Cisco Unified Phones 9951 and 9971. See:  
  • Set Up Bluetooth Profiles, on page 221  
  • Cisco Unified Communications Manager Administration Guide                                                                                                                                                                                                                                                                                   |
| Block External to External Transfer       | Prevents users from transferring an external call to another external number. See Cisco Unified Communications Manager Features and Services Guide, "External Call Transfer Restrictions" chapter.                                                                                                                                                                                                                                               |
| Busy Lamp Field (BLF)                     | Allows a user to monitor the call state of a directory number that associates with a speed-dial button, call log, or directory listing on the phone. With the Pickup feature, when the DN receives an incoming call, the system alerts the monitoring user, who can then pick up the call. See Cisco Unified Communications Manager Features and Services Guide, "Presence" and "Call Pickup" chapters. |
| Busy Lamp Field (BLF) Pickup              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Call Back                                 | Provides users with an audio and visual alert on the phone when a busy or unavailable party becomes available. See:  
  • Cisco Unified Communications Manager System Guide, "Cisco Unified IP Phone" chapter  
  • Cisco Unified Communications Manager Features and Services Guide, "Cisco CallBack" chapter                                                                                                                                                                                                                                               |
| Call Chaperone                            | Allows an authorized Call Chaperone user to supervise and record a call. An announcement alerts call participants that the call is being recorded. See Cisco Unified Communications Manager Features and Services Guide, "External Call Control" chapter.                                                                                                                                                                                                                     |
| Call Display Restrictions                 | Determines the information that displays for calling or connected lines, depending on the parties who are involved in the call. See:  
  • Cisco Unified Communications Manager Administration Guide, "Cisco Unified IP Phone Configuration" chapter  
  • Cisco Unified Communications Manager Features and Services Guide, "Call Display Restrictions" chapter                                                                                                                                                                                                                                      |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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:  
- *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter  
- *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phone” chapter  
- Customize the Self Care Portal Display, on page 100                                                                                                                                                                                                                                                                                                                                                               |
| 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. See *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phone” chapter.                                                                                                                                                                                                                                      |
| Call Forward All Loop Prevention             | Prevents a user from configuring a Call Forward All destination directly on the phone that creates a Call Forward All loop or that creates a Call Forward All chain with more hops than the existing Forward Maximum Hop Count service parameter allows. See *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phone” chapter.                                                                                                                                                                                                                       |
| 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 *Cisco Unified Communications Manager System Guide*, “Understanding Directory Numbers” chapter.                                                                                                                                                         |
| Call Forward Notification                    | Allows you to configure the information that the user sees upon receiving a forwarded call. See *Set Up Call Forward Notification*, on page 222.                                                                                                                                                                                                                                                                                      |
| Call History Display Enhancement             | Displays only the call history of a selected line. See *Enable the Call History Display Enhancement*, on page 232.                                                                                                                                                                                                                                                                                                                                               |
| Call History for Shared Line                 | Allows the user to view shared line activity in the phone's call logs. This feature:  
- Logs missed calls for a shared line  
- Logs all answered and placed calls for a shared line  
See *Enable Call History for Shared Line*, on page 233.                                                                                                                                                                                                                                                                                                                                 |
<p>| Call ID Display Consistency for cBarge Across Shared Line | Displays the same call ID on all calls participating in a conference call initiated on a shared line using cBarge.                                                                                                                                                                                                                                                                                                                                                               |
| Call Park                                    | Allows users to park (temporarily store) a call and then retrieve the call by using another phone in the Cisco Unified Communications Manager system. See <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Call Park and Directed Call Park” chapter.                                                                                                                                                                                                                     |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Pickup</td>
<td>Allows a user to answer a call that is ringing on another phone in the pickup group by redirecting the call.</td>
</tr>
<tr>
<td></td>
<td>See <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Call Pickup” chapter.</td>
</tr>
<tr>
<td>Call Recording</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>See <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Monitoring and Recording” chapter.</td>
</tr>
<tr>
<td>Call Transfer Notification</td>
<td>Enables users to see who transferred the call to them.</td>
</tr>
<tr>
<td>Call Waiting</td>
<td>Indicates and allows users to answer an incoming call that rings while on another call. Displays incoming call information on the phone screen.</td>
</tr>
<tr>
<td></td>
<td>See <em>Cisco Unified Communications Manager System Guide</em>, “Understanding Directory Numbers” chapter.</td>
</tr>
<tr>
<td>Caller ID</td>
<td>Displays caller identification, such as a phone number, name, or other descriptive text, on the phone screen.</td>
</tr>
<tr>
<td></td>
<td>See:</td>
</tr>
<tr>
<td></td>
<td>• <em>Cisco Unified Communications Manager Administration Guide</em>, ”Cisco Unified IP Phone Configuration” chapter</td>
</tr>
<tr>
<td></td>
<td>• <em>Cisco Unified Communications Manager System Guide</em>, “Understanding Route Plans” chapter</td>
</tr>
<tr>
<td></td>
<td>• <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Call Display Restrictions” chapter</td>
</tr>
<tr>
<td></td>
<td>• <em>Cisco Unified Communications Manager Administration Guide</em>, “Directory Number Configuration” chapter</td>
</tr>
<tr>
<td>Caller ID Blocking</td>
<td>Allows a user to block their phone number or e-mail address from phones that have caller identification enabled.</td>
</tr>
<tr>
<td></td>
<td>See:</td>
</tr>
<tr>
<td></td>
<td>• <em>Cisco Unified Communications Manager System Guide</em>, “Understanding Route Plans” chapter</td>
</tr>
<tr>
<td></td>
<td>• <em>Cisco Unified Communications Manager Administration Guide</em>, “Directory Number Configuration” chapter</td>
</tr>
<tr>
<td>Calling Party Normalization</td>
<td>Globalizes or localizes the incoming calling party number so that the appropriate calling number presentation displays on the phone. Supports the international escape character “+”.</td>
</tr>
<tr>
<td></td>
<td>See <em>Cisco Unified Communications Features and Services Guide</em>, “Calling Party Normalization” chapter.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| CAST for SIP                | Establishes communication between Cisco Unified Video Advantage (CUVA) and the Cisco Unified IP Phones to support video on the PC even on IP phones that do not have video capability.  
See *Cisco Unified Communications Manager Features and Services Guide*. |
| CGI CallInfo and LineInfo   | Provides phone information that can be used for troubleshooting phone problems. Web access must be enabled on the phone to view the information.  
See *Request Information from the Phone in XML, on page 297*.                                            |
| CGI ModellInfo              | Provides phone information that can be used for troubleshooting phone problems. Web access must be enabled on the phone to view the information. A user must be associated with the phone.  
See *Request Information from the Phone in XML, on page 297*.                                             |
| Cisco Extension Mobility Change PIN | Enables a user to change the PIN from a Cisco Unified IP Phone. Change the PIN using  
• ChangePIN softkey on the Extension Mobility logout screen  
• Change Credential IP Phone Service on the phone  
See:  
• *Cisco Unified Communications Manager Features and Services Guide*, “Cisco Extension Mobility” chapter  
• *Cisco Unified Communications Manager Administration*, “Configuring the Change Credential IP Phone Service” section |
| Cisco Extension Mobility    | Enables a user configured in one cluster to sign into a Cisco Unified IP Phone in another cluster. Users from a home cluster sign into a Cisco Unified IP Phone at a visiting cluster.  
Configure Cisco Extension Mobility on Cisco Unified IP Phones before you configure EMCC.  
See *Cisco Unified Communications Manager Features and Services Guide*, “Cisco Extension Mobility Cross Cluster” chapter. |
| Cisco Extension Mobility Cross Cluster | Enables a user configured in one cluster to sign into a Cisco Unified IP Phone in another cluster.  
See *Cisco Unified Communications Manager Features and Services Guide*, “Cisco Extension Mobility Cross Cluster” chapter. |
| Cisco IP Manager Assistant (IPMA) | Provides call routing and other call management features to help managers and assistants handle phone calls more effectively.  
See *Set Up Cisco IP Manager Assistant*, on page 244.                                                        |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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*, on page 14 | **Cisco Unified Communications Manager Express (Unified CME)** Version Negotiation |
| Provides integrated VPN functionality for Cisco Virtualization Experience Clients (Cisco VXC) 2111 and 2112. See *Cisco VXC VPN*, on page 253. | **Cisco VXC VPN** |
| Allows users to make calls from web and desktop applications. See *Cisco Unified Communications Manager Features and Services Guide*, "Cisco Web Dialer" chapter. | **Cisco Web Dialer** |
| Requires a user to enter a code to identify that the call relates to a specific client matter. See:  
  - *Client Matter Codes and Forced Authorization Codes*, on page 223  
  - *Cisco Unified Communications Manager Administration Guide*, “Route Pattern Configuration” section. | **Client Matter Code** |
<p>| Allows a user to talk simultaneously with multiple parties by calling each participant individually. See <em>Cisco Unified Communications Manager System Guide</em>, &quot;Conference Bridges&quot; and &quot;Cisco Unified IP Phone&quot; chapters. | <strong>Conference</strong> |
| Enables conference and transfer actions to use the Simplified New Call Window or the New Call Window, depending on the setting of the Simplified New Call UI field. See <em>Cisco Unified Communications Manager Administration Guide</em>. | <strong>Conference and Transfer Enhancement</strong> |
| 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. See <em>Cisco Unified Communications Manager Administration Guide</em>. | <strong>Confidential Access Level (CAL)</strong> |
| Controls how network packets are sent. Packets can be sent in chunks (fragments) of various sizes. When the DF bit is set to 1 in the packet header, the network payload does not fragment when going through network devices, such as switches and routers. Removing fragmenting avoids incorrect parsing on the receiving side, but results in slightly slower speeds. By default, the DF bit is set to 0. See <em>Set Up the DF Bit</em>, on page 217 | <strong>Configurable DF Bit</strong> |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configurable Font Size</td>
<td>Allows users to increase or decrease the maximum number of characters the IP phone displays for Call History and Call Screen by changing the font size. A smaller font increases the maximum number of displayed characters, and a larger font decreases the maximum number of displayed characters.</td>
</tr>
<tr>
<td>Configurable RTP/sRTP Port Range</td>
<td>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 241.</td>
</tr>
<tr>
<td>Configurable TLS Session Resumption Timer</td>
<td>Enables the resumption of the TLS handshake without repeating the authentication, or confidentiality, or authorization processes. See Set Up TLS Resumption Timer, on page 242.</td>
</tr>
<tr>
<td>CTI Applications</td>
<td>A computer telephony integration (CTI) route point can designate a virtual device to receive multiple, simultaneous calls for application-controlled redirection. See Cisco Unified Communications Manager Administration Guide, &quot;CTI Route Point Configuration&quot; chapter.</td>
</tr>
<tr>
<td>CTL/ITL Signature</td>
<td>Enhances security by using the secure hash algorithm (SHA-1) in the CTL and ITL files. No configuration required.</td>
</tr>
<tr>
<td>CTL and ITL Status Display and Report</td>
<td>Enables you to report the CTL and ITL information to the Cisco Unified Communications Manager, using a Cisco Unified IP Phone. See the Cisco Unified Communications Manager Administration Guide.</td>
</tr>
<tr>
<td>Custom Line Filters</td>
<td>Enables users to set the alerting call notification priority on a subset of lines covered by an alert filter. The custom filter generates either traditional pop-up alerts or actionable alerts for incoming calls on the selected lines. For each filter, only the subset of lines under coverage will generate an alert. If a filter is turned off, lines under its coverage will not show alert notifications. See Set Up Custom Line Filter, on page 233.</td>
</tr>
<tr>
<td>Default Back To All Calls</td>
<td>Improves the experience for users with multiple lines by displaying the primary line with the All Calls view when a call completes. See Cisco Unified Communications Manager Administration Guide.</td>
</tr>
<tr>
<td>Default Wallpaper Control</td>
<td>When the Enable End User Access to Phone Background Image Setting check box is enabled, users can change the background image (or wallpaper) for the LCD screen on their phone. See Cisco Unified Communications Manager Administration Guide, “Common Phone Profile Configuration” chapter.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Device Invoked Recording</td>
<td>Provides end users with the ability to record their telephone calls via a softkey. For more information, see Enable Device Invoked Recording, on page 227.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Dial Tone From Release Key</td>
<td>Allows users to disconnect a call and get the dial tone by pressing only one button. When the user presses the Release button while on a call or while dialing off-hook, the active call ends and dial tone sounds. The New Call window appears on the selected line on the phone screen. For more information, see Set Up Dial Tone from Release Button, on page 228.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Directed Call Park</td>
<td>Allows a user to transfer an active call to an available directed call park number that the user dials or speed dials. See Cisco Unified Communications Manager Features and Services Guide, “Call Park and Directed Call Park” chapter.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Divert</td>
<td>Allows a user to transfer a ringing, connected, or held call directly to a voice-messaging system or to the busy target. Divert acts on the highlighted call only. Incoming calls are not automatically highlighted. If a second call rings while the user is on the first call, Divert acts on the first call unless the user actively highlights the second call. When a call is diverted, the line becomes available to make or receive new calls. For more information about diverting calls to voicemail, see Cisco Unified Communications Manager Features and Services Guide, “Immediate Divert” chapter. For more information about Enhanced Immediate Divert, see Cisco Unified Communications Manager System Guide, “Cisco Unified IP Phone” chapter.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Dual Bank Information</td>
<td>Allows the Cisco Unified Communications Manager administrator to upgrade phone firmware with a new load before resetting the previous load to an Inactive load status. See Set Up Dual Bank Information, on page 224.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Do Not Disturb (DND)</td>
<td>When DND is turned on, either no audible rings occur during the ringing-in state of a call, or no audible or visual notifications of any type occur. See Cisco Unified Communications Manager Features and Services Guide, “Do Not Disturb” chapter.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Video On/Off</td>
<td>Improves the video conference call flow by removing the black box that is displayed when one party has the Auto Transmit setting on their phone set to Off. See Set Up Enable Video On/Off, on page 228.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>EnergyWise</td>
<td>Enables an IP Phone to sleep (power down) and wake (power up) at predetermined times, to promote energy savings See Schedule Power Save Plus (EnergyWise) on Cisco IP Phone, on page 212.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Enhanced Secure Extension</td>
<td>Improves the Secure Extension Mobility Cross Cluster (EMCC) feature by preserving the network and security configurations on the login phone. Doing so maintains security policies, preserves network bandwidth, and avoids network failure within the visiting cluster (VC). See Cisco Unified Communications Manager Features and Services Guide.</td>
</tr>
<tr>
<td>Mobility Cross Cluster</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enlarge Unique Call Identifier</td>
<td>The unique call identifier displays at the same font size as the calling number.</td>
</tr>
<tr>
<td>E-SRST Service Improvements</td>
<td>Enables Video, Shared Line, and BLF Speed Dial in SRST mode.</td>
</tr>
<tr>
<td></td>
<td>See Survivable Remote Site Telephony, on page 95.</td>
</tr>
<tr>
<td>External Call Control</td>
<td>Allows Cisco Unified Communications Manager to route audio and video calls to a route server that hosts routing rules.</td>
</tr>
<tr>
<td></td>
<td>See Cisco Unified Communications Manager Features and Services Guide, &quot;External Call Control&quot; chapter.</td>
</tr>
<tr>
<td>Fast Dial Service</td>
<td>Allows a user to enter a Fast Dial code to place a call. You can assign Fast Dial codes to phone numbers or to Personal Address Book entries. See &quot;Services&quot; in this table. See Modify Phone Button Template for PAB or Fast Dial, on page 236.</td>
</tr>
<tr>
<td>FIPS 140-2 Level 1 Support</td>
<td>Federal Information Processing Standard (FIPS) 140-2 Level 1 provides a secure, encrypted environment that meets the United States Department of Defense Unified Capabilities Requirements (UCR) 2008 standard. The default setting is Disable. See Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>Forced Authorization Code</td>
<td>Requires a user to enter an authorization code to place a call. Controls the types of calls that certain users can place. See:</td>
</tr>
<tr>
<td></td>
<td>• Client Matter Codes and Forced Authorization Codes, on page 223</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager Administration Guide, &quot;Route Pattern Configuration&quot; section</td>
</tr>
<tr>
<td>Gateway Recording For SIP</td>
<td>Provides the ability to record calls using Cisco Voice Gateway. This allows you to record calls made on Cisco Jabber, a Cisco IP Phone (SIP), or calls made on a mobile device. See Cisco Unified Communications Manager Features and Services Guide.</td>
</tr>
<tr>
<td>Handset Bass Adjustment</td>
<td>Allows a user to set the phone to use either a reduced bass tone or the full bass tone. Reduced bass removes low frequencies, which can improve muffled voices or insufficient volume on handsets. The default setting is for reduced bass.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Headset Sidetone Controls | Allows you to adjust headset sidetone levels.  
**Note** This feature is only for analog headsets.  
See:  
* Cisco Unified Communications Manager System Guide, “Cisco Unified IP Phone” chapter  
* Cisco Unified Communications Manager Administration Guide, “Setting Headset Sidetone Controls” section  
* Set Headset Sidetone Control, on page 226 |
| Hide Softkeys in Full Screen Video Mode | Controls the way that softkeys display in full screen video mode. |
| Hide Video Option | Provides flexibility with the flexibility to hide the video window. When the video is displayed, the user sees the Hide Video softkey; when the video is hidden, the user sees the Show Video softkey.  
| Hide Wi-Fi User Interface Setting | Removes the Wireless Setup option from the Network Setup menu when Wi-Fi is disabled from the Cisco Unified Communications Manager.  
This feature is supported only on the Cisco Unified IP Phone 9971.  
| Hold Reversion | Limits the amount of time that a call can be on hold before it reverts back to the phone that put the call on hold and alerts the user.  
Reverting calls are distinguished from incoming calls by a single ring (or beep, depending on the new call indicator setting for the line). This notification repeats at intervals if the call is not resumed.  
A call that triggers Hold Reversion also displays an animated icon in the call bubble and a brief message on the status line.  
You can configure call focus priority to favor incoming or reverting calls.  
See Cisco Unified Communications Manager Features and Services Guide, “Hold Reversion” chapter. |
| Hold Status | Enables phones with a shared line to distinguish between the local and remote lines that placed a call on hold. |
| 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 the "Music on Hold" entry in this table for information.  
See "Hold Reversion" in this table. |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hold/Resume Toggle</td>
<td>Allows users to toggle a call between an active state and on-hold state using the Hold button.</td>
</tr>
<tr>
<td>Hunt Group Display</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>When an incoming call is offered to a directory number that is part of the hunt group, this feature displays the main directory number in addition to the calling party.</td>
</tr>
<tr>
<td></td>
<td>See:</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager Administration Guide, &quot;Hunt Group Configuration&quot; chapter</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager System Guide, &quot;Understanding Route Plans&quot; chapter</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager Administration Guide, &quot;CTI Route Point Configuration&quot; chapter</td>
</tr>
<tr>
<td>Incoming Call Toast Timer</td>
<td>Allows you to set the length of time that an incoming call toast (notification) appears on the phone screen.</td>
</tr>
<tr>
<td></td>
<td>See Set Up Incoming Call Toast Timer, on page 224.</td>
</tr>
<tr>
<td>Intercom</td>
<td>Allows users to place and receive intercom calls using programmable phone buttons. You can configure intercom line buttons to:</td>
</tr>
<tr>
<td></td>
<td>• Directly dial a specific intercom extension</td>
</tr>
<tr>
<td></td>
<td>• Initiate an intercom call and then prompt the user to enter a valid intercom number</td>
</tr>
<tr>
<td></td>
<td>See Cisco Unified Communications Manager Feature and Services Guide, &quot;Intercom&quot; chapter</td>
</tr>
<tr>
<td>Intelligent Session Control</td>
<td>Reroutes an enterprise originated call that was placed a user’s mobile phone through the enterprise number. The call only rings the user mobile but not the desk phone. When the user answers the call on the mobile phone, the desk phone displays a Remote in Use message. During these calls, a user can use the various features of the mobile phone.</td>
</tr>
<tr>
<td></td>
<td>See Cisco Unified Communications Manager Features and Services Guide, &quot;Cisco Unified Mobility&quot; chapter</td>
</tr>
<tr>
<td>IPv6 Support</td>
<td>Provides support for expanded IP addressing on Cisco IP Phones. IPv6 support is provided in standalone or in dual-stack configurations. In dual-stack mode, the phone is able to communicate using IPv4 and IPv6 simultaneously, independent of the content.</td>
</tr>
<tr>
<td></td>
<td>See Configure Network Settings, on page 70.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Line Select                     | If this feature is disabled (default), the ringing line is selected. When the feature is enabled, the primary line is picked up even if a call is ringing on another line. The user must manually select the other line. See "Always use prime line" in the following chapters of the *Cisco Unified Communications Manager Administration Guide*:  
  • "Device Profile Configuration"  
  • "Common Phone Profile Configuration"  
  • "Cisco Unified IP Phone Services Configuration"                                                                                                                                                                                                                                                                                                                                                                     |
| Line Select for Voice Messages  | When disabled (default), pressing the Messages button selects the line that has a voice message. If more than one line has voice mail, the first available line is selected. When the feature is enabled, the primary line is always used to retrieve voice messages. See "Always use prime line for voice message" in the following chapters of the *Cisco Unified Communications Manager Administration Guide*:  
  • "Device Profile Configuration"  
  • "Common Phone Profile Configuration"  
  • "Cisco Unified IP Phone Services Configuration"                                                                                                                                                                                                                                                                                                                                                                           |
| Line State Display Enhancement  | Enables users to see if a Cisco Unified IP Phone is in the Remote-in-use state when there is a call alert on shared lines. For more information, see *Cisco Unified Communications Manager Administration Guide*.                                                                                                                                                                                                                                                            |
| Line Status for Call Lists      | Allows the user to see the Line Status availability status of monitored line numbers in the Call History list. See Enable BLF for Call Lists, on page 223.                                                                                                                                                                                                                                                                             |
| 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 247.                                                                                                                                                                                                                                                                                                                                                                                                  |
| Log Out Of Hunt Groups          | Allows users to sign out of a hunt group and temporarily block calls from ringing their phone when they are not available to take calls. Logging out of hunt groups does not prevent non-hunt group calls from ringing their phone. See:  
  • Configure Phone Services for Users, on page 86  
  • *Cisco Unified Communications Manager System Guide*, "Understanding Route Plans" chapter                                                                                                                                                                                                                                                                                                               |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Malicious Caller Identification (MCID) | Allows users to notify the system administrator about suspicious calls. See:  
  - *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phone” chapter  
  - *Cisco Unified Communications Manager Features and Services Guide*, “Malicious Call Identification” chapter |
| Meet Me Conference | Allows a user to host a Meet Me conference in which other participants call a predetermined number at a scheduled time. See *Cisco Unified Communications Manager Administration Guide*, “Meet-Me Number/Pattern Configuration” chapter. |
| Message Waiting | Defines directory numbers for message waiting on and message waiting off indicators. A directly connected voice-messaging system uses the specified directory number to set or to clear a message-waiting indication for a particular Cisco Unified IP Phone. See:  
  - *Cisco Unified Communications Manager Administration Guide*, "Message Waiting Configuration" chapter  
  - *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Unified Communications Manager” chapter |
<p>| Message Waiting Indicator (MWI) | The MWI is both a visual indicator, viewable from 360 degrees and an audible message waiting indicator. Users change the voice message light on their handset and the audible voice message indicator on their phone by logging in to their User Options web pages and accessing the message indicator settings. Users change the setting to on or off. See <em>Cisco Unified Communications Manager System Guide</em>, “Cisco Unified IP Phone” chapter. |
| Missed Call History | Allows a user to specify whether missed calls are logged in the missed calls history for a given line appearance. See <em>Cisco Unified Communications Manager Administration Guide</em>, “Directory Number Configuration” chapter. |
| Mobile Connect | Enables users to manage business calls by using a single phone number and pick up in-progress calls on the desktop phone and a remote device, such as on a mobile phone. Users can restrict the group of callers according to phone number and time of day. Also see the Session Handoff entry in this table. See <em>Cisco Unified Communications Manager Features and Services Guide</em>, &quot;Cisco Unified Mobility” chapter. |
| Mobile Voice Access | Extends Mobile Connect capabilities by allowing users to access an interactive voice response (IVR) system to originate a call from a remote device, such as a cellular phone. See <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Cisco Unified Mobility” chapter. |</p>
<table>
<thead>
<tr>
<th><strong>Feature</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring and Recording</td>
<td>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. See <em>Cisco Unified Communications Manager Features and Services Guide</em>, &quot;Monitoring and Recording&quot; chapter.</td>
</tr>
<tr>
<td>Multiple Calls Per Line Appearance</td>
<td>Each line can support multiple calls. Only one call can be active at any time; other calls are automatically placed on hold.</td>
</tr>
<tr>
<td></td>
<td>See <em>Cisco Unified Communications Manager System Guide</em>, “Understanding Directory Numbers” chapter.</td>
</tr>
<tr>
<td>Music On Hold</td>
<td>Plays music while callers are on hold.</td>
</tr>
<tr>
<td></td>
<td>See <em>Cisco Unified Communications Manager Features and Services Guide</em>, &quot;Music On Hold&quot; chapter.</td>
</tr>
<tr>
<td>Mute</td>
<td>Mutes the microphone from the handset or headset.</td>
</tr>
<tr>
<td>New Versions of Cisco Unified IP Phone 8961, 9951, and 9971</td>
<td>Provides new versions of the existing phone models. The model numbers remain the same. This feature affects all phones manufactured after October 31, 2012. These phones must run Firmware Release 9.3(2) or later. The phone firmware does not allow the phone to be downgraded to releases earlier than Release 9.3(2).</td>
</tr>
<tr>
<td>On-Hook Dialing</td>
<td>Allows a user to dial a number without going off hook. The user can then either pick up the handset, press Call, or press either the headset or speaker buttons to initiate the call.</td>
</tr>
<tr>
<td></td>
<td>See <em>Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager (SIP)</em>, &quot;Calling Features&quot; chapter.</td>
</tr>
<tr>
<td>One Button Access to Call History</td>
<td>Provides the user with quick access to the Call History screen.</td>
</tr>
<tr>
<td>One Touch Private Line Automatic Ringdown (PLAR)</td>
<td>Improves the Private Line Automated Ringdown (PLAR) feature by automatically selecting the line for the call.</td>
</tr>
<tr>
<td></td>
<td>See <em>Cisco Unified Communications Manager Administration Guide</em>, “Directory Number Configuration” chapter.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Park Monitoring                     | Monitors the status of a parked call. The park monitoring call bubble is not cleared until the parked call gets retrieved or is abandoned by the parkee. This parked call can be retrieved by using the same call bubble on the parker phone.  

See:  
- Park Monitoring, on page 229  
- Cisco Unified Communications Manager Features and Services Guide, "Call Park and Directed Call Park" chapter                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
## Telephony Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Negotiation over LLDP</td>
<td>Allows the phone to negotiate power using LLDP and CDP protocols. Power Negotiation should not be disabled when the phone is connected to a switch that supports power negotiation. If disabled, it could cause the switch to shut off power to the phone. See <em>Cisco Unified Communications Manager Administration Guide</em>.</td>
</tr>
<tr>
<td>Presence-Enabled Directories</td>
<td>Allows a user to monitor the call state of another directory number (DN) that is listed in call logs, speed dials, and corporate directories. See <em>Cisco Unified Communications Manager Features and Services Guide</em>, “Presence” chapter.</td>
</tr>
</tbody>
</table>
| Privacy                               | Prevents users who share a line from adding themselves to a call and from viewing information on their phone screens about the call of another user. See:  
  - *Cisco Unified Communications Manager Administration Guide*, “Cisco Unified IP Phone Configuration” chapter  
  - *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phone” chapter  
  - *Cisco Unified Communications Manager Features and Services Guide*, “Barge and Privacy” chapter |
| Privacy Setting Enhancement            | Controls the information displayed on the assistant phone and in the assistant phone log for private manager calls. For more information, see *Enable Privacy Settings*, on page 246. |
| Private Line Automated Ringdown (PLAR) | The Cisco Unified Communications Manager administrator can configure a phone number that the Cisco Unified IP Phone dials as soon as the handset goes off hook. This feature can be useful for phones that are designated for calling emergency or “hotline” numbers. See *Cisco Unified Communications Manager Administration Guide*, “Directory Number Configuration” chapter. |
| Programmable Feature Button           | The administrator can assign features to programmable keys. When the administrator configures features on a feature button, the features always remain visible and accessible to the user; for example, the administrator can assign a dedicated Pickup button on the phone. See:  
  - *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phone” chapter  
  - *Cisco Unified Communications Manager Administration Guide*, “Phone Button Template Configuration” chapter |
<p>| Prompt for Barge                       | Provides an option to display a visual alert prompt when a user tries to barge into a call.                                                                                                                     |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>See</th>
</tr>
</thead>
</table>
| Protected Calling             | Provides a secure (encrypted) connection between two phones. A security tone plays at the beginning of the call to indicate that both phones are protected.                                                       | • Supported Security Features, on page 160  
• Cisco Unified Communications Manager Security Guide |
| Quality Reporting Tool (QRT)  | Allows users to use Report Quality on a phone to submit information about problem phone calls. QRT can be configured for either of two user modes, depending upon the amount of desired user interaction with QRT. | • Cisco Unified Communications Manager System Guide, “Cisco Unified IP Phone” chapter  
• Cisco Unified Communications Manager Features and Services Guide, “Quality Report Tool” chapter |
| Redial                        | Allows users to call the most recently dialed phone number by pressing Redial.                                                                                                                                  |                                                                                             |
| Remote Port Configuration     | Allows the administrator to configure the speed and duplex function of the phone Ethernet ports remotely by using Cisco Unified Communications Manager Administration. This practice enhances the performance for large deployments with specific port settings. | See Set Up Remote Port Configuration, on page 226.                                           |
| Ring Tone Setting             | Identifies ring type that is used for a line when a phone has another active call.                                                                                                                           | • Cisco Unified Communications Manager Administration Guide, “Directory Number Configuration” chapter  
• Custom Phone Rings, on page 175 |
<p>| Ringtone                      | Users can customize how their phone indicates an incoming call and a new voice mail message.                                                                                                                | See Cisco Unified Communications Manager Features and Services Guide, &quot;Custom Phone Rings&quot; chapter. |
| RTCP Always On                | Simplifies the phone administration by removing the need to set the RTCP Control for Video field. RTCP is always turned on for phones.                                                                      |                                                                                             |
| RTCP Control For Video        | The administrator can enable the phones to transmit and receive RTCP packets for both audio and video streams in a video call.                                                                               | See Cisco Unified Communications Manager Administration Guide.                             |
| RTCP Hold For SIP             | Ensures that the gateway does not drop held calls. The gateway checks the status of the RTCP port to determine whether a call is active or not. By keeping the phone port open, the gateway will not end held calls. |                                                                                             |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure and Nonsecure Indication Tone</td>
<td>Controls the playing of the Secure indication tone. See <a href="#">Phone Call Security, on page 164</a>.</td>
</tr>
<tr>
<td>Secure Extension Mobility Cross Cluster</td>
<td>Secure Extension Mobility Cross Cluster&lt;br&gt;See <a href="#">Cisco Unified Communications Manager Features and Services Guide</a>, &quot;Cisco Extension Mobility Cross Cluster&quot; chapter.</td>
</tr>
<tr>
<td>Secure Conference</td>
<td>Allows secure phones to place conference calls by using a secured conference bridge. See:</td>
</tr>
<tr>
<td></td>
<td>• <a href="#">Supported Security Features, on page 160</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="#">Cisco Unified Communications Manager System Guide</a>, “Conference Bridges” chapter</td>
</tr>
<tr>
<td></td>
<td>• <a href="#">Cisco Unified Communications Manager Administration Guide</a>, “Conference Bridge Configuration” chapter</td>
</tr>
<tr>
<td></td>
<td>• <a href="#">Cisco Unified Communications Manager Security Guide</a></td>
</tr>
<tr>
<td>Separate Audio and Video Mute</td>
<td>Allows the administrator to control the user’s ability to mute the audio while transmitting a video image. See <a href="#">Set Up Separate Audio and Video Mute, on page 241</a>.</td>
</tr>
<tr>
<td>Separate Audio and Video Port Range</td>
<td>Enables you to improve Quality of Service (QoS) by configuring audio traffic and video traffic on different ports. See <a href="#">Set Up the Audio and Video Port Range, on page 242</a>.</td>
</tr>
<tr>
<td>Range Configuration</td>
<td>Serviceability for SIP Endpoints</td>
</tr>
<tr>
<td></td>
<td>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. See <a href="#">Control Debug Information from Cisco Unified Communications Manager, on page 324</a>.</td>
</tr>
<tr>
<td>Services</td>
<td>Allows you to use the Cisco Unified IP Phone Services Configuration menu in Cisco Unified Communications Manager Administration to define and maintain the list of phone services to which users can subscribe. <strong>Note</strong> Some services appear on the phone by default, or you can disable them so that they do not display on the phone. See:</td>
</tr>
<tr>
<td></td>
<td>• <a href="#">Cisco Unified Communications Manager Administration Guide</a>, “Cisco Unified IP Phone Configuration” chapter</td>
</tr>
<tr>
<td></td>
<td>• <a href="#">Cisco Unified Communications Manager System Guide</a>, “Cisco Unified IP Phone Services” chapter</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Services URL Button  | Allows users to access services from a programmable button rather than by using the Services menu on a phone.  
See:  
  • *Cisco Unified Communications Manager Administration Guide*, “Cisco Unified IP Phone Configuration” chapter  
  • *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phone Services” chapter                                                                                                                                                                                  |
| Session Handoff     | Allows users to switch calls from a mobile phone to Cisco Unified devices that share the same line. Handsets on all the devices on the shared line then flash simultaneously.  
See:  
  • *Cisco Unified Communications Manager Features and Services Guide*, “Cisco Unified Mobility” chapter  
  • *Cisco Unified Communications Manager Features and Services Guide*, ”Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator Integration” chapter                                                                                                                                 |
| Shared Line          | Allows a user with multiple phones to share the same phone number or allows a user to share a phone number with a coworker.  
See *Cisco Unified Communications Manager System Guide*, “Understanding Directory Numbers” chapter.                                                                                                                                                                                                                             |
| Simplified New Call Bubble | Provides a new user interface for off-hook dialing.  
See:  
  • Set Up Simplified New Call Window, on page 220  
  • *Cisco Unified Communications Manager Administration Guide*.                                                                                                                                                                                                                     |
| SIP Phone No Alert Name | Makes it easier for end users to identify alert calls by displaying the alert name in the Placed Calls history.                                                                                                                                                                                                            |
| SSH Disable          | Enables or disables the use of SSH on the phone.  
See Set Up SSH Access, on page 221.                                                                                                                                                                                                                                           |
| Softkey Policy Control | Enables you to configure certain features as either softkeys or programmable feature buttons.  
See Enable Softkey Policy Control, on page 237.                                                                                                                                                                                                                 |
| Softkey Template     | Allows you to manage the softkeys on the Cisco Unified IP Phones.  
See:  
  • *Cisco Unified Communications Manager Administration Guide*  
  • Set Up a Softkey Template, on page 238                                                                                                                                                                                                                           |
### Telephony Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Speed Dial**                  | Allows users to speed dial a phone number by entering an assigned index code (1-99) on the phone keypad. Users assign index codes from the User Options web pages.  
See:  
  - *Cisco Unified Communications Manager Administration Guide*, “Cisco Unified IP Phone Configuration” chapter  
  - *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phone” chapter |
| **sRTP Secure Video**           | The administrator can configure the RTCP authentication tag length for secure video calls.  
  - Native Video supports security, but CUVA has only a nonsecure stream.  
  - For secure video calls, the secure icon displays on phone screen in the top right corner if Picture in Picture (PIP) is not active. When PIP is active, the icon displays in the top left corner.  
  - The RTCP authentication tag length can only be configured for the audio stream. The video stream has a default 80-bit configuration and cannot be configured.  
Configure the 80-bit SRTCP field from the Phone Configuration, Common Phone Profile Configuration, or Enterprise Phone Configuration window in Cisco Unified Communications Manager Administration.  
See *Cisco Unified Communications Manager Administration Guide*. |
| **Support For Hold Button On USB Headsets** | Provides support for USB headsets equipped with a Hold button. Users can put a call on hold using the headset button and retrieve the call using the Resume softkey on their phone. |
| **Time-of-Day Routing**         | Restricts access to specified telephony features by time period.  
See:  
  - *Cisco Unified Communications Manager Administration Guide*, “Time Period Configuration” chapter  
| **Time Zone Update**            | Updates the Cisco Unified IP Phone with time zone changes.  
See *Cisco Unified Communications Manager Administration Guide*, “Date/Time Group Configuration” chapter. |
| **Transfer**                    | Allows users to redirect connected calls from their phones to another number. The user can connect two calls to each other. |
| **Unified Font Size Enhancement** | Allows users to change the font size used for the call history, call session, phone line label and key expansion module line label using a single menu, |
### Uniform Resource Identifier (URI) Dialing

The Uniform Resource Identifier (URI) Dialing feature enables the user to place calls by using an alphanumeric URI address as a directory number, for example, bob@cisco.com. The user must enter the URI address to select the contact.

The phone screen displays the call information for the URI call. The call logs record the URI call information in the Call History and the Details page.

An enhancement allows you to specify the device display preference for calls that have both Directory Number (DN) and URI available.

See:
- Cisco Unified Communications Manager Features and Services Guide
- Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager (SIP)

### Uniform Resource Identifier Dialing Enhancement

Allows you to specify the device display preference for calls that have both Directory Number (DN) and URI available.

If the URI Dialing Display Preference is set to DN then DN is displayed when available. If the URI Dialing Display Preference is set to URI then URI is displayed available.

See:
- Cisco Unified Communications Manager Features and Services Guide
- Cisco Unified IP Phone 8961, 9951, and 9971 User Guide for Cisco Unified Communications Manager (SIP)

### Unique Call ID Display

Ensures that all calls with the same group call ID display the same call ID on all the phones in the group. Displaying the same call ID on all phones ensures that group users can identify the correct active call.

### Unique eBarge Call Instance ID

Enhances eBarge by giving the legs of the call the same Call ID.

### VDI VPN

Provides integrated VPN functionality for Cisco virtual desktop infrastructure (VDI) clients. See Cisco VXC VPN, on page 253.

### Video Mode

Allows a user to select the video display mode for viewing a video conference, depending on the modes that are configured in the system.

See:
- Cisco Unified Communications Manager Administration Guide, "Conference Bridge Configuration" chapter
- Cisco Unified Communications Manager System Guide, "Understanding Video Telephony" chapter
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video Support</td>
<td>Enables video support on the phone.</td>
</tr>
<tr>
<td></td>
<td>See</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager Administration Guide, “Conference Bridge Configuration” chapter</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager System Guide, “Understanding Video Telephony” chapter</td>
</tr>
<tr>
<td></td>
<td>• Cisco VT Advantage Administration Guide, “Overview of Cisco VT Advantage” chapter</td>
</tr>
<tr>
<td>Visual Message Waiting Indicator</td>
<td>A light on the handset that indicates that a user has one or more new voice messages.</td>
</tr>
<tr>
<td></td>
<td>See</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager Administration Guide, “Message Waiting Configuration” chapter</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager System Guide, “Voice Mail Connectivity to Cisco Unified Communications Manager” chapter</td>
</tr>
<tr>
<td>VPN</td>
<td>Using SSL, provides a virtual private network (VPN) connection on the Cisco Unified IP Phone when it is located outside a trusted network or when network traffic between the phone and Unified Communications Manager must cross untrusted networks.</td>
</tr>
<tr>
<td></td>
<td>Note  This VPN is differs from VXC VPN. See the description of Cisco VXC VPN in this table.</td>
</tr>
<tr>
<td>Voice Messaging System</td>
<td>Enables callers to leave messages if calls are unanswered.</td>
</tr>
<tr>
<td></td>
<td>See</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager Administration Guide, “Cisco Voice-Mail Port Configuration” chapter</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager System Guide, “Voice Mail Connectivity to Cisco Unified Communications Manager” chapter</td>
</tr>
</tbody>
</table>

**Feature Buttons and Softkeys**

The following table provides information about features that are available on softkeys, features that are available on dedicated feature buttons, and features that you need to configure as programmable feature buttons. An “X” in the table indicates that the feature is supported for the corresponding button type or softkey. Of the two button types and softkeys, only programmable feature buttons require configuration in Cisco Unified IP Phone administration.
For information about configuring programmable feature buttons, see Phone Button Templates, on page 234. For information about configuring features that can appear as softkeys or programmable buttons, see Create Feature Control Policy, on page 208.

### Table 23: Features and Corresponding Buttons and Softkeys

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Dedicated Feature Button</th>
<th>Programmable Feature Button</th>
<th>Softkey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Calls</td>
<td>X</td>
<td></td>
<td>X (available while on a conference only)</td>
</tr>
<tr>
<td>All Calls</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Answer</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Call Back</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Call Forward All</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Call Park</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Call Park Line Status</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Call Pickup (Pick Up)</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Call Pickup Line Status</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Conference</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Divert</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Do Not Disturb</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Group Pickup (Group Pick Up)</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Hide video</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Show video</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Hold</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Hunt Groups</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Intercom</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Malicious Call Identification (MCID)</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Meet Me</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
### Feature Control Policy

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

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Dedicated Feature Button</th>
<th>Programmable Feature Button</th>
<th>Softkey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Connect (Mobility)</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Mute</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Pickup</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>PLK Support for Queue Status</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Privacy</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Queue Status</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Quality Reporting Tool (QRT)</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Redial</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Speed Dial</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Speed Dial Line Status</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Support for Hold Button on USB Headsets</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Transfer</td>
<td>X</td>
<td></td>
<td>X (available during a transfer only)</td>
</tr>
</tbody>
</table>
Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose Device > Device Settings > Feature Control Policy.

Step 2 Click Add New to define a set of policies.

Step 3 Enter the following settings.

- Name: Enter a name for a new Feature Control Policy
- Description: Enter a description.
- Feature Control Section: Check the check box for the features for which you want to change the default setting.

Step 4 Click Save.

Step 5 Apply the policy to the phone by including it in the following windows:

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

Feature Control Policy Default Values

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

Table 24: Feature Control Policy Default Values

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward All</td>
<td>Enabled</td>
</tr>
<tr>
<td>Park</td>
<td>Disabled</td>
</tr>
<tr>
<td>To Voicemail</td>
<td>Disabled</td>
</tr>
<tr>
<td>Conference List</td>
<td>Enabled</td>
</tr>
<tr>
<td>Speed Dial</td>
<td>Enabled</td>
</tr>
<tr>
<td>Call Back</td>
<td>Enabled</td>
</tr>
<tr>
<td>Redial</td>
<td>Enabled</td>
</tr>
<tr>
<td>Barge</td>
<td>Enabled</td>
</tr>
<tr>
<td>Malicious Caller ID</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
### Disable Speakerphone

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

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

**Procedure**

**Step 1** From Cisco Unified Communications Manager Administration, select Device > Phone.
**Step 2** Select the phone you want to modify.
**Step 3** In the Phone Configuration window for the phone, check the **Disable Speakerphone** check box.
**Step 4** Select **Save**.

### Schedule Power Save for Cisco IP Phone

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

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

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

- Press any button on the phone.
  - The phone takes the action designated by that button in addition to turning on the display.
- Lift the handset.
When you turn the display on, it remains on until the phone has remained idle for a designated length of time, then it turns off automatically.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In Cisco Unified Communications Manager Administration, select <strong>Device &gt; Phone</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Locate the phone that you need to set up.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Navigate to the Product Specific Configuration area and set the following fields:</td>
</tr>
<tr>
<td></td>
<td>• Days Display Not Active</td>
</tr>
<tr>
<td></td>
<td>• Display On Time</td>
</tr>
<tr>
<td></td>
<td>• Display On Duration</td>
</tr>
<tr>
<td></td>
<td>• Display Idle Timeout</td>
</tr>
</tbody>
</table>

**Table 25: PowerSave Configuration Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Days Display Not Active</td>
<td>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.</td>
</tr>
<tr>
<td>Display On Time</td>
<td>Time each day that the display turns on automatically (except on the days specified in the Days Display Not Active field). Enter the time in this field in 24-hour format, where 0:00 is midnight. For example, to automatically turn the display on at 07:00 a.m. (0700), enter <strong>07:00</strong>. To turn the display on at 02:00 p.m. (1400), enter <strong>14:00</strong>. If this field is blank, the display will automatically turn on at 0:00.</td>
</tr>
<tr>
<td>Display On Duration</td>
<td>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 <strong>hours:minutes</strong>. For example, to keep the display on for 4 hours and 30 minutes after it turns on automatically, enter <strong>04:30</strong>. If this field is blank, the phone will turn off at the end of the day (0:00). <strong>Note</strong> If Display On Time is 0:00 and the display on duration is blank (or 24:00), the display will remain on continuously.</td>
</tr>
</tbody>
</table>
Schedule Power Save Plus (EnergyWise) on Cisco IP Phone

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

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

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

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

Procedure

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

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

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

- Enable Power Save Plus
- Phone On Time
- Phone Off Time
- Phone Off Idle Timeout
- Enable Audible Alert

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Idle Timeout</td>
<td>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.</td>
</tr>
</tbody>
</table>
Schedule Power Save Plus (EnergyWise) on Cisco IP Phone

- EnergyWise Domain
- EnergyWise Secret
- Allow EnergyWise Overrides

Table 26: EnergyWise Configuration Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Power Save Plus</td>
<td>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. <strong>Caution</strong> 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. <strong>Note</strong> 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.</td>
</tr>
<tr>
<td>Phone On Time</td>
<td>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. <strong>Note</strong> 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.</td>
</tr>
<tr>
<td>Phone Off Time</td>
<td>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. <strong>Note</strong> 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.</td>
</tr>
</tbody>
</table>
### Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone Off Idle Timeout</td>
<td>The length of time that the phone must be idle before the phone powers down. The timeout occurs under the following conditions:</td>
</tr>
<tr>
<td></td>
<td>• 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 <strong>Select</strong> key.</td>
</tr>
<tr>
<td></td>
<td>• When the phone is repowered by the attached switch.</td>
</tr>
<tr>
<td></td>
<td>• When the Phone Off Time is reached but the phone is in use.</td>
</tr>
<tr>
<td></td>
<td>The range of the field is 20 to 1440 minutes. The default value is 60 minutes.</td>
</tr>
<tr>
<td>Enable Audible Alert</td>
<td>When enabled, instructs the phone to play an audible alert starting 10 minutes before the time that the Phone Off Time field specifies.</td>
</tr>
<tr>
<td></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• At 10 minutes before power down, play the ringtone four times.</td>
</tr>
<tr>
<td></td>
<td>• At 7 minutes before power down, play the ringtone four times.</td>
</tr>
<tr>
<td></td>
<td>• At 4 minutes before power down, play the ringtone four times.</td>
</tr>
<tr>
<td></td>
<td>• At 30 seconds before power down, play the ringtone 15 times or until the phone powers off.</td>
</tr>
<tr>
<td></td>
<td>This check box applies only if the Enable Power Save Plus list box has one or more days selected.</td>
</tr>
<tr>
<td>EnergyWise Domain</td>
<td>The EnergyWise domain that the phone is in. The maximum length of this field is 127 characters.</td>
</tr>
<tr>
<td>EnergyWise Secret</td>
<td>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.</td>
</tr>
</tbody>
</table>
This checkbox 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.

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 receive 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.

---

**Enable Agent Greeting**

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

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

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

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

**Procedure**

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

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

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

**Step 4**
Select Save.

**Step 5**
Check the setting of the bridge:

a) Choose System > Service Parameters.

b) Select the appropriate Server and Service.

c) Scroll to the Clusterwide Parameters (Device - Phone) pane and set Builtin Bridge Enable to On.

d) Select Save.

---

**Set Up the DF Bit**

The Configurable DF Bit feature controls how network packets are sent. Packets can be sent in chunks (fragments) of various sizes. When the DF bit is set to 1 in the packet header, the network payload does not fragment when going through network devices, such as switches and routers. Removing fragmenting avoids incorrect parsing on the receiving side, but results in slightly slower speeds. By default, the DF bit is set to 0.

The DF bit setting does not apply to ICMP, VPN, VXC VPN, or DHCP traffic.
**Set Up Do Not Disturb**

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

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

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

**Procedure**

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

**Step 2** Locate the phone to be configured.

**Step 3** Set the following parameters.

- **Do Not Disturb:** This check box allows you to enable DND on the phone.

- **DND Option:** Ring Off, Call Reject, or Use Common Phone Profile Setting.

- **DND Incoming Call Alert:** Choose the type of alert, if any, to play on a phone for incoming calls when DND is active.

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

**Step 4** Select Save.

**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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In Cisco Unified Communications Manager Administration, select User Management &gt; Application User.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Check the Standard CTI Allow Call Monitoring user group and the Standard CTI Allow Call Recording user groups.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Add Selected.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Add to User Group.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Add the user phones to the list of Application Users controlled devices.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Select Save.</td>
</tr>
</tbody>
</table>

**Set Up Power Negotiation for LLDP**

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

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

The Power Negotiation feature is enabled by default.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the Cisco Unified Communications Manager Administration, select Device &gt; Phone.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Locate the phone that you need to set up.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Product Specific Configuration area, set the Power Negotiation parameter.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select Save.</td>
</tr>
</tbody>
</table>
Set Up RTCP Control

Configure the RTCP for video parameter from the Phone Configuration or Common Phone Profile Configuration window in Cisco Unified Communications Manager Administration.

**Note**

By default, RTCP is turned on.

**Procedure**

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

- Device > Device Settings > Common Phone Profile
- Device > Phone

**Step 2** Configure the RTCP for Video parameter.

Set Up Simplified New Call Window

The Simplified New Call Window feature provides a new user interface for off-hook dialing. It is disabled by default.

The Simplified New Call Window does not allow the user to select a number from the call history.

**Procedure**

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

**Step 2** Set the Simplified New Call UI field to Enabled.

Set Up Automatic Port Synchronization

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

**Procedure**

**Step 1** To configure Automatic Port Synchronization for a single phone,

a) In the Cisco Unified Communications Manager Administration application, choose Device > Phone

b) Locate the phone.

c) In the Product Specific Configuration Layout pane, set the Automatic Port Synchronization parameter.
To configure Automatic Port Synchronization for a group of phones,

a) In the Cisco Unified Communications Manager Administration application, choose System > Enterprise Phone Configuration.

b) Set the Automatic Port Synchronization parameter.

c) Select Save.

---

## Set Up Bluetooth Profiles

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

**Procedure**

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

**Step 2**
Find your phone from the list of phones that display in Cisco Unified Communications Manager.

**Step 3**
Click on the Device Name of the phone.
The Phone Configuration window appears.

**Step 4**
Go to the Product Specific Configuration Layout area and from the Bluetooth Profiles drop-down list, choose the applicable profile.
The Handsfree profile is selected by default.

**Step 5**
Check the Override Common Settings check box for any setting in the Product Specific Configuration area that you wish to update.

- If you do not check this check box, the corresponding parameter setting does not take effect.

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

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

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

---

## Set Up SSH Access

You can enable or disable access to the SSH daemon through port 22. Leaving port 22 open leaves the phone vulnerable to Denial of Service (DoS) attacks. By default, the SSH daemon is disabled.
The SSH Access parameter is disabled by default. You must enable the SSH Access parameter before users of these phones can use SSH.

**Procedure**

**Step 1** In Cisco Unified Communications Manager Administration, choose one of the following windows:
- Device > Device Settings > Common Phone Profile
- Device > Phone > Phone Configuration

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

**Step 2** Select the appropriate phones.

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

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

---

### Set Up Call Forward Notification

You can control the call forward settings.

**Procedure**

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

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caller Name</td>
<td>When this check box is checked, the caller name displays in the notification window. By default, this check box is checked.</td>
</tr>
<tr>
<td>Caller Number</td>
<td>When this check box is checked, the caller number displays in the notification window. By default, this check box is not checked.</td>
</tr>
<tr>
<td>Redirected Number</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Dialled 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**.

---

### Client Matter Codes and Forced Authorization Codes

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

- **CMC**—forces users to identify the reason for the call.
- **FAC**—controls the ability for a user to dial a number.

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

### Enable BLF for Call Lists

**Procedure**

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

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

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

**Step 3** Select **Save**.
Set Up Dual Bank Information

To set up Dual Bank Information, follow these steps:

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In Cisco Unified Communications Manager Administration, choose <strong>Device &gt; Device Defaults</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Check the load information in the Inactive Load Information field.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose <strong>Bulk Administration &gt; Import/Export &gt; Export &gt; Device Defaults</strong>, and schedule an export job.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Download the exported tar file and untar it.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Check the file format in the exported CSV file and verify that the CSV file has an Inactive Load Information column with the correct value.</td>
</tr>
</tbody>
</table>

**Note** The CSV file value must match the Device Default value in the Cisco Unified Communications Manager Administration window.

Set Up Incoming Call Toast Timer

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

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In Cisco Unified Communications Manager Administration, select one of the following windows:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>Device &gt; Phone</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Device &gt; Device Settings &gt; Common Phone Profile</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>System &gt; Enterprise Phone Configuration</strong></td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Step 2</th>
<th>If required, locate the phone.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>Set the Incoming Call Toast Timer field.</td>
</tr>
</tbody>
</table>
Incoming Call Toast Timer

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

Step 4
Select Save.

Set Up Peer Firmware Sharing

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

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

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

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

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

- Enabled, which is the default value.
- Disabled

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

Procedure

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

Step 2
Find your phone from the list of phones that associate with the Cisco Unified Communications Manager.

Step 3
Click on the Device Name of the phone.

Step 4
Go to Product Specific Configuration Layout area and select Enable from the Peer Firmware Sharing drop-down list.
The Peer Firmware Sharing is enabled by default.
Step 5  Check the Override Common Settings check box for any setting in the Product Specific Configuration area that you wish to update.

- If you do not check this check box, the corresponding parameter setting does not take effect.
- Parameters that you set in the Product Specific Configuration area may also appear in the Phone Configuration window for various devices and in the Enterprise Phone Configuration window.

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

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

Step 6  Select Save.

Set Up Remote Port Configuration

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

Procedure

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

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

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

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

Set Headset Sidetone Control

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

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

**Procedure**

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

**Step 2** Find your phone from the list of phones.

**Step 3** Click on the Device Name of the phone.

**Step 4** Go to Product Specific Configuration Layout area and from the Wideband Headset UI Control drop-down list box, choose the applicable profile. The Off option is selected by default (should be enabled only if the user headset supports wideband).

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

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

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

**Step 5** Select **Save**.

---

**Enable Device Invoked Recording**

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

**Procedure**

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

**Step 2** Set Recording Option to **Selective Call Recording Enabled**.

**Step 3** Select the appropriate Recording Profile.
Set Up Enable Video On/Off

The Enable Video On/Off setting improves the video conference call flow by removing the black box that is displayed when one party has the Auto Transmit setting on their phone set to Off.

This setting works in conjunction with Auto Transmit. If the Enable Video feature is set to Off, it overrides the Auto Transmit setting and you can send audio calls. But if Enable Video is set to On and Auto Transmit is set to Off, the video stream is blocked and the user sends a black box to the other party. For this feature to function, Cisco recommends Auto Transmit remains On.

The Enable Video On/Off setting functions like Video Capability: Enable/Disable on Cisco Unified Communications Manager (Unified CM). However, the server settings override the phone settings so if video is disabled on the Unified CM, this feature is not available on the phone and all calls are audio only.

Procedure
to be added

Set Up Dial Tone from Release Button

You can provide users with one-button access to the dial tone and the New Call window from an active call. The following table describes the field for the Dial Tone from Release button feature.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide Dial Tone from Release Key</td>
<td>Identifies if pressing the Release key causes the user to hear dial tone (Enabled) or not (Disabled). The possible values are Disabled or Enabled. The default is Disabled</td>
</tr>
</tbody>
</table>

Procedure

Step 1 In Cisco Unified Communications Manager Administration, navigate to one of the following windows:

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

Step 2 Set the Provide Dial Tone from Release Key field.
Park Monitoring

Park monitoring is supported only when a Cisco Unified IP Phone 8961, 9951, or 9971 parks a call. Park monitoring then monitors the status of a parked call. The park monitoring call bubble does not clear until the parked call gets retrieved or is abandoned by the parked call. This parked call can be retrieved by using the same call bubble on the phone that parked the call.

Set Up Park Monitoring Timers

Cisco Unified Communications Manager Administration provides three cluster-wide service timer parameters for park monitoring: Park Monitoring Reversion Timer, Park Monitoring Periodic Reversion Timer, and Park Monitoring Forward No Retrieve Timer. Each service parameter includes a default and requires no special configuration. These timer parameters are for park monitoring only; the Call Park Display Timer and Call Park Reversion Timer are not used for park monitoring. See the following table for descriptions of these parameters.

Configure the timers in the Cisco Unified Communications Manager Service Parameters page.

Procedure

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

Step 2
Update the Park Monitoring Reversion Timer, Park Monitoring Periodic Reversion Timer, and Park Monitoring Forward No Retrieve Timer fields in the Clusterwide Parameters (Feature-General) pane.

Table 27: Service Parameters for Park Monitoring

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Park Monitoring Reversion Timer</td>
<td>Default is 60 seconds. This parameter determines the number of seconds that Cisco Unified Communications Manager waits before prompting the user to retrieve a call that the user parked. This timer starts when the user presses Park on the phone, and a reminder is issued when the timer expires. You can override the value that this service parameter specifies on a per-line basis in the Park Monitoring section of the Directory Number Configuration window (in Cisco Unified Communications Manager Administration, choose Call Routing &gt; Directory Number). Specify a value of 0 to immediately utilize the periodic reversion interval that the Park Monitoring Periodic Reversion Timer service parameter specifies. (See the description that follows.) For example, if this parameter is set to zero and the Park Monitoring Periodic Reversion Timer is set to 15, the user is immediately prompted about the parked call and every 15 seconds thereafter until the Park Monitoring Forward No Retrieve Timer (see the description that follows) expires.</td>
</tr>
</tbody>
</table>
**Field** | **Description**
--- | ---
Park Monitoring Periodic Reversion Timer | Default is 30 seconds. This parameter determines the interval (in seconds) that Cisco Unified Communications Manager waits before prompting the user again that a call is parked. To connect to the parked call, the user can simply go off-hook during one of these prompts. Cisco Unified Communications Manager continues to prompt the user about the parked call as long as the call remains parked and until the time that the Park Monitoring Forward No Retrieve Timer (see the description that follows) specifies expires. Specify a value of 0 to disable periodic prompts about the parked call.

Park Monitoring Forward No Retrieve Timer | Default is 300 seconds. This parameter determines the number of seconds that park reminder notifications occur before the parked call forwards to the Park Monitoring Forward No Retrieve destination that is specified in the parker Directory Number Configuration window. (If no forward destination is provided in Cisco Unified Communications Manager Administration, the call returns to the line that parked the call.) This parameter starts when the time that the Park Monitoring Reversion Timer service parameter specifies expires. When the Park Monitoring Forward No Retrieve Timer expires, the call is removed from park and forwards to the specified destination or returns to the parker line.

---

**Set Park Monitoring Parameters for Directory Numbers**

The Directory Number Configuration window contains a Park Monitoring area where you can configure the three parameters.

**Procedure**

**Step 1**
In Cisco Unified Communications Manager Administration, choose **Call Routing > Directory Number**.

**Step 2**
Set the park monitoring fields as described in the following table.

**Table 28: Park Monitoring Parameters**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Park Monitoring Forward No Retrieve Destination External</td>
<td>When the parkee is an external party, the call forwards to the specified destination in the parker Park Monitoring Forward No Retrieve Destination External parameter. If the Forward No Retrieve Destination External field value is empty, the parkee is redirected to the parker line.</td>
</tr>
<tr>
<td>Park Monitoring Forward No Retrieve Destination Internal</td>
<td>When the parkee is an internal party, the call forwards to the specified destination in the parker’s Park Monitoring Forward No Retrieve Destination Internal parameter. If the Forward No Retrieve Destination Internal is empty, the parkee is redirected to the parker line.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Park Monitoring Reversion Timer</td>
<td>This parameter determines the number of seconds that Cisco Unified Communications Manager waits before prompting the user to retrieve a call that the user parked. This timer starts when the user presses Park on the phone, and a reminder is issued when the timer expires. Default: 60 seconds If you configure a nonzero value, this value overrides the value of this parameter set in the Service Parameters window. However, if you configure a value of 0 here, then the value in the Service Parameters window is used.</td>
</tr>
</tbody>
</table>

**Set Up Park Monitoring for Hunt Lists**

When a call that was routed via the hunt list is parked, the Hunt Pilot Park Monitoring Forward No Retrieve Destination parameter value is used (unless it is blank) when the Park Monitoring Forward No Retrieve Timer expires.

**Procedure**

**Step 1** In Cisco Unified Communications Manager Administration, choose Call Routing > Route/Hunt > Hunt Pilot.

**Step 2** Set the Hunt Pilot Park Monitoring Forward No Retrieve Destination parameter. If the Hunt Pilot Park Monitoring Forward No Retrieve Destination parameter value is blank, the call forwards to the destination that is configured in the Directory Number Configuration window when the Park Monitoring Forward No Retrieve Timer expires.

**Enable Actionable Incoming Call Alert**

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

**Note**

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

**Procedure**

**Step 1** Go to Cisco Unified Communications Manager Administration and choose one of the following:
Enable the Call History Display Enhancement

**Procedure**

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

**Step 2** Find your phone from the list of phones associated with the Cisco Unified Communications Manager.

**Step 3** Click on the Device Name of the phone.

The Phone Configuration window appears.

**Step 4** Go to Product Specific Configuration Layout area and from the Logging Display drop-down list box, choose **Enable**.

The Disabled option is selected by default.

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

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

1. Device Configuration window settings
2. Common Phone Profile window settings
3. Enterprise Phone Configuration window settings
Enable Call History for Shared Line

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

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Go to Cisco Unified Communications Manager Administration and choose Device &gt; Phone.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Find your phone from the list of phones associated with the Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click on the Device Name of the phone.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Go to Product Specific Configuration Layout area and from the Logging Display drop-down list box, choose the applicable profile. The Disabled option is selected by default. Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window. If you set these same parameters in these other windows as well, the setting that takes precedence is determined in the following order:</td>
</tr>
<tr>
<td>1</td>
<td>Device Configuration window settings</td>
</tr>
<tr>
<td>2</td>
<td>Common Phone Profile window settings</td>
</tr>
<tr>
<td>3</td>
<td>Enterprise Phone Configuration window settings</td>
</tr>
</tbody>
</table>

Set Up the Default Line Filter

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Go to Cisco Unified Communications Manager Administration and choose Device &gt; Phone.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Locate the Default Line Filter field and enter the line DN. Separate device name entries with a comma. The specified line is added to the default filter.</td>
</tr>
</tbody>
</table>

Set Up Custom Line Filter

The Custom Line Filter feature provides configurable options that help reduce alert activity by filtering it to high-priority lines as desired. Only you can configure or edit the default phone filter.
When the default line filter is configured, a filter named Daily schedule is available to users under the Call notifications options in the Settings > Preferences menu of the phone. This daily schedule filter is in addition to the preset All Calls filter.

If the default line filter is not configured, the phone checks all provisioned lines. If configured, the phone checks the lines set on Cisco Unified Communications Manager if the user selects Default filter as the active filter, or if there are no custom filters.

**Procedure**

**Step 1** In Cisco Unified Communications Manager Administration, choose Device > Phone.  
**Step 2** Set the Default line filter field.  
A comma-separated list of phone device names to be included in the default filter.  
By default, the list is blank, and all provisioned lines are checked.

---

**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.
Assign Phone Button Template for All Calls

Assign an All Calls button in the phone template for users with multiple shared lines. When you configure an All Calls button on the phone, users use the All Calls button to:

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

Procedure

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

Set Up PAB or Speed Dial as IP Phone Service

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

Modify Phone Button Template for PAB or Fast Dial

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

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

Procedure

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

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

Note

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

Procedure

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

Related Topics

Access Web Page for Phone, on page 284

Enable Softkey Policy Control

Softkey Policy Control enables you to configure the following features as softkeys or programmable feature buttons:

- Malicious Caller ID
- Pick Up
- Group Pick Up
- Other Pick Up
- Meet Me
- Quality Reporting Tool
- Mobility

For more information, see:
Set Up a Softkey Template

Using Cisco Unified Communications Manager Administration, you can associate a maximum of 18 softkeys with applications that are supported by the phone. Cisco Unified Communications Manager supports the Standard User and Standard Feature softkey template.

An application that supports softkeys has one or more standard softkey templates associated with it. You modify a standard softkey template by copying it, renaming it, and then updating the new template. You can also modify a nonstandard softkey template.

The Softkey Control parameter shows if softkeys of a phone are controlled by the Feature Control Policy or the Softkey Template feature. The Softkey Control parameter is a required field.

The default is Feature Control Policy.

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

The Cisco Unified IP Phones do not support all the softkeys that are configurable in Softkey Template Configuration on Cisco Unified Communications Manager Administration. Cisco Unified Communications Manager allows you to enable or disable some softkeys in the control policy configuration settings. The following table lists the features and the softkeys that can be configured on a softkey template, and identifies whether it is supported on the Cisco Unified IP Phones.

| Note | Cisco Unified Communications Manager allows you to configure any softkey in a softkey template, but unsupported softkeys do not display on the phone. |
### Table 29: Configurable Softkeys

<table>
<thead>
<tr>
<th>Feature</th>
<th>Configurable Softkeys in the Softkey Template configuration</th>
<th>Supported as a Softkey on Cisco Unified IP Phone 8961, 9951 and 9971</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Answer</td>
<td>Answer (Answer)</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>Call Back</td>
<td>Call Back (CallBack)</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>Call Forward All</td>
<td>Forward All (cfwdAll)</td>
<td>Yes</td>
<td>Phone displays Forward All or Forward Off.</td>
</tr>
<tr>
<td>Call Park</td>
<td>Call Park (Park)</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>Call Pickup</td>
<td>Pick Up (Pickup)</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>cBarge</td>
<td>Conference Barge (cBarge)</td>
<td>Yes</td>
<td>Both Barge and cBarge are supported. But only one will be displayed on the phone.</td>
</tr>
<tr>
<td>Conference</td>
<td>Conference (Confrn)</td>
<td>Yes</td>
<td>Conference is a dedicated button.</td>
</tr>
<tr>
<td>Conference List</td>
<td>Conference List (ConfList)</td>
<td>Yes</td>
<td>Phone displays Show Detail.</td>
</tr>
<tr>
<td>Divert</td>
<td>Immediate Divert (iDivert)</td>
<td>Yes</td>
<td>Phone displays Divert.</td>
</tr>
<tr>
<td>Do Not Disturb</td>
<td>Toggle Do Not Disturb (DND)</td>
<td>Yes</td>
<td>Configure Do Not Disturb as a programmable line button or as a softkey.</td>
</tr>
<tr>
<td>End Call</td>
<td>End Call (EndCall)</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>Group Pickup</td>
<td>Group Pick UP (GPickUp)</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>Hold</td>
<td>Hold (Hold)</td>
<td>No</td>
<td>Hold is a dedicated button.</td>
</tr>
<tr>
<td>Hunt Group</td>
<td>HLog (HLog)</td>
<td>Yes</td>
<td>Configure Hunt Group as a programmable feature button.</td>
</tr>
<tr>
<td>Join</td>
<td>Join (Join)</td>
<td>No</td>
<td>—</td>
</tr>
<tr>
<td>Malicious Call Identification</td>
<td>Toggle Malicious Call Identification (MCID)</td>
<td>Yes</td>
<td>Configure Malicious Call Identification as a programmable feature button or as a softkey.</td>
</tr>
<tr>
<td>Meet Me</td>
<td>Meet Me (MeetMe)</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>Feature</td>
<td>Configurable Softkeys in the Softkey Template configuration</td>
<td>Supported as a Softkey on Cisco Unified IP Phone 8961, 9951 and 9971</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>---------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mobile Connect</td>
<td>Mobility (Mobility)</td>
<td>Yes</td>
<td>Configure Mobile Connect as a softkey.</td>
</tr>
<tr>
<td>New Call</td>
<td>New Call (NewCall)</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>Other Pickup</td>
<td>Other Pickup (oPickup)</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>PLK Support for Queue Statistics</td>
<td>Queue Status</td>
<td>No</td>
<td>—</td>
</tr>
<tr>
<td>Quality Reporting Tool</td>
<td>Quality Reporting Tool (QRT)</td>
<td>Yes</td>
<td>Configure Quality Reporting Tool as a programmable feature button or as a softkey.</td>
</tr>
<tr>
<td>Redial</td>
<td>Redial (Redial)</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>Remove Last Conference Participant</td>
<td>Remove Last Conference Participant (Remove)</td>
<td>No</td>
<td>—</td>
</tr>
<tr>
<td>Resume</td>
<td>Resume (Resume)</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>Select</td>
<td>Select (Select)</td>
<td>No</td>
<td>—</td>
</tr>
<tr>
<td>Speed Dial</td>
<td>Abbreviated Dial (AbbrDial)</td>
<td>Yes</td>
<td>Phone displays SpeedDial.</td>
</tr>
<tr>
<td>Transfer</td>
<td>Direct Transfer (DirTrfr)</td>
<td>Yes</td>
<td>Transfer is a dedicated button. Configure transfer (Direct Transfer policy) in the Product Specific Configuration Layout section in Phone Configuration.</td>
</tr>
<tr>
<td>Video Mode Command</td>
<td>Video Mode Command (VidMode)</td>
<td>No</td>
<td>—</td>
</tr>
</tbody>
</table>

Cisco IP Manager Assistant (IPMA) provides additional softkeys that can be controlled by the softkey template. For information on the IPMA softkeys, see Set Up Cisco IP Manager Assistant, on page 244.
Set Up Separate Audio and Video Mute

You can control the ability of your users to mute the audio on a call.

**Procedure**

- **Step 1**  In Cisco Unified Communications Manager Administration, select **System > Enterprise Phone Configuration**.
- **Step 2**  To enable the feature, set the Separate Audio and Video parameter to **Enabled**.
- **Step 3**  Select **Save**.

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 49152 to 53247
used for local ephemeral ports

port range 53248 to 65535
used for the VxC single tunnel VPN feature

Step 5  Click Save.
Step 6  Click Apply Config.

Set Up TLS Resumption Timer

TLS Session resumption enables a TLS session to resume without repeating the entire TLS authentication process. It can significantly reduce the time taken for TLS connection to exchange data.

Although the phones support TLS sessions, all TLS sessions do not support TLS resumption. The following list describes the different sessions and TLS resumption support:

- TLS session for SIP signaling: supports resumption
- HTTPs client: supports resumption
- CAPF: supports resumption
- TVS: supports resumption
- EAP-TLS: does not support resumption
- EAP-FAST: does not support resumption
- VPN client: does not support resumption

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

Procedure

Step 1  In Cisco Unified Communications Manager Administration, select Device > Phone.
Step 2  Set the TLS Resumption Timer parameter.
        The range for the timer is 0 to 3600 sec. The default value is 3600. If the field is set to 0, then TLS session resumption is disabled.

Set Up the Audio and Video Port Range

Audio and video traffic can be sent to different RTP port ranges in order to improve Quality of Service (QoS).

The following fields control the port ranges in the Cisco Unified Communications Manager Administration:
• Audio ports
  • Start Media Port (default: 16384)
  • Stop Media Port (default: 32766)

• Video ports
  • Start Video RTP Port
  • Stop Video RTP Port

The following rules apply when configuring the video port fields:
After the Start Video RTP Port and Stop Video RTP Port are configured, the phone uses ports within the video port range for video traffic. The audio traffic uses the media ports.
If the audio and video port ranges overlap, the overlapped ports carry both audio and video traffic. If the video port range is not configured correctly, the phone uses the configured audio ports for both audio and video traffic.
For more information, see the documentation for your particular Cisco Unified Communications Manager release.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, select Device > Device Settings > SIP Profile
Step 2 Set the Start Media Port and Stop Media Port fields for the audio port range.
  Audio ports can be configured to use ports 16384 to 32766.
Step 3 Select Save.
Step 4 Select one of the following windows:
  • System > Enterprise Phone Configuration
  • Device > Device Settings > Common Phone Profile
  • Device > Phone > Phone Configuration
Step 5 Set the Start Video RTP Port and Stop Video RTP Port fields for the range of ports required.
The following rules apply when configuring the video port fields:
  • Each field must contain a number between 2048 and 65535.
  • The value in the Stop Video RTP Port field must be larger than the value in the Start Video RTP Port field.
  • The difference between the Start Video RTP Port field and the Stop Video RTP Port field must be at least 16.
Step 6 Select Save.
Set Up Cisco IP Manager Assistant

Cisco IP Manager Assistant (IPMA) provides call routing and other call management features to help managers and assistants handle phone calls more effectively.

IPMA services must be configured in Cisco Unified Communications Manager before users can access them. For detailed information on configuring IPMA, see the documentation for your particular Cisco Unified Communications Manager release.

IPMA has three key components:

Manager
A manager is the user whose incoming calls are intercepted by the call routing service.

Assistant
An assistant is the user who handles calls on behalf of a manager.

Assistant Console
The assistant console is a desktop application that can be used by assistants to perform tasks and manage most features.

IPMA supports two modes of operation: proxy line support and shared line support. Both modes support multiple calls per line for the manager. The IPMA service supports both proxy line and shared line support in a cluster.

In shared-line mode, the manager and assistant share a directory number and calls are handled on the shared line. Both the manager phone and the assistant phone ring when a call is received on the shared line. Shared-line mode does not support default assistant selection, assistant watch, call filtering or divert all calls.

If you configure Cisco IPMA in shared-line mode, the manager and assistant share a directory number; for example, 1701. The assistant handles calls for a manager on the shared directory number. When a manager receives a call on directory number 1701, both the manager phone and the assistant phone rings.

Not all IPMA features are available in shared-line mode including default assistant selection, assistant watch, call filtering, and divert all calls. An assistant cannot see or access these features on the Assistant Console application. The assistant phone does not have the softkey for the divert all feature. The manager phone does not have the softkeys for assistant watch, call intercept, or divert all feature.

In order to access shared-line support on user devices, you must first use Cisco Unified Communications Manager Administration to configure and start the Cisco IP Manager Assistant service.

In proxy-line mode, the assistant handles calls on behalf of a manager using a proxy number. Proxy-line mode supports all IPMA features.

When you configure Cisco IPMA in proxy-line mode, the manager and assistant do not share a directory number. The assistant handles calls for a manager using a proxy number. The proxy number is not the directory number for the manager, but an alternate number chosen by the system and that an assistant uses to handle manager calls. In proxy-line mode, a manager and an assistant have access to all features that are available in IPMA, which include default assistant selection, assistant watch, call filtering, and divert all.
In order to access proxy-line support on user devices, you must first use Cisco Unified Communications Manager Administration to configure and start the Cisco IP Manager Assistant service.

IPMA features are accessed by softkeys and through Phone Services. The softkey template is configured in Cisco Unified Communications Manager. IPMA supports the following standard softkey templates:

**Standard Manager**
- Supports manager for proxy mode.

**Standard Shared Mode Manager**
- Supports manager for shared mode.

**Standard Assistant**
- Supports assistant in proxy or in shared mode.

The following table describes the softkeys available in the softkey templates.

<table>
<thead>
<tr>
<th>Softkey</th>
<th>Call State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirect</td>
<td>Ringing, Connected, OnHold</td>
<td>Divert the selected call to a preconfigured target.</td>
</tr>
<tr>
<td>Intercept</td>
<td>All states</td>
<td>Divert a call from the assistant's phone to the manager's phone and autoanswer it.</td>
</tr>
<tr>
<td>Set Watch</td>
<td>All states</td>
<td>View the status of call being handled by an assistant.</td>
</tr>
<tr>
<td>TransVM</td>
<td>Ringing, Connected, OnHold</td>
<td>Redirect the selected call to the manager's voice mail.</td>
</tr>
<tr>
<td>Divert All</td>
<td>All states</td>
<td>Divert all calls that are routed to the manager to a preconfigured target.</td>
</tr>
</tbody>
</table>

**Note**

Intercept, Set Watch, and Divert All should only be configured for a manager phone in proxy line mode.

The following procedure is an overview of the steps required. For detailed instructions, see the documentation for your particular Cisco Unified Communications Manager release.
Procedure

Step 1  Configure the phones and users.
Step 2  Associate the phones to the users.
Step 3  Activate the Cisco IP Manager Assistant service in the Service Activation window.
Step 4  Configure system administration parameters.
Step 5  If required, configure IPMA clusterwide services parameters.
Step 6  (Optional) Configure the user CAPF profile
Step 7  (Optional) Configure the IPMA service parameters for security
Step 8  Stop and restart the IPMA service.
Step 9  Configure phone parameter, manager, and assistant settings, including the softkey templates.
Step 10 Configure Cisco Unified Communications Manager Assistant application.
Step 11 Configure dial rules.
Step 12 Install the Assistant Console application.
Step 13 Configure the manager and assistant console applications.

Enable Privacy Settings

You can control the information displayed on the assistant phone and in the assistant phone log for private manager calls using the parameters: Show Remote Private Calls and Record Call Log for Remote Private Calls.

When Privacy is turned on for the manager phone and the Show Remote Private Calls is enabled on the assistant, the assistant phone shows “Private” instead of the caller information for private calls on the manager phone. When Privacy is turned on for the manager phone and the Show Remote Private Calls is disabled on the assistant phone, the assistant phone does not display any call session information about private calls on the manager phone. In this case, the assistant phone displays the solid red LED for the shared line.

By default, Show Remote Private Calls is disabled.

When Privacy is turned on for a call and Record Call Log for Remote Private Calls are enabled, the call log for the assistant phone shows the call information for the private call on the manager phone. When Privacy is turned on for a call and Record Call Log for Remote Private Calls is disabled, the call log for the assistant phone does not store call information for private calls on the manager phone.

Procedure

Step 1  In the Cisco Unified Communications Manager Administration window, select Device > Phone.
Step 2  To show “Private” on the manager's private call on an assistant phone, enable the Show Remote Private Calls field for the assistant phone.
Step 3  To log a manager's private calls on an assistant phone, enable Record Call Log for Remove Private Calls for the assistant phone.
Step 4  Click Save.
Set Up Audio EQ

Procedure

Step 1  In the Cisco Unified Communications Manager Administration window, select Device > Phone.
Step 2  Scroll to the Audio EQ field and select the appropriate setting from the list. The Audio EQ field supports the following settings:

- Default:Default
- Default:Low Bass/High Treble
- Default:Low Bass/High Mid/High Treble
- Open Space:Default
- Open Space:Low Bass/High Treble
- Open Space:Low Bass/High Mid/High Treble

In the above pairs, the left element is for handsfree and the right element is for the handset.

Step 3  Click Save.

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.

Procedure

Step 1  Using 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.
Corporate and Personal Directory Setup

• Corporate Directory Setup, page 249
• Personal Directory Setup, page 249
• User Personal Directory Entries Setup, page 250

Corporate Directory Setup

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

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

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

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

Personal Directory Setup

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

Personal Directory consists of the following features:

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

Users can use these methods to access Personal Directory features:

• From a web browser: Users can access the PAB and Speed Dials features from the Cisco Unified Communications Self Care Portal.
From the Cisco IP Phone: Choose Contacts to search the corporate directory or the user personal directory.

From a Microsoft Windows application: Users can use the 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 250 and Set Up Synchronizer, on page 251.

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 99 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 250.

Download Cisco IP Phone Address Book Synchronizer

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

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>To obtain the installer, choose Application &gt; Plugins from Cisco Unified Communications Manager Administration.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select Download, which is located next to the Cisco IP Phone Address Book Synchronizer plugin name.</td>
</tr>
<tr>
<td>Step 3</td>
<td>When the file download dialog box displays, select Save.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Send the TabSyncInstall.exe file and the instructions in Cisco IP Phone Address Book Synchronizer Deployment, on page 250 to all users who require this application.</td>
</tr>
</tbody>
</table>

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.
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**

1. **Step 1** Get the Cisco IP Phone Address Book Synchronizer installer file from your system administrator.
2. **Step 2** Double-click the TabSyncInstall.exe file that your administrator provided.
3. **Step 3** Select **Run**.
4. **Step 4** Select **Next**.
5. **Step 5** Read the license agreement information, and select the **I Accept**. Select **Next**.
6. **Step 6** Choose the directory in which you want to install the application and select **Next**.
7. **Step 7** Select **Install**.
8. **Step 8** Select **Finish**.
9. **Step 9** To complete the process, follow the steps in **Set Up Synchronizer**, on page 251.

**Set Up Synchronizer**

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

**Procedure**

1. **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**.
2. **Step 2** To configure user information, select **User**.
3. **Step 3** Enter the Cisco IP Phone user name and password and select **OK**.
4. **Step 4** To configure Cisco Unified Communications Manager server information, select **Server**.
5. **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.
6. **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.
Cisco VXC VPN

- Cisco VXC Requirements, page 253
- Set Up Cisco VXC VPN, page 255
- Cisco VXC VPN Limitations and Restrictions, page 259

Cisco VXC Requirements

The Cisco VXC VPN feature provides integrated VPN functionality for Cisco Virtualization Experience Clients (Cisco VXC) 2111 and 2112. The feature enables VPN tunneling for the Cisco VXC 2111 and Cisco VXC 2112 clients when they attach to a Cisco Unified IP Phone 8961, 9951, or 9971.

You can set up the Cisco VXC VPN and the phone VPN to use the same tunnel or separate tunnels in the following configurations:

- One tunnel for both Cisco VXC VPN traffic and phone VPN traffic
- Two tunnels that use the same access credentials (one for Cisco VXC VPN traffic and another for phone VPN traffic)
- Two tunnels that use different access credentials (one for Cisco VXC VPN traffic and another for phone VPN traffic). This configuration is only supported when a one-time password is applied.

You can configure the feature to prompt the user only once for access credentials (in the Phone VPN Sign In window), or once each for the phone VPN (in the Phone VPN Sign In window) and for the Cisco VXC VPN (in the VXC VPN Sign In window).

Cisco VXC Firmware

To support the VXC VPN feature, the Cisco VXC clients must be running the following minimum firmware releases:

- Cisco VXC 2112: ICA Firmware Release 7.1_118
- Cisco VXC 2111: PCoIP Firmware Release 4.0 (Q3CY12)
Cisco Unified Communications Manager for Cisco VXC VPN

The following Cisco Unified Communications Manager configuration is required to support the Cisco VXC VPN:

**PC Port Enabled**

You must set the PC Port to Enabled. If the PC port is disabled, the Cisco VXC cannot access the network. The phone provides no enforcement of this configuration.

**Span to PC Port Disabled**

You must set the Span to PC Port option to Disabled. The Cisco VXC does not require this feature.

You can set the preceding parameters in Cisco Unified Communications Manager Administration by using any of the following configuration windows:

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

VPN Concentrator for Cisco VXC VPN

The recommended VPN concentrator for use with this feature is the Cisco ASA 5500 Series Adaptive Security Appliance. To support the Cisco VXC VPN, you must set up the ASA for multisession support so that the phone can establish two tunnels that use the same credentials.

Network Guidelines for Cisco VXC VPN

The following network guidelines exist for the Cisco VXC VPN feature implementation:

- The MTU size in the phone VPN profile is a configurable value. The default value is 1290.
- The maximum MTU value on the phone itself is hardcoded at 1406.
- The MTU value must be no greater than 1406, but it should not be less than 576, because some IIS and virtualization servers do not accept values less than 576.
- You must set up the firewall to allow the MTU value that you specify in the phone VPN profile.
- If the phone cannot download the certificate file or the phone configuration file, check for the allowed packet size in the network.
- If the Cisco VXC VPN cannot establish a tunnel, then ping the VPN concentrator IP address with a packet size (load) to match the MTU value that the VPN profile specifies.
- If the ping fails, try another ping that specifies no load. If the ping still fails without the load, check the routing configuration.
- If the ping fails only with the load included, check the firewall to ensure that it is configured to allow the required MTU.
- Perform a traceroute to the VPN concentrator IP address, and then ping each route with the load to determine the source of the issue.
• Ensure the Don’t Fragment (DF) bit is not set on the server, network, or IP phone VPN tunnel.

Set Up Cisco VXC VPN

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

Note

The Cisco VXC clients require no configuration to support the VPN. All VPN configuration is performed for the phone only.

Procedure

Step 1
To set up the Cisco VXC VPN feature, set up the VPN feature for the attached IP phone in Cisco Unified Communications Manager Administration. Use the submenus in Advanced Features > VPN.

Step 2
To enable the Cisco VXC VPN feature, populate the Enable VXC VPN for MAC field using one of the following configuration windows:

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

Cisco VXC VPN Descriptions

The following table describes the Cisco VXC VPN fields.
### Table 31: Cisco VXC VPN Fields

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Parameter Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable VXC VPN for MAC</td>
<td>This field enables or disables the Cisco VXC VPN feature. When you populate this field, the phone allows traffic from the device with the specified MAC address and that connects to the phone PC Port to access the tunnel.</td>
</tr>
<tr>
<td></td>
<td>• When this field is blank, the phone does not establish a Cisco VXC VPN tunnel.</td>
</tr>
<tr>
<td></td>
<td>• When this field specifies one broadcast MAC address (FFFFFFFFFFFF), the phone establishes the Cisco VXC VPN tunnel and allows any connected Cisco VXC 2111/2112 device to access the tunnel.</td>
</tr>
<tr>
<td></td>
<td>• When this field specifies one nonbroadcast MAC address, the phone establishes the Cisco VXC VPN tunnel and allows only the Cisco VXC device with the specified MAC address to access the tunnel.</td>
</tr>
<tr>
<td></td>
<td>By default, this field is blank.</td>
</tr>
<tr>
<td>VXC VPN Option</td>
<td>This field indicates the type of VXC VPN support.</td>
</tr>
<tr>
<td></td>
<td>• Dual Tunnel: The phone establishes two VPN tunnels, one for the phone and another for the Cisco VXC device. To ensure the highest quality of service for the phone voice and video services, Cisco recommends the Dual Tunnel setting, which is the default setting. With two VPN tunnels, the host Cisco Unified IP Phone can provide prioritization of CPU and memory resources to the data that associates with the phone voice and with video functions over the data that associates with the Cisco VXC VPN tunnel. This approach requires two manual login entries, depending on security parameters: one for the phone VPN and another for the Cisco VXC VPN. The two-tunnel approach also requires two VPN concentrator ports and two IP addresses.</td>
</tr>
<tr>
<td></td>
<td>• Single Tunnel: The phone establishes only one VPN tunnel for the phone and the Cisco VXC device to share. For customers who are willing to trade off potential voice and video quality for a simplified operating model, the single VPN tunnel option is available. All data travels over a single VPN tunnel by sharing the available phone processor and memory resources across the voice, video, and Cisco VXC services. The IP phone does not prioritize data handing of one service over another. As a result, possible performance degradation of the IP phone voice and video media handling and UI functions may occur due to IP phone CPU loading.</td>
</tr>
<tr>
<td></td>
<td>Default: Dual Tunnel</td>
</tr>
</tbody>
</table>
### Parameter Name | Parameter Description
--- | ---
VXC challenge | This field indicates whether or not to challenge the user for a password for the Cisco VXC VPN.
| 1 Challenge: The phone challenges the user for a password to enable the Cisco VXC VPN.
| 2 No Challenge: The phone does not challenge the user for a password for the Cisco VXC VPN.
| Default: Challenge
| **Note** | If the phone uses only a certificate for authentication, the Sign In windows do not display.

VXC-M Servers | This field indicates the Cisco VXC Manager Server IP address list, where each entry is separated by commas.
| Maximum length: 255 (character length)
| Default: blank
| **Note** | VXC-M Servers is an IP address list which includes VXC-M servers and repository servers (if present). The phone considers the first IP address in this string as the VXC-M server and offers this information to VXC devices. Therefore, after you configure VXC-M Servers, make sure that the IP addresses of any VXC-M servers are placed in front of the IP addresses of the repository servers.

The following table describes how the VXC VPN Option and Challenge field settings alter the operation of the Cisco VXC VPN feature.

**Table 32: Cisco VXC VPN operation as determined by VXC VPN Option and Challenge settings**

<table>
<thead>
<tr>
<th>VXC VPN Option setting</th>
<th>VXC Challenge setting</th>
<th>Result after enabling the VXC VPN feature (with Cisco VXC connected to the phone)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dual Tunnel (default)</td>
<td>Challenge (default)</td>
<td>The phone displays the VXC VPN Sign In window to prompt the user to enter a password. If one-time password is configured on the VPN concentrator (that is, a new password is always required to reauthenticate the tunnel), the user must enter a password for the Cisco VXC VPN that differs from the password that was used for the phone VPN tunnel.</td>
</tr>
</tbody>
</table>
The following table describes how a change in the VXC VPN Option setting alters the operation of the VXC VPN feature when the feature is already enabled.

**Table 33: Cisco VXC VPN operation as determined by VXC VPN Option change**

<table>
<thead>
<tr>
<th>VXC VPN action</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change from Dual Tunnel to Single Tunnel</td>
<td>The phone disconnects the VXC VPN tunnel and leaves the phone VPN tunnel intact. Cisco VXC traffic receives permission to go over the phone VPN tunnel.</td>
</tr>
<tr>
<td>Change from Single Tunnel to Dual Tunnel</td>
<td>The phone attempts to reuse the phone VPN credentials for the Cisco VXC VPN tunnel silently without considering the VXC Challenge field. If the VPN concentrator is configured for one-time password, the attempt fails and the phone displays the VXC VPN Sign In window, which prompts the user to enter a different password.</td>
</tr>
</tbody>
</table>
Cisco VXC VPN Limitations and Restrictions

The following limitations and restrictions apply:

• Only Layer 3 packets are tunneled. The Cisco VXC VPN feature does not support Layer 2 tunneling. Therefore any Layer 2 capabilities are lost if the Cisco VXC connects through VPN.

• The VPN client supports only IPv4 addresses.

• The Cisco VXC VPN tunnel cannot be established over a Wi-Fi interface.

• The Enable VXC VPN for MAC feature option is configurable only after you set up the phone VPN parameters, including VPN Group and VPN Profile. This restriction exists because the Cisco VXC VPN can share the same VPN parameters as the phone VPN.

• All existing limitations and restrictions that apply to the phone VPN support apply to the Cisco VXC VPN as well.

Note

Do not turn on the VPN before a downgrade to a load previous to 9.2(3), or the phone will be unregistered.
Part V

Cisco Unified IP Phone Troubleshooting

- Monitoring Phone Systems, page 263
- Troubleshooting, page 301
- Maintenance, page 327
- International User Support, page 333
Monitoring Phone Systems

- Cisco Unified IP Phone Status, page 263
- Cisco IP Phone Web Page, page 284
- Request Information from the Phone in XML, page 297

Cisco Unified IP Phone Status

This section describes how to view model information, status messages, and network statistics on the Cisco Unified IP Phone 8961, 9951, and 9971.

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

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

You can also obtain much of this information, and obtain other related information, remotely through the phone web page. For more information, see Cisco IP Phone Web Page, on page 284.

For more information about troubleshooting the Cisco Unified IP Phone 8961, 9951, and 9971, see Troubleshooting, on page 301.

Display Phone Information Window

To display the Model Information screen, follow these steps.

Procedure

Step 1 Press Applications.
Step 2 Select Phone Information.

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

Related Topics

Cisco IP Phone Web Page, on page 284

Model Information Fields

The following table describes the Model Information settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Number</td>
<td>Model number of the phone.</td>
</tr>
<tr>
<td>IPv4 Address or IPv6 address</td>
<td>IP address of the phone. The address displayed depends on the IPv6 setup.</td>
</tr>
<tr>
<td>Host name</td>
<td>Host name of the phone.</td>
</tr>
<tr>
<td>Active Load</td>
<td>Version of firmware currently installed on the phone. The user can press Details for more information.</td>
</tr>
<tr>
<td></td>
<td>Inactive Load appears only when a download is in progress. A download icon and a status of &quot;Upgrade in Progress&quot; or &quot;Upgrade Failed&quot; also display. If a user presses Details during an upgrade, the download filename and components are listed. A new firmware image can be set to download in advance of a maintenance window. Thus instead of waiting for all of the phones to download the firmware, the system switches more rapidly between resetting an existing load to Inactive status and installing the new load. When the download is complete, the icon changes to indicate the completed status; and a check mark displays for a successful download, or an “X” displays for a failed download. If possible, the rest of the loads continue to download.</td>
</tr>
<tr>
<td></td>
<td>Inactive Load</td>
</tr>
<tr>
<td>Last Upgrade</td>
<td>Date of the most recent firmware upgrade.</td>
</tr>
<tr>
<td>Active Server</td>
<td>Domain name of the server to which the phone is registered.</td>
</tr>
<tr>
<td>Stand-by Server</td>
<td>Domain name of the standby server.</td>
</tr>
</tbody>
</table>

Display Status Menu

The Status menu includes the following options, which provide information about the phone and phone operations:
• Status Messages: Displays the Status Messages screen, which shows a log of important system messages.
• Ethernet Statistic: Displays the Ethernet Statistics screen, which shows Ethernet traffic statistics.
• Wireless Statistics: Displays the Wireless Statistics screen, if applicable.
• Call Statistics: Displays counters and statistics for the current call.
• Current Access Point: Displays the Current Access Point screen, if applicable.

To display the Status menu, perform these steps:

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>To display the Status menu, press <strong>Applications</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select <strong>Administrator Settings &gt; Status</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>To exit the Status menu, press <strong>Exit</strong>.</td>
</tr>
</tbody>
</table>

**Display Status Messages Window**

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

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Press <strong>Applications</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select <strong>Administrator Settings &gt; Status &gt; Status Messages</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>To remove the current status messages, press <strong>Clear List</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>To exit the Status Messages screen, press <strong>Exit</strong>.</td>
</tr>
</tbody>
</table>

**Related Topics**

- [Phone Displays Error Messages](#), on page 304

**Status Messages Fields**

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

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Possible explanation and action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFG TFTP Size Error</td>
<td>The configuration file is too large for file system on the phone.</td>
<td>Power cycle the phone.</td>
</tr>
</tbody>
</table>

Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 10.0
<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Possible explanation and action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checksum Error</td>
<td>Downloaded software file is</td>
<td>Obtain a new copy of the phone firmware and place it in the TFTPPath directory. You should only</td>
</tr>
<tr>
<td></td>
<td>corrupted.</td>
<td>copy files into this directory when the TFTP server software is shut down; otherwise, the files</td>
</tr>
<tr>
<td></td>
<td></td>
<td>may be corrupted.</td>
</tr>
<tr>
<td>CTL and ITL installed</td>
<td>The CTL and ITL files are installed on the phone.</td>
<td>None. This message is informational only. Neither the CTL file nor the ITL file was installed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>previously.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information about the trust list, see Cisco Unified Communications Manager Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guide.</td>
</tr>
<tr>
<td>CTL Installed</td>
<td>A certificate trust list (CTL) file is installed in the phone.</td>
<td>None. This message is informational only. The CTL file was not installed previously.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information about the CTL file, see the Cisco Unified Communications Manager Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guide.</td>
</tr>
<tr>
<td>CTL update failed</td>
<td>The phone could not update the</td>
<td>Problem with the CTL file on the TFTP server.</td>
</tr>
<tr>
<td></td>
<td>certificate trust list (CTL) file.</td>
<td>For more information, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>DHCP timeout</td>
<td>DHCP server did not respond.</td>
<td>Network is busy: The errors should resolve themselves when the network load reduces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No network connectivity between the DHCP server and the phone: Verify the network connections.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DHCP server is down: Check configuration of DHCP server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Errors persist: Consider assigning a static IP address.</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Possible explanation and action</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DNS timeout</td>
<td>DNS server did not respond.</td>
<td>Network is busy: The errors should resolve themselves when the network load reduces. No network connectivity between the DNS server and the phone: Verify the network connections. DNS server is down: Check configuration of the DNS server.</td>
</tr>
<tr>
<td>DNS unknown host</td>
<td>DNS could not resolve the name of the TFTP server or Cisco Unified Communications Manager.</td>
<td>Verify that the host names of the TFTP server or Cisco Unified Communications Manager are configured properly in DNS. Consider using IP addresses rather than host names.</td>
</tr>
<tr>
<td>Duplicate IP</td>
<td>Another device is using the IP address that is assigned to the phone.</td>
<td>If the phone has a static IP address, verify that you did not assign a duplicate IP address. If you are using DHCP, check the DHCP server configuration.</td>
</tr>
<tr>
<td>Erasing CTL and ITL files</td>
<td>Erasing CTL or ITL file.</td>
<td>None. This message is informational only. For more information about the CTL and ITL files, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
</tbody>
</table>
| Error update locale     | One or more localization files could not be found in the TFTPPath directory or were not valid. The locale was not changed. | From Cisco Unified Operating System Administration, check that the following files are located within subdirectories in the TFTP File Management:  
  • Located in subdirectory with same name as network locale:  
    ▪ tones.xml  
  • Located in subdirectory with same name as user locale:  
    ▪ glyphs.xml  
    ▪ dictionary.xml  
    ▪ kate.xml |
<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Possible explanation and action</th>
</tr>
</thead>
<tbody>
<tr>
<td>File not found &lt;Cfg File&gt;</td>
<td>The name-based and default configuration file was not found on the TFTP Server.</td>
<td>The configuration file for a phone is created when the phone is added to the Cisco Unified Communications Manager database. If the phone does not exist in the Cisco Unified Communications Manager database, the TFTP server generates a CFG File Not Found response.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Phone is not registered with Cisco Unified Communications Manager. You must manually add the phone to Cisco Unified Communications Manager if you are not allowing phones to autoregister. See Phone Addition Methods, on page 91 for details.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If you are using static IP addresses, check configuration of the TFTP server.</td>
</tr>
<tr>
<td>File Not Found &lt;CTLFile.tlv&gt;</td>
<td>This message displays on the phone when the Cisco Unified Communications Manager cluster is not in secure mode.</td>
<td>No impact; the phone can still register to Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>IP address released</td>
<td>The phone is configured to release the IP address.</td>
<td>The phone remains idle until it is power cycled or until you reset the DHCP address.</td>
</tr>
<tr>
<td>ITL installed</td>
<td>The ITL file is installed in the phone.</td>
<td>None. This message is informational only. The ITL file was not installed previously. For more information about the ITL file, see Cisco Unified Communications Manager Security Guide.</td>
</tr>
</tbody>
</table>

The configuration file for a phone is created when the phone is added to the Cisco Unified Communications Manager database. If the phone does not exist in the Cisco Unified Communications Manager database, the TFTP server generates a CFG File Not Found response.
<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Possible explanation and action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load rejected HC</td>
<td>The application that was downloaded is not compatible with the phone hardware.</td>
<td>Occurs if you attempted to install a version of software on this phone that did not support hardware changes on this phone. Check the load ID that is assigned to the phone (from Cisco Unified Communications Manager, choose <strong>Device &gt; Phone</strong>). Reenter the load that displays on the phone.</td>
</tr>
<tr>
<td>No default router</td>
<td>DHCP or static configuration did not specify a default router.</td>
<td>If the phone has a static IP address, verify that the default router is configured. If you are using DHCP, the DHCP server has not provided a default router. Check the DHCP server configuration.</td>
</tr>
<tr>
<td>No DNS server IP</td>
<td>A name was specified but DHCP or static IP configuration did not specify a DNS server address.</td>
<td>If the phone has a static IP address, verify that the DNS server is configured. If you are using DHCP, the DHCP server has not provided a DNS server. Check the DHCP server configuration.</td>
</tr>
<tr>
<td>No Trust List installed</td>
<td>The CTL file or the ITL file is not installed on the phone.</td>
<td>The trust list is not configured on the Cisco Unified Communications Manager, which does not support security by default. For more information about the trust list, see the <strong>Cisco Unified Communications Manager Security Guide</strong>.</td>
</tr>
<tr>
<td>Restart requested by Cisco Unified Communications Manager</td>
<td>The phone is restarting due to a request from Cisco Unified Communications Manager.</td>
<td>Configuration changes were likely made to the phone in Cisco Unified Communications Manager, and Apply was pressed so that the changes take effect.</td>
</tr>
<tr>
<td>TFTP access error</td>
<td>TFTP server is pointing to a directory that does not exist.</td>
<td>If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server. If you are using static IP addresses, check configuration of TFTP server.</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Possible explanation and action</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TFTP error</td>
<td>The phone does not recognize an error code that the TFTP server provided.</td>
<td>Contact Cisco TAC.</td>
</tr>
<tr>
<td>TFTP timeout</td>
<td>TFTP server did not respond.</td>
<td>Network is bus: The errors should resolve themselves when the network load reduces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No network connectivity between the TFTP server and the phone: Verify the network connections.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TFTP server is down: Check configuration of TFTP server.</td>
</tr>
<tr>
<td>Timed Out</td>
<td>Supplicant attempted 802.1X transaction but timed out to due the absence of an authenticator.</td>
<td>Authentication typically times out if 802.1X is not configured on the switch.</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Possible explanation and action</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Trust List update failed</td>
<td>Update of the CTL and ITL files failed.</td>
<td>Phone has CTL and ITL files installed and it failed to update the new CTL and ITL files. Possible reasons for failure:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Network failure occurred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TFTP server was down.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The new security token that was used to sign CTL file and the TFTP certificate that was used to sign ITL file are introduced, but are not available in the current CTL and ITL files in the phone.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Internal phone failure occurred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible solutions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check network connectivity.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the TFTP server is active and functioning normally.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the Transactional Vsam Services (TVS) server is supported on Cisco Unified Communications Manager, check whether the TVS server is active and functioning normally.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Verify whether the security token and the TFTP server are valid.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Manually delete the CTL and ITL files if all the preceding solutions fail; reset the phone.</td>
</tr>
<tr>
<td>Trust List updated</td>
<td>The CTL file, the ITL file, or both files are updated.</td>
<td>None. This message is informational only. For more information about the trust list, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>Version error</td>
<td>The name of the phone load file is incorrect.</td>
<td>Make sure that the phone load file has the correct name.</td>
</tr>
</tbody>
</table>
Related Topics

Configure Network Settings, on page 70

Display Ethernet Statistics Screen

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

To display the Ethernet Statistics screen, follow these steps:

**Procedure**

1. Press **Applications.**
2. Select **Administrator Settings.**
3. Select **Status.**
4. Select **Status > Ethernet Statistics.** See Ethernet Statistics Information, on page 272 for a description of the Ethernet statistics fields.
5. To reset the Rx Frames, Tx Frames, and Rx Broadcasts statistics to 0, press **Clear List.**
6. To exit the Ethernet Statistics screen, press **Exit.**

**Ethernet Statistics Information**

The following tables describe the information in the Ethernet Statistics screen.

**Table 36: Ethernet Statistics Information**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Frames</td>
<td>Number of packets that the phone received.</td>
</tr>
<tr>
<td>Tx Frames</td>
<td>Number of packets that the phone sent.</td>
</tr>
<tr>
<td>Rx Broadcasts</td>
<td>Number of broadcast packets that the phone received.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Restart Cause</td>
<td>Cause of the last reset of the phone. Specifies one of the following values:</td>
</tr>
<tr>
<td></td>
<td>- Initialized</td>
</tr>
<tr>
<td></td>
<td>- TCP-timeout</td>
</tr>
<tr>
<td></td>
<td>- CM-closed-TCP</td>
</tr>
<tr>
<td></td>
<td>- TCP-Bad-ACK</td>
</tr>
<tr>
<td></td>
<td>- CM-reset-TCP</td>
</tr>
<tr>
<td></td>
<td>- CM-aborted-TCP</td>
</tr>
<tr>
<td></td>
<td>- CM-NAKed</td>
</tr>
<tr>
<td></td>
<td>- KeepaliveTO</td>
</tr>
<tr>
<td></td>
<td>- Failback</td>
</tr>
<tr>
<td></td>
<td>- Phone-Keypad</td>
</tr>
<tr>
<td></td>
<td>- Phone-Re-IP</td>
</tr>
<tr>
<td></td>
<td>- Reset-Reset</td>
</tr>
<tr>
<td></td>
<td>- Reset-Restart</td>
</tr>
<tr>
<td></td>
<td>- Phone-Reg-Rej</td>
</tr>
<tr>
<td></td>
<td>- Load Rejected HC</td>
</tr>
<tr>
<td></td>
<td>- CM-ICMP-Unreach</td>
</tr>
<tr>
<td></td>
<td>- Phone-Abort</td>
</tr>
<tr>
<td>Elapsed Time</td>
<td>Amount of time that has elapsed since the phone last rebooted.</td>
</tr>
<tr>
<td>Port 1</td>
<td>Link state and connection of the Network port. For example, Auto 100 Mb Full-Duplex means that the Network port is in a link-up state and has autonegotiated a full-duplex, 100-Mbps connection.</td>
</tr>
<tr>
<td>Port 2</td>
<td>Link state and connection of the PC port.</td>
</tr>
<tr>
<td>DHCP state (IPv4 / IPv6)</td>
<td>- In IPv4-mode, displays only the DHCPv4 state, such as DHCP BOUND.</td>
</tr>
<tr>
<td></td>
<td>- In IPv6-mode, displays only the DHCPv6 state, such as ROUTER ADVERTISE., (GOOD IP).</td>
</tr>
<tr>
<td></td>
<td>- In dual-stack mode, both DHCPv4 and DHCPv6 state information is displayed.</td>
</tr>
</tbody>
</table>

The following tables describe the messages that appear for DHCPv4 and DHCPv6 states.
### Table 37: DHCPv4 ethernet statistics messages

<table>
<thead>
<tr>
<th>DHCPv4 state</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDP INIT</td>
<td>CDP is not bound or WLAN is not in service</td>
</tr>
<tr>
<td>DHCP BOUND</td>
<td>DHCPv4 is BOUND</td>
</tr>
<tr>
<td>DHCP DISABLED</td>
<td>DHCPv4 is disabled</td>
</tr>
<tr>
<td>DHCP INIT</td>
<td>DHCPv4 is INIT</td>
</tr>
<tr>
<td>DHCP INVALID</td>
<td>DHCPv4 is INVALID; this is initial state</td>
</tr>
<tr>
<td>DHCP RENEWING</td>
<td>DHCPv4 is RENEWING</td>
</tr>
<tr>
<td>DHCP REBINDING</td>
<td>DHCPv4 is REBINDING</td>
</tr>
<tr>
<td>DHCP REBOOT</td>
<td>DHCPv4 is init-reboot</td>
</tr>
<tr>
<td>DHCP REQUESTING</td>
<td>DHCPv4 is requesting</td>
</tr>
<tr>
<td>DHCP RESYNC</td>
<td>DHCPv4 is RESYNCH</td>
</tr>
<tr>
<td>DHCP WAITING COLDBOOT TIMEOUT</td>
<td>DHCPv4 is booting</td>
</tr>
<tr>
<td>DHCP UNRECOGNIZED</td>
<td>Unrecognized DHCPv4 state</td>
</tr>
<tr>
<td>DISABLED DUPLICATE IP</td>
<td>Duplicated IPv4 Address</td>
</tr>
<tr>
<td>DHCP TIMEOUT</td>
<td>DHCPv4 Timeout</td>
</tr>
<tr>
<td>IPV4 STACK TURNED OFF</td>
<td>Phone is in IPv6-only mode with IPv4 Stack turned off</td>
</tr>
<tr>
<td>ILLEGAL IPV4 STATE</td>
<td>Illegal IPv4 state and should not happen</td>
</tr>
</tbody>
</table>

### Table 38: DHCPv6 ethernet statistics messages

<table>
<thead>
<tr>
<th>DHCPv6 State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDP INIT</td>
<td>CDP is initializing</td>
</tr>
<tr>
<td>DHCP6 BOUND</td>
<td>DHCPv6 is BOUND</td>
</tr>
<tr>
<td>DHCP6 DISABLED</td>
<td>DHCPv6 is DISABLED</td>
</tr>
<tr>
<td>DHCP6 RENEW</td>
<td>DHCPv6 is renewing</td>
</tr>
<tr>
<td>DHCP6 REBIND</td>
<td>DHCPv6 is rebinding</td>
</tr>
<tr>
<td><strong>DHCPv6 State</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>DHCP6 INIT</td>
<td>DHCPv6 is initializing</td>
</tr>
<tr>
<td>DHCP6 SOLICIT</td>
<td>DHCPv6 is soliciting</td>
</tr>
<tr>
<td>DHCP6 REQUEST</td>
<td>DHCPv6 is requesting</td>
</tr>
<tr>
<td>DHCP6 RELEASING</td>
<td>DHCPv6 is releasing</td>
</tr>
<tr>
<td>DHCP6 RELEASED</td>
<td>DHCPv6 is released</td>
</tr>
<tr>
<td>DHCP6 DISABLING</td>
<td>DHCPv6 is disabling</td>
</tr>
<tr>
<td>DHCP6 DECLINING</td>
<td>DHCPv6 is declining</td>
</tr>
<tr>
<td>DHCP6 DECLINED</td>
<td>DHCPv6 is declined</td>
</tr>
<tr>
<td>DHCP6 INFOREQ</td>
<td>DHCPv6 is INFOREQ</td>
</tr>
<tr>
<td>DHCP6 INFOREQ DONE</td>
<td>DHCPv6 is INFOREQ DONE</td>
</tr>
<tr>
<td>DHCP6 INVALID</td>
<td>DHCPv6 is INVALID; this is initial state</td>
</tr>
<tr>
<td>DISABLED DUPLICATE IPV6</td>
<td>DHCPv6 is DISABLED, but DUPLICATE IPV6 DETECTED</td>
</tr>
<tr>
<td>DHCP6 DECLINED DUPLICATE IP</td>
<td>DHCPv6 is DECLINED -- DUPLICATE IPV6 DETECTED</td>
</tr>
<tr>
<td>ROUTER ADVERTISE., (DUPLICATE IP)</td>
<td>Duplicated autoconfigured IPv6 address</td>
</tr>
<tr>
<td>DHCP6 WAITING COLDBOOT TIMEOUT</td>
<td>DHCPv6 is booting</td>
</tr>
<tr>
<td>DHCP6 TIMEOUT USING RESTORED VAL</td>
<td>DHCPv6 timeout, using the value saved in flash memory</td>
</tr>
<tr>
<td>DHCP6 TIMEOUT CANNOT RESTORE</td>
<td>DHCPv6 timeout and there is no backup from flash memory</td>
</tr>
<tr>
<td>IPV6 STACK TURNED OFF</td>
<td>Phone is in IPv4-only mode with IPv6 Stack turned off</td>
</tr>
<tr>
<td>ROUTER ADVERTISE., (GOOD IP)</td>
<td></td>
</tr>
<tr>
<td>ROUTER ADVERTISE., (BAD IP)</td>
<td></td>
</tr>
<tr>
<td>UNRECOGNIZED MANAGED BY</td>
<td>IPv6 Address is not from router or DHCPv6 server</td>
</tr>
<tr>
<td>ILLEGAL IPV6 STATE</td>
<td>Illegal IPv6 state and should not happen</td>
</tr>
</tbody>
</table>
Display Wireless Statistics Screen

The Wireless Statistics screen displays statistics about the wireless Cisco Unified IP Phone 9971.

To display the Wireless Statistics screen, follow these steps:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Press Applications.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select Administrator Settings.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select Status.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select Wireless Statistics.</td>
</tr>
<tr>
<td>Step 5</td>
<td>To reset the Wireless statistics to 0, press Clear List.</td>
</tr>
<tr>
<td>Step 6</td>
<td>To exit the Wireless Statistics screen, press Exit.</td>
</tr>
</tbody>
</table>

*Wireless Statistics*

The following table describes the Wireless statistics on the phone.

**Table 39: Wireless Statistics on the Cisco Unified IP Phone**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmit Frames</td>
<td>Number of packets that the phone transmitted.</td>
</tr>
<tr>
<td>Directed Frames Received</td>
<td>Number of directed packets that the phone received.</td>
</tr>
<tr>
<td>Multicast Frames Received</td>
<td>Number of multicast packets that the phone received.</td>
</tr>
<tr>
<td>Broadcast Frames Received</td>
<td>Number of broadcast packets that the phone received.</td>
</tr>
<tr>
<td>Receive Errors</td>
<td>Number of packets with errors that the phone received.</td>
</tr>
<tr>
<td>Receive No Buffers</td>
<td>The phone has no buffers available to receive the packet.</td>
</tr>
<tr>
<td>Frame Checksum (FCS) Errors</td>
<td>Increments when an FCS error is detected in a received MPDU.</td>
</tr>
<tr>
<td>Duplicate Frames</td>
<td>Number of duplicate packets received by the phone.</td>
</tr>
<tr>
<td>Fragments Received</td>
<td>Number of fragmented packets that the phone received.</td>
</tr>
<tr>
<td>Beacons Received</td>
<td>Number of beacons that the phone received.</td>
</tr>
<tr>
<td>Association Rejected</td>
<td>Number of AP association rejections that the phone received.</td>
</tr>
<tr>
<td>Association Timeouts</td>
<td>Number of AP association timeouts that the phone received.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Authentication Rejects</td>
<td>Number of authentication rejects that the phone received.</td>
</tr>
<tr>
<td>Authentication Timeouts</td>
<td>Number of authentication timeouts that the phone received.</td>
</tr>
<tr>
<td>QOS Null Frames</td>
<td>Number of QOS null packets that the phone received.</td>
</tr>
<tr>
<td>QOS Data Received</td>
<td>Number of QOS packets that the phone received.</td>
</tr>
<tr>
<td>Transmit Ok</td>
<td>Number of packets that the phone transmitted without error.</td>
</tr>
<tr>
<td>Transmit Errors</td>
<td>Number of packets with errors that the phone transmitted.</td>
</tr>
<tr>
<td>Direct Frames Transmitted</td>
<td>Number of direct packets that the phone transmitted.</td>
</tr>
<tr>
<td>Multicast Frames Transmitted</td>
<td>Number of multicast packets that the phone transmitted.</td>
</tr>
<tr>
<td>Broadcast Frames Transmitted</td>
<td>Number of broadcast packets that the phone transmitted.</td>
</tr>
<tr>
<td>RTS Failed</td>
<td>A corresponding CTS was not received.</td>
</tr>
<tr>
<td>ACK Failed</td>
<td>AP did not acknowledge a transmission.</td>
</tr>
<tr>
<td>Retries</td>
<td>Counter of total retries.</td>
</tr>
<tr>
<td>Multiple Retries</td>
<td>Transmission of packet required two or more retries before success.</td>
</tr>
<tr>
<td>Retry Failures</td>
<td>Transmission of packet failed.</td>
</tr>
<tr>
<td>Transmit Timeouts</td>
<td>Transmission of packet failed due to queue time.</td>
</tr>
<tr>
<td>Success Counter</td>
<td>Counter of successful transmissions.</td>
</tr>
<tr>
<td>Max Retry Failure</td>
<td>Counter of successive transmission failures that caused a roaming attempt.</td>
</tr>
</tbody>
</table>

**The following Wireless Statistics items display these AP queues: Background (BK), Best Effort (BE), Video (VI), and Voice (VO)**

- QOS Data Received
- Transmit Ok
- Transmit Errors
- Direct Frames Transmitted
- Multicast Frames Transmitted
- Broadcast Frames Transmitted
- RTS Failed
- ACK Failed
- Retries
- Multiple Retries
- Retry Failures
- Transmit Timeouts
- Success Counter
- Max Retry Failure

**Display Call Statistics Window**

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

**Note**

You can also remotely view the call statistics information by using a web browser to access the Streaming Statistics web page. This web page contains additional RTCP statistics that are not available on the phone. For more information about remote monitoring, see Cisco IP Phone Web Page, on page 284.
A single call can use multiple voice streams, but data is captured for only the last voice stream. A voice stream is a packet stream between two endpoints. If one endpoint is put on hold, the voice stream stops even though the call is still connected. When the call resumes, a new voice packet stream begins, and the new call data overwrites the former call data.

**Procedure**

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

**Call Statistics fields**

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

**Table 40: Call Statistics items for the Cisco Unified Phone**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rcvr Codec</td>
<td>Type of received voice stream (RTP streaming audio from codec): G.729,</td>
</tr>
<tr>
<td></td>
<td>G.722, G.711 mu-law, G.711 A-law, and iLBC.</td>
</tr>
<tr>
<td>Sender Codec</td>
<td>Type of transmitted voice stream (RTP streaming audio from codec): G.729,</td>
</tr>
<tr>
<td></td>
<td>G.722, G.711 mu-law, G.711 A-law, and iLBC.</td>
</tr>
<tr>
<td>Rcvr Size</td>
<td>Size of voice packets, in milliseconds, in the receiving voice stream (RTP</td>
</tr>
<tr>
<td></td>
<td>streaming audio).</td>
</tr>
<tr>
<td>Sender Size</td>
<td>Size of voice packets, in milliseconds, in the transmitting voice stream.</td>
</tr>
<tr>
<td>Rcvr Packets</td>
<td>Number of RTP voice packets that were received since voice stream opened.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This number is not necessarily identical to the number of RTP voice</td>
</tr>
<tr>
<td></td>
<td>packets that were received since the call began because the call might have</td>
</tr>
<tr>
<td></td>
<td>been placed on hold.</td>
</tr>
<tr>
<td>Sender Packets</td>
<td>Number of RTP voice packets that were transmitted since voice stream opened.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This number is not necessarily identical to the number of RTP voice</td>
</tr>
<tr>
<td></td>
<td>packets that were transmitted since the call began because the call might</td>
</tr>
<tr>
<td></td>
<td>have been placed on hold.</td>
</tr>
<tr>
<td>Avg Jitter</td>
<td>Estimated average RTP packet jitter (dynamic delay that a packet encounters</td>
</tr>
<tr>
<td></td>
<td>when going through the network), in milliseconds, that was observed since</td>
</tr>
<tr>
<td></td>
<td>the receiving voice stream opened.</td>
</tr>
<tr>
<td>Max Jitter</td>
<td>Maximum jitter, in milliseconds, that was observed since the receiving voice</td>
</tr>
<tr>
<td></td>
<td>stream opened.</td>
</tr>
</tbody>
</table>
### Voice-Quality Metrics

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rcvr Discarded</td>
<td>Number of RTP packets in the receiving voice stream that were discarded (bad packets, too late, and so on).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The phone discards payload type 19 comfort noise packets that Cisco Gateways generate, because they increment this counter.</td>
</tr>
<tr>
<td>Rcvr Lost Packets</td>
<td>Missing RTP packets (lost in transit).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOS LQK</td>
<td>Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding eight-second interval of the voice stream. For more information, see Voice Quality Monitoring, on page 330.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.</td>
</tr>
<tr>
<td>Avg MOS LQK</td>
<td>Average MOS LQK score that was observed for the entire voice stream.</td>
</tr>
<tr>
<td>Min MOS LQK</td>
<td>Lowest MOS LQK score that was observed from the start of the voice stream.</td>
</tr>
<tr>
<td>Max MOS LQK</td>
<td>Baseline or highest MOS LQK score that was observed from the start of the voice stream. These codecs provide the following maximum MOS LQK score under normal conditions with no frame loss:</td>
</tr>
<tr>
<td></td>
<td>• G.711 yields a score of 4.5.</td>
</tr>
<tr>
<td></td>
<td>• G.729 A/AB yields a score of 3.7.</td>
</tr>
<tr>
<td>MOS LQK Version</td>
<td>Version of the Cisco proprietary algorithm that is used to calculate MOS LQK scores.</td>
</tr>
<tr>
<td>Cumulative Conceal Ratio</td>
<td>Total number of concealment frames divided by total number of speech frames that were received from start of the voice stream.</td>
</tr>
<tr>
<td>Interval Conceal Ratio</td>
<td>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.</td>
</tr>
<tr>
<td>Max Conceal Ratio</td>
<td>Highest interval concealment ratio from start of the voice stream.</td>
</tr>
<tr>
<td>Conceal Secs</td>
<td>Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).</td>
</tr>
<tr>
<td>Severely Conceal Secs</td>
<td>Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.</td>
</tr>
</tbody>
</table>
**Display Video Statistics Window**

You can access the Video Statistics screen on the phone to display counters, statistics of the most recent call.

**Note**

You can also remotely view the video statistics information by using a web browser to access the Streaming Statistics web page. This web page contains additional RTCP statistics that are not available on the phone. For more information about remote monitoring, see *Cisco IP Phone Web Page*, on page 284.

A video stream is a frame stream between two endpoints. If one endpoint pauses the video streaming, the video stream stops even though the call is still connected. When the video streaming resumes, a new video frame stream begins, and the new video data overwrites the former video data.

To display the Video Statistics screen for information about the latest video stream, follow these steps:

**Procedure**

1. Press **Applications**.
2. Select **Administrator Settings**.
3. Select **Call Statistics**.
4. Select **Video**.
5. To exit the Video screen, press **Exit**.

**Video Statistics Fields**

The following table describes the Video Statistics fields.

*Table 41: Video Statistics Items for the Cisco Unified Phone*

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rcvr Codec</td>
<td>Type of received video stream (RTP streaming video from codec).</td>
</tr>
<tr>
<td>Sender Codec</td>
<td>Type of transmitted video stream (RTP streaming video from codec).</td>
</tr>
<tr>
<td>Rcvr Packets</td>
<td>Number of RTP video packets that were received since the video stream opened.</td>
</tr>
</tbody>
</table>

**Note** This number is not necessarily identical to the number of RTP video packets received since the call began because the call might have been placed on hold.
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender Packets</td>
<td>Number of RTP video packets that were transmitted since the video stream opened.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This number is not necessarily identical to the number of RTP video packets transmitted since the call began because the call might have been placed on hold.</td>
</tr>
<tr>
<td>Avg Jitter</td>
<td>Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network), in milliseconds, that was observed since the receiving video stream opened.</td>
</tr>
<tr>
<td>Max Jitter</td>
<td>Maximum jitter, in milliseconds, observed since the receiving video stream opened.</td>
</tr>
<tr>
<td>Rcvr Discarded</td>
<td>Number of RTP packets in the receiving video stream that were discarded (bad packets, too late, and so on).</td>
</tr>
<tr>
<td>Rcvr Lost Packets</td>
<td>Missing RTP video packets (lost in transit).</td>
</tr>
<tr>
<td>Rcvr Size</td>
<td>Size of video frames, in milliseconds, in the receiving video stream (RTP streaming video).</td>
</tr>
<tr>
<td>Sender Size</td>
<td>Size of video frames, in milliseconds, in the transmitting video stream.</td>
</tr>
<tr>
<td>Sender Frames</td>
<td>Number of video frames that by the camera/phone transmitted since the video stream opened.</td>
</tr>
<tr>
<td>Sender Partial Frames</td>
<td>Number of P-frames that the camera sent since the video stream opened.</td>
</tr>
<tr>
<td>Sender IFrames</td>
<td>Number of I-frames that the camera sent since the video stream opened.</td>
</tr>
<tr>
<td>Sender Frame Rate</td>
<td>Rate at which video frames are transmitted (in frames per second).</td>
</tr>
<tr>
<td>Sender Bandwidth</td>
<td>Bandwidth of the transmitted video steam in kbps (kilo bits per second).</td>
</tr>
<tr>
<td>Sender Resolution</td>
<td>Resolution of the video stream that the camera transmits. VGA(640x480), CIF (352x288), QCIF (176x144)</td>
</tr>
<tr>
<td>Rcvr Frames</td>
<td>Number of video frames that the phone received since the video stream opened.</td>
</tr>
<tr>
<td>Rcvr Partial Frames</td>
<td>Number of P-frames that the phone received since the video stream opened.</td>
</tr>
<tr>
<td>Rcvr IFrames</td>
<td>Number of I-frames that the phone received since the video stream opened.</td>
</tr>
<tr>
<td>Rcvr IFrames Req</td>
<td>Number of IDR requests that the phone sent to the remote endpoint since the video stream opened.</td>
</tr>
<tr>
<td>Rcvr Frame Rate</td>
<td>Rate at which video frames are received (in frames per second).</td>
</tr>
</tbody>
</table>
### Display Current Access Point Window

The Current Access Point screen displays statistics about the current access point on the wireless Cisco Unified IP Phone 9971. *Current Access Point Fields*, on page 282 describes the information that appears in this screen.

To display the Current Access Point screen, follow these steps:

#### Procedure

1. **Step 1** Press **Applications**.
2. **Step 2** Select **Administrator Settings**.
3. **Step 3** Select **Status**.
4. **Step 4** Select **Current Access Point**.
5. **Step 5** To exit the Current Access Point screen, press **Exit**.

#### Current Access Point Fields

The following table describes the fields in the Current Access Point screen.

*Table 42: Current Access Point Items*

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Name</td>
<td>Name of the AP, if it is CCX-compliant; otherwise, the MAC address displays here.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC address of the AP.</td>
</tr>
<tr>
<td>Frequency</td>
<td>The latest frequency where this AP was observed.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last RSSI</td>
<td>The latest RSSI in which this AP was observed.</td>
</tr>
<tr>
<td>Beacon Interval</td>
<td>Number of time units between beacons. A time unit is 1.024 ms.</td>
</tr>
<tr>
<td>Capability</td>
<td>This field contains a number of subfields that are used to indicate requested or advertised optional capabilities.</td>
</tr>
<tr>
<td>Basic Rates</td>
<td>Data rates that the AP requires and the AP at which the station must be capable of operating.</td>
</tr>
<tr>
<td>Optional Rates</td>
<td>Data rates that the AP supports and the AP that are optional for the station to operate at.</td>
</tr>
<tr>
<td>Current Channel</td>
<td>The latest channel where this AP was observed.</td>
</tr>
<tr>
<td>dtime Period</td>
<td>Every nth beacon is a dtime period. After each DTIM beacon, the AP sends any broadcast or multicast packets that are queued for power-save devices.</td>
</tr>
<tr>
<td>Country Code</td>
<td>A two-digit country code. Country information might not be display if the country information element (IE) is not present in the beacon.</td>
</tr>
<tr>
<td>Channels</td>
<td>A list of supported channels (from the country IE).</td>
</tr>
<tr>
<td>Power Constraint</td>
<td>The amount of power by which the maximum transmit power should be reduced from the regulatory domain limit.</td>
</tr>
<tr>
<td>Power Limit</td>
<td>Maximum transmit power in dBm that is permitted for that channel.</td>
</tr>
<tr>
<td>Channel Utilization</td>
<td>The percentage of time, normalized to 255, in which the AP sensed the medium was busy, as indicated by the physical or virtual carrier sense (CS) mechanism.</td>
</tr>
<tr>
<td>Station Count</td>
<td>Data rates that the AP requires and at which the station must be capable of operating.</td>
</tr>
<tr>
<td>Admission Capacity</td>
<td>An unsigned integer that specifies the remaining amount of medium time that is available through explicit admission control, in units of 32 microseconds per second. If the value is 0, the AP does not support this information element and the capacity is unknown.</td>
</tr>
<tr>
<td>WMM Supported</td>
<td>Support for Wi-Fi multimedia extensions.</td>
</tr>
<tr>
<td>UAPSD Supported</td>
<td>The AP supports Unscheduled Automatic Power Save Delivery. May only be available if WMM is supported. This feature is critical for talk time and for achieving maximum call density on the wireless IP Phone.</td>
</tr>
<tr>
<td>Proxy ARP</td>
<td>CCX-compliant AP supports responding to IP ARP requests on behalf of the associated station. This feature is critical to standby time on the wireless IP Phone.</td>
</tr>
<tr>
<td>CCX Version</td>
<td>If the AP is CCX compliant, this field shows the CCX version.</td>
</tr>
</tbody>
</table>
Cisco IP Phone Web Page

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

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

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

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

Related Topics
- Display Phone Information Window, on page 263
- Control Phone Web Page Access, on page 237

Access Web Page for Phone

The Cisco Unified IP Phone can be configured to use:

- HTTPS protocol only
- HTTP or HTTPS protocols

If the Cisco Unified IP Phone is configured to use the HTTP or HTTPS protocols, use http://<IP_address> or https://<IP_address> for phone web access.

If the Cisco Unified IP Phone is configured to use only HTTPS protocol, use https://<IP_address> for phone web access.
If you cannot access the web page, it may be disabled by default.

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

**Procedure**

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

a) Search for the phone in Cisco Unified Communications Manager Administration by choosing **Device > Phone**. Phones that register with Cisco Unified Communications Manager display the IP address on the Find and List Phones window and at the top of the Phone Configuration window.

b) On the Cisco Unified IP Phone, press **Applications**, choose **Administrator Settings > Network Setup > IPv4 Setup**, and then scroll to the IP Address option.

**Step 2**
Open a web browser and enter the following URL, where `<IP_address>` is the IP address of the Cisco Unified IP Phone:

http://<IP_address> or https://<IP_address> (depending on the protocol supported by the Cisco Unified IP Phone)

**Related Topics**

Control Phone Web Page Access, on page 237

**Device Information**

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

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

To display the Device Information area, access the web page for the phone as described in **Access Web Page for Phone**, on page 284, and then click the Device Information hyperlink.

**Table 43: Device Information Area Items**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Media Access Control (MAC) address of the phone.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Unique, fixed name that is automatically assigned to the phone based on the MAC address.</td>
</tr>
<tr>
<td>Phone DN</td>
<td>Directory number that is assigned to the phone.</td>
</tr>
<tr>
<td>Version</td>
<td>Identifier of the firmware that is running on the phone.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Key Expansion Module 1</td>
<td>Identifier for the first KEM, if applicable.</td>
</tr>
<tr>
<td>Key Expansion Module 2</td>
<td>Identifier for the second KEM, if applicable.</td>
</tr>
<tr>
<td>Key Expansion Module 3</td>
<td>Identifier for the third KEM, if applicable.</td>
</tr>
<tr>
<td>Hardware Revision</td>
<td>Revision value of the phone hardware.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Unique serial number of the phone.</td>
</tr>
<tr>
<td>Model Number</td>
<td>Model number of the phone.</td>
</tr>
<tr>
<td>Message Waiting</td>
<td>Indicates whether is a voice message is waiting on the primary line for this phone.</td>
</tr>
</tbody>
</table>
| UDI                         | Displays the following Cisco Unique Device Identifier (UDI) information about the phone:  
                                 |     • Device Type: Indicates hardware type. For example, phone displays for all phone models.  
                                 |     • Device Description: Displays the name of the phone associated with the indicated model type.  
                                 |     • Product Identifier: Specifies the phone model.  
                                 |     • Serial Number: Displays the unique serial number of the phone. |
| Key Expansion Module UDI    | Cisco Unique Device Identifier (UDI) of the KEM.                           |
| Time                        | Time for the Date/Time Group to which the phone belongs. This information comes from Cisco Unified Communications Manager. |
| Time Zone                   | Time zone for the Date/Time Group to which the phone belongs. This information comes from Cisco Unified Communications Manager. |
| Date                        | Date for the Date/Time Group to which the phone belongs. This information comes from Cisco Unified Communications Manager. |
| FIPS Mode Enabled           | Indicates if the Federal Information Processing Standard (FIPS) Mode is enabled. |

**Network Setup**

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

You can view and set many of these items from the Network Setup menu on the Cisco Unified IP Phone. For more information, see Cisco Unified IP Phone Installation, on page 59.
To display the Network Setup area, access the web page for the phone as described in Access Web Page for Phone, on page 284, and then click the Network Setup hyperlink.

**Table 44: Network Setup Area Items**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Server</td>
<td>IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains the IP address.</td>
</tr>
<tr>
<td>BOOTP Server</td>
<td>Indicates whether the phone obtains the configuration from a Bootstrap Protocol (BootP) server.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Media Access Control (MAC) address of the phone.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Host name that the DHCP server assigned to the phone.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Name of the Domain Name System (DNS) domain in which the phone resides.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Internet Protocol (IP) address of the phone.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Subnet mask that the phone uses.</td>
</tr>
<tr>
<td>TFTP Server 1</td>
<td>Primary Trivial File Transfer Protocol (TFTP) server used that the phone uses.</td>
</tr>
<tr>
<td>TFTP Server 2</td>
<td>Backup Trivial File Transfer Protocol (TFTP) server used that the phone uses.</td>
</tr>
<tr>
<td>Default Router 1</td>
<td>Default router used that the phone uses.</td>
</tr>
<tr>
<td>DNS Server 1–3</td>
<td>Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2 and 3) that the phone uses.</td>
</tr>
<tr>
<td>Operational VLAN ID</td>
<td>Operational Virtual Local Area Network (VLAN) that is configured on a Cisco Catalyst switch in which the phone is a member.</td>
</tr>
<tr>
<td>Admin VLAN ID</td>
<td>Auxiliary VLAN in which the phone is a member.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Unified CM           | Host names or IP addresses, in prioritized order, of the Cisco Unified Communications Manager servers with which the phone can register. An item can also show the IP address of an SRST router that is capable of providing limited Cisco Unified Communications Manager functionality, if such a router is available. For an available server, an item shows the Cisco Unified Communications Manager server IP address and one of the following states:  
  • Active: Cisco Unified Communications Manager server from which the phone is currently receiving call-processing services  
  • Standby: Cisco Unified Communications Manager server to which the phone switches if the current server becomes unavailable  
  • Blank: No current connection to this Cisco Unified Communications Manager server  
An item may also include the Survivable Remote Site Telephony (SRST) designation, which identifies an SRST router capable of providing Cisco Unified Communications Manager functionality with a limited feature set. This router assumes control of call processing if all other Cisco Unified Communications Manager servers become unreachable. The SRST Cisco Unified Communications Manager always appears last in the list of servers, even if it is active. You configure the SRST router address in the Device Pool section in Cisco Unified Communications Manager Configuration window. |
<p>| Information URL      | URL of the help text that appears on the phone.                                                                                                                                                             |
| Directories URL      | URL of the server from which the phone obtains directory information.                                                                                                                                       |
| Messages URL         | URL of the server from which the phone obtains message services.                                                                                                                                             |
| Services URL         | URL of the server from which the phone obtains Cisco Unified IP Phone services.                                                                                                                               |
| DHCP Enabled         | Indicates whether the phone uses DHCP.                                                                                                                                                                     |
| DHCP Address Released| Indicates the setting of the DHCP Address Released option on the phone Network Configuration menu.                                                                                                         |
| Alternate TFTP       | Indicates whether the phone is using an alternative TFTP server.                                                                                                                                             |
| Idle URL             | URL that the phone displays when the phone is idle for the time that the Idle URL Time field specifies and no menu is open.                                                                               |
| Idle URL Time        | Number of seconds that the phone is idle and no menu is open before the XML service that the Idle URL specifies activates.                                                                                |
| Proxy Server URL     | URL of proxy server, which makes HTTP requests to nonlocal host addresses on behalf of the phone HTTP client and provides responses from the nonlocal host to the phone HTTP client. |</p>
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication URL</td>
<td>URL that the phone uses to validate requests that are made to the phone web server.</td>
</tr>
<tr>
<td>SW Port Setup</td>
<td>Speed and duplex of the switch port, where:</td>
</tr>
<tr>
<td></td>
<td>• A = Auto Negotiate</td>
</tr>
<tr>
<td></td>
<td>• 10H = 10-BaseT/half duplex</td>
</tr>
<tr>
<td></td>
<td>• 10F = 10-BaseT/full duplex</td>
</tr>
<tr>
<td></td>
<td>• 100H = 100-BaseT/half duplex</td>
</tr>
<tr>
<td></td>
<td>• 100F = 100-BaseT/full duplex</td>
</tr>
<tr>
<td></td>
<td>• 1000F = 1000-BaseT/full duplex</td>
</tr>
<tr>
<td></td>
<td>• No Link = No connection to the switch port</td>
</tr>
<tr>
<td>PC Port Setup</td>
<td>Speed and duplex of the switch port, where:</td>
</tr>
<tr>
<td></td>
<td>• A = Auto Negotiate</td>
</tr>
<tr>
<td></td>
<td>• 10H = 10-BaseT/half duplex</td>
</tr>
<tr>
<td></td>
<td>• 10F = 10-BaseT/full duplex</td>
</tr>
<tr>
<td></td>
<td>• 100H = 100-BaseT/half duplex</td>
</tr>
<tr>
<td></td>
<td>• 100F = 100-BaseT/full duplex</td>
</tr>
<tr>
<td></td>
<td>• 1000F = 1000-BaseT/full duplex</td>
</tr>
<tr>
<td></td>
<td>• No Link = No connection to the PC port</td>
</tr>
<tr>
<td>TFTP Server 2</td>
<td>Backup TFTP server that the phone uses if the primary TFTP server is unavailable.</td>
</tr>
<tr>
<td>User Locale</td>
<td>User locale that associates with the phone user. Identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information.</td>
</tr>
<tr>
<td>Network Locale</td>
<td>Network locale that associates with the phone user. Identifies a set of detailed information to support the phone in a specific location, including definitions of the tones and cadences that the phone uses.</td>
</tr>
<tr>
<td>Headset Enabled</td>
<td>Indicates whether the Headset button is enabled on the phone.</td>
</tr>
<tr>
<td>User Locale Version</td>
<td>Version of the user locale that is loaded on the phone.</td>
</tr>
<tr>
<td>Network Locale Version</td>
<td>Version of the network locale that is loaded on the phone.</td>
</tr>
<tr>
<td>PC Port Disabled</td>
<td>Indicates whether the PC port on the phone is enabled or disabled.</td>
</tr>
<tr>
<td>Speaker Enabled</td>
<td>Indicates whether the speakerphone is enabled on the phone.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>GARP Enabled</td>
<td>Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.</td>
</tr>
<tr>
<td>Video Capability Enabled</td>
<td>Indicates whether the phone can participate in video calls when it connects to an appropriately equipped camera.</td>
</tr>
<tr>
<td>Voice VLAN Enabled</td>
<td>Indicates whether the phone allows a device that is attached to the PC port to access the Voice VLAN.</td>
</tr>
<tr>
<td>DSCP for Call Control</td>
<td>DSCP IP classification for call control signaling.</td>
</tr>
<tr>
<td>DSCP for Configuration</td>
<td>DSCP IP classification for any phone configuration transfer.</td>
</tr>
<tr>
<td>DSCP for Services</td>
<td>DSCP IP classification for phone-based services.</td>
</tr>
<tr>
<td>Security Mode</td>
<td>Security mode that is set for the phone.</td>
</tr>
<tr>
<td>Web Access Enabled</td>
<td>Indicates whether web access is enabled (Yes) or disabled (No) for the phone.</td>
</tr>
<tr>
<td>Span to PC Port</td>
<td>Indicates whether the phone forwards packets that are transmitted and received on the network port to the access port.</td>
</tr>
<tr>
<td>PC VLAN</td>
<td>VLAN that identifies and removes 802.1P/Q tags from packets that are sent to the PC.</td>
</tr>
<tr>
<td>CDP on PC Port</td>
<td>Indicates whether CDP is supported on the PC port (default is enabled). When CDP is disabled in Cisco Unified Communications Manager, a warning is displayed to indicate that disabling CDP on the PC port prevents CVTA from working. The current PC and switch port CDP values are shown in the Settings menu.</td>
</tr>
<tr>
<td>CDP on SW Port</td>
<td>Indicates whether CDP support exists on the switch port (default is enabled). Enable CDP on the switch port for VLAN assignment for the phone, power negotiation, QoS management, and 802.1x security. Enable CDP on the switch port when the phone connects to a Cisco switch. When CDP is disabled in Cisco Unified Communications Manager, a warning is presented, indicating that CDP should be disabled on the switch port only if the phone connects to a non-Cisco switch. The current PC and switch port CDP values are shown on the Settings menu.</td>
</tr>
<tr>
<td>LLDP-MED: SW Port</td>
<td>Indicates whether Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) is enabled on the switch port.</td>
</tr>
<tr>
<td>LLDP: PC Port</td>
<td>Indicates whether Link Layer Discovery Protocol (LLDP) is enabled on the PC port.</td>
</tr>
</tbody>
</table>
Advertises the phone power priority to the switch, thus enabling the switch to appropriately provide power to the phones. Settings include:

- Unknown: This is the default value.
- Low
- High
- Critical

Identifies the asset ID that is assigned to the phone for inventory management.

### Network Statistics

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

- Ethernet Information: Displays information about Ethernet traffic.
- Access: 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.

### Ethernet Information Web Page

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

**Table 45: Ethernet Information Items**

<table>
<thead>
<tr>
<th>Description</th>
<th>Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of packets that the phone transmits.</td>
<td>Rx Frames</td>
</tr>
<tr>
<td>Total number of broadcast packets that the phone transmits.</td>
<td>Rx broadcast</td>
</tr>
<tr>
<td>Total number of multicast packets that the phone transmits.</td>
<td>Rx multicast</td>
</tr>
<tr>
<td>Total number of unicast packets that the phone transmits.</td>
<td>Rx unicast</td>
</tr>
<tr>
<td>Total number of packets received by the phone.</td>
<td>Rx Frames</td>
</tr>
<tr>
<td>Total number of broadcast packets that the phone receives.</td>
<td>Rx broadcast</td>
</tr>
<tr>
<td>Total number of multicast packets that the phone receives.</td>
<td>Rx multicast</td>
</tr>
<tr>
<td>Total number of unicast packets that the phone receives.</td>
<td>Rx unicast</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Rx PacketNoDes</td>
<td>Total number of shed packets that the no Direct Memory Access (DMA) descriptor causes.</td>
</tr>
</tbody>
</table>

**Access Area and Network Area Web Pages**

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

**Table 46: Access Area and Network Area Fields**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx totalPkt</td>
<td>Total number of packets that the phone received.</td>
</tr>
<tr>
<td>Rx crcErr</td>
<td>Total number of packets that were received with CRC failed.</td>
</tr>
<tr>
<td>Rx alignErr</td>
<td>Total number of packets between 64 and 1522 bytes in length that were received and that have a bad Frame Check Sequence (FCS).</td>
</tr>
<tr>
<td>Rx multicast</td>
<td>Total number of multicast packets that the phone received.</td>
</tr>
<tr>
<td>Rx broadcast</td>
<td>Total number of broadcast packets that the phone received.</td>
</tr>
<tr>
<td>Rx unicast</td>
<td>Total number of unicast packets that the phone received.</td>
</tr>
<tr>
<td>Rx shortErr</td>
<td>Total number of received FCS error packets or Align error packets that are less than 64 bytes in size.</td>
</tr>
<tr>
<td>Rx shortGood</td>
<td>Total number of received good packets that are less than 64 bytes size.</td>
</tr>
<tr>
<td>Rx longGood</td>
<td>Total number of received good packets that are greater than 1522 bytes in size.</td>
</tr>
<tr>
<td>Rx longErr</td>
<td>Total number of received FCS error packets or Align error packets that are greater than 1522 bytes in size.</td>
</tr>
<tr>
<td>Rx size64</td>
<td>Total number of received packets, including bad packets, that are between 0 and 64 bytes in size.</td>
</tr>
<tr>
<td>Rx size65to127</td>
<td>Total number of received packets, including bad packets, that are between 65 and 127 bytes in size.</td>
</tr>
<tr>
<td>Rx size128to255</td>
<td>Total number of received packets, including bad packets, that are between 128 and 255 bytes in size.</td>
</tr>
<tr>
<td>Rx size256to511</td>
<td>Total number of received packets, including bad packets, that are between 256 and 511 bytes in size.</td>
</tr>
<tr>
<td>Rx size512to1023</td>
<td>Total number of received packets, including bad packets, that are between 512 and 1023 bytes in size.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Rx size 1024 to 1518</td>
<td>Total number of received packets, including bad packets, that are between 1024 and 1518 bytes in size.</td>
</tr>
<tr>
<td>Rx token Drop</td>
<td>Total number of packets that were dropped due to lack of resources (for example, FIFO overflow).</td>
</tr>
<tr>
<td>Tx excess Defer</td>
<td>Total number of packets that were delayed from transmitting due to busy medium.</td>
</tr>
<tr>
<td>Tx late Collision</td>
<td>Number of times that collisions occurred later than 512 bit times after the start of packet transmission.</td>
</tr>
<tr>
<td>Tx total Good Pkt</td>
<td>Total number of good packets (multicast, broadcast, and unicast) that the phone received.</td>
</tr>
<tr>
<td>Tx Collisions</td>
<td>Total number of collisions that occurred while a packet was transmitted.</td>
</tr>
<tr>
<td>Tx excess Length</td>
<td>Total number of packets that were not transmitted because the packet experienced 16 transmission attempts.</td>
</tr>
<tr>
<td>Tx broadcast</td>
<td>Total number of broadcast packets that the phone transmitted.</td>
</tr>
<tr>
<td>Tx multicast</td>
<td>Total number of multicast packets that the phone transmitted.</td>
</tr>
<tr>
<td>LLDP Frames Out Total</td>
<td>Total number of LLDP frames that the phone sent out.</td>
</tr>
<tr>
<td>LLDP Age outs Total</td>
<td>Total number of LLDP frames that timed out in the cache.</td>
</tr>
<tr>
<td>LLDP Frames Discarded Total</td>
<td>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.</td>
</tr>
<tr>
<td>LLDP Frames In Errors Total</td>
<td>Total number of LLDP frames that were received with one or more detectable errors.</td>
</tr>
<tr>
<td>LLDP Frames In Total</td>
<td>Total number of LLDP frames that the phone receives.</td>
</tr>
<tr>
<td>LLDP TLV Discarded Total</td>
<td>Total number of LLDP TLVs that are discarded.</td>
</tr>
<tr>
<td>LLDP TLV Unrecognized Total</td>
<td>Total number of LLDP TLVs that are not recognized on the phone.</td>
</tr>
<tr>
<td>CDP Neighbor Device ID</td>
<td>Identifier of a device connected to this port that CDP discovered.</td>
</tr>
<tr>
<td>CDP Neighbor IP Address</td>
<td>IP address of the neighbor device discovered that CDP protocol discovered.</td>
</tr>
<tr>
<td>CDP Neighbor Port</td>
<td>Neighbor device port to which the phone is connected discovered by CDP protocol.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LLDP Neighbor Device ID</td>
<td>Identifier of a device connected to this port discovered by LLDP discovered.</td>
</tr>
<tr>
<td>LLDP Neighbor IP Address</td>
<td>IP address of the neighbor device that LLDP protocol discovered.</td>
</tr>
<tr>
<td>LLDP Neighbor Port</td>
<td>Neighbor device port to which the phone connects that LLDP protocol discovered.</td>
</tr>
<tr>
<td>Port Information</td>
<td>Speed and duplex information.</td>
</tr>
</tbody>
</table>

**Device Logs**

The following device log hyperlinks on a phone web page provide information that helps to monitor and troubleshoot 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.
- **Debug Display**: Displays debug messages that might be useful to Cisco TAC if you require assistance with troubleshooting.

**Streaming Statistics**

A Cisco Unified IP Phone can stream information to and from up to three devices simultaneously. A phone streams information when it is on a call or is running a service that sends or receives audio or data. The Streaming statistics areas on a phone web page provide information about the streams.

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

*Table 47: Streaming Statistics area items*

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Address</td>
<td>IP address and UDP port of the destination of the stream.</td>
</tr>
<tr>
<td>Local Address</td>
<td>IP address and UDP port of the phone.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Internal time stamp indicates when Cisco Unified Communications Manager requested that the phone start transmitting packets.</td>
</tr>
<tr>
<td>Stream Status</td>
<td>Indication of whether streaming is active or not.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Host Name</td>
<td>Unique, fixed name that is automatically assigned to the phone based on the MAC address.</td>
</tr>
<tr>
<td>Sender Packets</td>
<td>Total number of RTP data packets that the phone transmitted since it started this connection. The value is 0 if the connection is set to receive-only mode.</td>
</tr>
<tr>
<td>Sender Octets</td>
<td>Total number of payload octets that the phone transmitted in RTP data packets since it started this connection. The value is 0 if the connection is set to receive-only mode.</td>
</tr>
<tr>
<td>Sender Codec</td>
<td>Type of audio encoding that is for the transmitted stream.</td>
</tr>
<tr>
<td>Sender Reports Sent</td>
<td>Number of times the RTCP Sender Report has been sent.</td>
</tr>
<tr>
<td>(see note)</td>
<td></td>
</tr>
<tr>
<td>Sender Report Time Sent</td>
<td>Internal time-stamp indication as to when the last RTCP Sender Report was sent.</td>
</tr>
<tr>
<td>(see note)</td>
<td></td>
</tr>
<tr>
<td>Rcvr Lost Packets</td>
<td>Total number of RTP data packets that have been lost since data reception started on this connection. Defined as the number of expected packets less the number of packets actually received, where the number of received packets includes any that are late or are duplicates. The value displays as 0 if the connection was set to send-only mode.</td>
</tr>
<tr>
<td>Avg Jitter</td>
<td>Estimate of mean deviation of the RTP data packet interarrival time, measured in milliseconds. The value displays as 0 if the connection was set to send-only mode.</td>
</tr>
<tr>
<td>Rcvr Codec</td>
<td>Type of audio encoding that is used for the received stream.</td>
</tr>
<tr>
<td>Rcvr Reports Sent</td>
<td>Number of times the RTCP Receiver Reports have been sent.</td>
</tr>
<tr>
<td>(see note)</td>
<td></td>
</tr>
<tr>
<td>Rcvr Report Time Sent</td>
<td>Internal time-stamp indication as to when a RTCP Receiver Report was sent.</td>
</tr>
<tr>
<td>(see note)</td>
<td></td>
</tr>
<tr>
<td>Rcvr Packets</td>
<td>Total number of RTP data packets that the phone has received since data reception started on this connection. Includes packets that were received from different sources if this call is a multicast call. The value displays as 0 if the connection was set to send-only mode.</td>
</tr>
<tr>
<td>Rcvr Octets</td>
<td>Total number of payload octets that the device received in RTP data packets since reception started on the connection. Includes packets that were received from different sources if this call is a multicast call. The value displays as 0 if the connection was set to send-only mode.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cumulative Conceal Ratio</td>
<td>Total number of concealment frames divided by total number of speech frames that were received from the start of the voice stream.</td>
</tr>
<tr>
<td>Interval Conceal Ratio</td>
<td>Ratio of concealment frames to speech frames in the preceding 3-second interval of active speech. If voice activity detection (VAD) is in use, a longer interval might be required to accumulate three seconds of active speech.</td>
</tr>
<tr>
<td>Max Conceal Ratio</td>
<td>Highest interval concealment ratio from the start of the voice stream.</td>
</tr>
<tr>
<td>MOS LQK</td>
<td>Score that is an objective estimate of the mean opinion score (MOS) for listening quality (LQK) that rates from 5 (excellent) to 1 (bad). This score is based on audible concealment events that are to frame loss in the preceding eight-second interval of the voice stream. For more information, see Voice Quality Monitoring, on page 330. <strong>Note</strong> The MOS LQK score can vary due to the codec type that the Cisco Unified IP Phone uses.</td>
</tr>
<tr>
<td>Avg MOS LQK</td>
<td>Average MOS LQK score that was observed for the entire voice stream.</td>
</tr>
<tr>
<td>Min MOS LQK</td>
<td>Lowest MOS LQK score that was observed from the start of the voice stream.</td>
</tr>
<tr>
<td>Max MOS LQK</td>
<td>Baseline or highest MOS LQK score that was observed from start of the voice stream.</td>
</tr>
<tr>
<td>MOS LQK Version</td>
<td>Version of the Cisco proprietary algorithm that is used to calculate MOS LQK scores.</td>
</tr>
<tr>
<td>Conceal Secs</td>
<td>Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).</td>
</tr>
<tr>
<td>Severely Conceal Secs</td>
<td>Number of seconds that have more than five percent concealment events (lost frames) from the start of the voice stream.</td>
</tr>
<tr>
<td>Latency (see note)</td>
<td>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.</td>
</tr>
<tr>
<td>Max Jitter</td>
<td>Maximum value of instantaneous jitter, in milliseconds.</td>
</tr>
<tr>
<td>Sender Size</td>
<td>RTP packet size, in milliseconds, for the transmitted stream.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Sender Reports Received</td>
<td>Number of times RTCP Sender Reports have been received.</td>
</tr>
<tr>
<td>(see note)</td>
<td></td>
</tr>
<tr>
<td>Sender Report Time Received</td>
<td>Most recent time when an RTCP Sender Report was received.</td>
</tr>
<tr>
<td>(see note)</td>
<td></td>
</tr>
<tr>
<td>Rcvr Size</td>
<td>RTP packet size, in milliseconds, for the received stream.</td>
</tr>
<tr>
<td>Rcvr Discarded</td>
<td>RTP packets that were received from the network but were discarded from the</td>
</tr>
<tr>
<td></td>
<td>jitter buffers.</td>
</tr>
<tr>
<td>Rcvr Reports Received</td>
<td>Number of times RTCP Receiver Reports have been received.</td>
</tr>
<tr>
<td>(see note)</td>
<td></td>
</tr>
<tr>
<td>Rcvr Report Time Received</td>
<td>Most recent time when an RTCP Receiver Report was received.</td>
</tr>
<tr>
<td>(see note)</td>
<td></td>
</tr>
</tbody>
</table>

### Voice Quality Metrics

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cumulative Conceal Ratio</td>
<td>Total number of concealment frames divided by total number of speech frames</td>
</tr>
<tr>
<td></td>
<td>that were received from the start of the voice stream.</td>
</tr>
<tr>
<td>Interval Conceal Ratio</td>
<td>Ratio of concealment frames to speech frames in preceding three-second</td>
</tr>
<tr>
<td></td>
<td>interval of active speech. If voice activity detection (VAD) is in use, a</td>
</tr>
<tr>
<td></td>
<td>longer interval might be required to accumulate 3 seconds of active speech.</td>
</tr>
<tr>
<td>Max Conceal Ratio</td>
<td>Highest interval concealment ratio from start of the voice stream.</td>
</tr>
<tr>
<td>Conceal Secs</td>
<td>Number of seconds that have concealment events (lost frames) from the start</td>
</tr>
<tr>
<td></td>
<td>of the voice stream (includes severely concealed seconds).</td>
</tr>
<tr>
<td>Severely Conceal Secs</td>
<td>Number of seconds that have more than five percent concealment events (lost</td>
</tr>
<tr>
<td></td>
<td>frames) from the start of the voice stream.</td>
</tr>
</tbody>
</table>

---

**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.
• ModelInfo 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 CallInfo, 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 LineInfo, 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 ModelInfo, 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
<?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>
</CiscoIPPhoneCallInfo>
</CiscoIPPhoneCallLineInfo>
```
Sample LineInfo Output

The following XML code is an example of the output from the LineInfo command.

```xml
<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
<?xml version="1.0" encoding="utf-8"?>
<CiscoIPPhoneModeInfo>
  <PlaneTitle>Applications</PlaneTitle>
  <PlaneFieldCount>12</PlaneFieldCount>
  <PlaneSoftKeyIndex>0</PlaneSoftKeyIndex>
  <PlaneSoftKeyMask>0</PlaneSoftKeyMask>
  <Prompt/>
  <Notify/>
  <Status>
    <CiscoIPPhoneFields>
      <FieldType>0</FieldType>
      <FieldAttr/>
    </CiscoIPPhoneFields>
  </Status>
</CiscoIPPhoneModeInfo>
```
Request Information from the Phone in XML

```xml
<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 17

Troubleshooting

- General Troubleshooting Information, page 301
- Startup Problems, page 303
- Phone Reset Problems, page 306
- Phone Cannot Connect to LAN, page 309
- Cisco IP Phone Security Problems, page 309
- Camera, Audio, and Video Problems, page 313
- VXC VPN Troubleshooting, page 318
- General Telephone Call Problems, page 319
- Troubleshooting Procedures, page 320
- Additional Troubleshooting Information, page 325

General Troubleshooting Information

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

Table 48: Cisco IP Phone troubleshooting

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

<table>
<thead>
<tr>
<th>Moving a network connection from the phone to a workstation</th>
<th>If you power your phone through the network connection, you must be careful if you decide to unplug the network connection of the phone and plug the cable into a desktop computer.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Caution</strong> The network card in the computer cannot receive power through the network connection; if power comes through the connection, the network card can be destroyed. To protect a network card, wait 10 seconds or longer after unplugging the cable from the phone before plugging it into a computer. This delay gives the switch enough time to recognize that there is no longer a phone on the line and to stop providing power to the cable.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Changing the telephone configuration</th>
<th>By default, the network configuration options are locked to prevent users from making changes that could impact their network connectivity. You must unlock the network configuration options before you can configure them. See Apply a Phone Password, on page 64 for details.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong> If the administrator password is not set in common phone profile, then user can modify the network settings.</td>
<td></td>
</tr>
</tbody>
</table>

| Codec mismatch between the phone and another device | The RxType and the TxType statistics show the codec that is used for a conversation between this Cisco IP Phone and the other device. The values of these statistics should match. If they do not, verify that the other device can handle the codec conversation, or that a transcoder is in place to handle the service. |

| Sound sample mismatch between the phone and another device | The RxSize and the TxSize statistics show the size of the voice packets that are used in a conversation between this Cisco IP Phone and the other device. The values of these statistics should match. |

<table>
<thead>
<tr>
<th>Loopback condition</th>
<th>A loopback condition can occur when the following conditions are met:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• The SW Port Configuration option in the Network Configuration menu on the phone is set to 10 Half (10-BaseT/half duplex).</td>
</tr>
<tr>
<td></td>
<td>• The phone receives power from an external power supply.</td>
</tr>
<tr>
<td></td>
<td>• The phone is powered down (the power supply is disconnected).</td>
</tr>
<tr>
<td></td>
<td>In this case, the switch port on the phone can become disabled and the following message appears in the switch console log:</td>
</tr>
<tr>
<td></td>
<td>HALF_DUX_COLLISION_EXCEED_THRESHOLD</td>
</tr>
<tr>
<td></td>
<td>To resolve this problem, reenable the port from the switch.</td>
</tr>
</tbody>
</table>
Startup Problems

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

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

Related Topics

Phone Startup Process, on page 85

Cisco IP Phone Does Not Go Through the Normal Startup Process

Problem

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

Cause

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

Solution

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

• Verify that the network port is functional:
  ◦ Exchange the Ethernet cables with cables that you know are functional.
  ◦ Disconnect a functioning Cisco IP Phone from another port and connect it to this network port to verify that the port is active.
  ◦ Connect the Cisco IP Phone that does not start up to a different network port that is known to be good.
  ◦ Connect the Cisco IP Phone that does not start up directly to the port on the switch, eliminating the patch panel connection in the office.

• Verify that the phone is receiving power:
  ◦ If you are using external power, verify that the electrical outlet is functional.
  ◦ If you are using in-line power, use the external power supply instead.
  ◦ If you are using the external power supply, switch with a unit that you know to be functional.

• If the phone still does not start up properly, power up the phone with the handset off-hook. When the phone is powered up in this way, it attempts to launch a backup software image.

• If the phone still does not start up properly, perform a factory reset of the phone.
• After you attempt these solutions, if the phone screen on the Cisco IP Phone does not display any characters after at least five minutes, contact a Cisco technical support representative for additional assistance.

Related Topics

Phone Startup Process, on page 85

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 320 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 265

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 321

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 322

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.

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 324.
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 91 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 90.

If the phone is already in the Cisco Unified Communications Manager database, the configuration file may be damaged. See Configuration File Corruption, on page 306 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 322

**Phone Resets Due to Incorrect Static IP Address**

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

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

**Phone Resets During Heavy Network Usage**

**Problem**
If the phone appears to reset during heavy network usage, it is likely that you do not have a voice VLAN configured.
Solution
Isolating the phones on a separate auxiliary VLAN increases the quality of the voice traffic.

Phone Resets Due to Intentional Reset

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

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

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

Phone Resets Due to DNS or Other Connectivity Issues

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

Solution
If the phone continues to reset, eliminate DNS or other connectivity errors by following the procedure in Determine DNS or Connectivity Issues, on page 321.

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.

802.1X Authentication Problems

801.1X authentication problems can be broken into the categories that are described in the following table.

Table 49: 802.1X Authentication Problem Identification

<table>
<thead>
<tr>
<th>If all the following conditions apply,</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Phone cannot obtain a DHCP-assigned IP address.</td>
<td>802.1X Enabled on Phone but Phone Does Not Authenticate, on page 312</td>
</tr>
<tr>
<td>• Phone does not register with Cisco Unified Communications Manager.</td>
<td></td>
</tr>
<tr>
<td>• Phone status displays Configuring IP or Registering.</td>
<td></td>
</tr>
<tr>
<td>• 802.1X Authentication Status displays Held.</td>
<td></td>
</tr>
<tr>
<td>• Status menu 802.1X status displays Failed</td>
<td></td>
</tr>
</tbody>
</table>
### 802.1X Not Enabled

**Problem**
The phone does not have 802.1X configured.

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

**Solution**
To resolve this problem, check the 802.1X and shared secret configuration. See Identify 802.1X Authentication Problems, on page 323.

---

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

**Problem**
The phone cannot authenticate.

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

**Solution**
To resolve this problem, check the 802.1X and shared secret configuration. See Identify 802.1X Authentication Problems, on page 323.

---

<table>
<thead>
<tr>
<th>If all the following conditions apply,</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Phone cannot obtain a DHCP-assigned IP address.</td>
<td>802.1X Not Enabled, on page 312</td>
</tr>
<tr>
<td>• Phone does not register with Cisco Unified Communications Manager.</td>
<td></td>
</tr>
<tr>
<td>• Phone status displays Configuring IP or Registering.</td>
<td></td>
</tr>
<tr>
<td>• 802.1X Authentication Status displays Disabled.</td>
<td></td>
</tr>
<tr>
<td>• Status menu displays that the DHCP status has timed out.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>If all the following conditions apply,</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Phone cannot obtain a DHCP-assigned IP address.</td>
<td>Factory Reset of Phone Has Deleted 802.1X Shared Secret, on page 313</td>
</tr>
<tr>
<td>• Phone does not register with Cisco Unified Communications Manager.</td>
<td></td>
</tr>
<tr>
<td>• Phone status display as Configuring IP or Registering.</td>
<td></td>
</tr>
<tr>
<td>• You are unable to access phone menus to verify 802.1X status.</td>
<td></td>
</tr>
</tbody>
</table>
Cause
These errors typically indicate that 802.1X authentication is not enabled on the phone.

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

Factory Reset of Phone Has Deleted 802.1X Shared Secret

Problem
After a reset, the phone does not authenticate.

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

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

Related Topics
Basic Reset

Camera, Audio, and Video Problems

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

No Video

Problem
The phone does not detect the camera or no picture appears on the screen.

Solution
Check the following conditions:

• Verify that the camera is connected properly by unplugging and reconnecting the camera to the phone.
• Verify that video is enabled in Cisco Unified Communications Manager.
• Check the resolution of the transmitting endpoint. Cisco Unified IP Phone 8961, 9951, and 9971 does not display videos that use a resolution higher than VGA. If the other endpoint transmits at a resolution greater than VGA, such a transmission results in a black screen.
• Verify that packets are being received. Check the Rcvr Packets (would be zero in this case) in Administrator Settings > Status > Call Statistics > Video > Video Statistics.
• Ensure that the transmitting phone has the camera shutter completely open.

**Phone Display Is Wavy**

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

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

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

**Video Freezes**

**Problem**
The video is frozen.

**Cause**
When the phone stops receiving video packets, the video display pauses and displays the last decoded video frame.

**Solution**
• Check whether the received packets count is incrementing or not, by navigating to Administrator Settings > Status > Call Statistics > Video > Video statistics > Rcvr Packets statistics.
• Put the call on hold and then resume the call to clear the issue.
• If the transmitting phone is an IP phone, check the LED on top of the camera. If no light is illuminated (either green or red), then the remote camera might not be transmitting video.

**Video Is Too Dark**

**Problem**
Video that the camera transmits is too dark or the subject too dark in the video.

**Solution**
The lighting conditions within the field of view of the camera affect the brightness of the video.
• Adjust the View Area for your camera. Try moving the location of the camera and check whether the brightness improves.
• Adjust the camera brightness by navigating to Accessories > Cisco Unified Video Camera > Brightness and adjusting the brightness settings.

Video Is Poor Quality or Grainy

Problem
The phone has poor video quality/grainy video.

Solution
When the resolution of the received video is grainy, the user may perceive that the video quality is poor. However, this does not cause video distortion or artifacts.

• Check the Cisco Unified Communications Manager bandwidth settings under Region settings.
• Check the Receiver Resolution in video statistics. This may be an issue if the Cisco Unified Communications Manager bandwidth setting limits the resolution to less than CIF, (352x288). Try increasing the bandwidth to at least 275 kbps.

Video Is Blocky or Distorted

Problem
The phone has blocky or distorted video.

Cause
Blocky or distorted video is generally a symptom of a degraded network. Endpoints that do not closely adhere to video transmission standards can also cause blocky or distorted video.

Solution
If the network is degraded, navigate to Administrator Settings > Status > CallStatistics > Video > Video Statistics and check the following fields:

• Rcvr Lost Packets
• Rcvr Discarded
• Avg Jitter
• Max Jitter

Video Is Slow Moving or Jittery

Problem
The phone has slow moving video or jittery video.
Cause
The frame rate of the received video is low.

Solution
Check the rate by navigating to Administrator Settings > Status > CallStatistics > Video > Video Statistics and checking the Rcvr Frame Rate field. Frame rates of fewer than 15 fps result in slow-moving video.

Audio/Video Is Not Synchronized

Problem
Audio/Video synchronization is poor.

Solution
To resolve synchronization issues:

• Check whether RTCP is enabled in Cisco Unified Communications Manager.
• Check for a degraded network connection by navigating to Administrator Settings > Status > Call Statistics > Video > Video Statistics and checking the Avg Jitter and Max Jitter values.
• Place the call on hold and then resume the call to restore audio/video synchronization.

No Audio

Problem
The recipient endpoint only sees a mute image.

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

No Speech Path

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

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

Problem
A user complains of choppy speech on a call.

Cause
There may be a mismatch in the jitter configuration.

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

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

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

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

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

Video Distorted or Pixilated

Problem
The video on the Cisco Unified IP Phone 9951 appears distorted or pixilated and the phone is using a 100-BaseT/full duplex connection.

Cause
The transmission speed of the connection is insufficient for the audio and video demands of the phone.

Solution
Upgrade the transmission speed to 1000-BaseT/full duplex.
VXC VPN Troubleshooting

When you are experiencing problems associated with the Virtualization Experience Client (VXC) Virtual Private Network (VPN), use this section to troubleshoot the problems.

Phone Does Not Set Up VXC VPN Tunnel

Problem
The VXC is on and physically connected with phone using the spine connector and network cable, but the VXC VPN status is not connected.

Solution
Perform the following steps:
1. Verify that:
   a. The phone is powered by the adapter.
   b. VXC is shown in accessories menu. If not, power cycle the phone.
   c. VPN status is connected.
2. Power cycle VXC device.

Phone Does Not Connect with VXC VPN

Problem
The phone cannot connect to the VXC VPN.

Solution
Perform the following steps:
• Check that the VXC is showing in the phone Accessories menu.
• Check the VXC VPN status in the phone VPN menu.
• In the Cisco Unified Communications Manager, check that the Enable VXC VPN for MAC fields contains all Fs or is the same MAC address of the user's VXC device.
• Check that the VXC VPN status is connected.
• Check that the Alternate TFTP is enabled and that the correct TFTP IP address is configured on the phone.
• Check that the VXC is physically connected in the PC port of the phone.
• Check that the VXC device gets an IP address from the phone, and not from the local router.
• From the VXC device, use the ping command to check that the device can successfully contact the Cisco Unified Communications Manager.
General Telephone Call Problems

The following sections help troubleshoot general telephone call problems.

VPN-Connected Phone Does Not Log Calls

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

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

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

Related Topics
Set Up Remote Phone, on page 320

Phone Call Cannot Be Established

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

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

Solution
1 Verify the following:
   a The Ethernet cable is attached.
   b The Cisco CallManager service is running on the Cisco Unified Communications Manager server.
   c Both phones are registered to the same Cisco Unified Communications Manager.

2 Audio server debug and capture logs are enabled for both phones. If needed, enable Java debug.
Phone Does Not Recognize DTMF Digits or Digits Are Delayed

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

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

Solution
Keys should not be pressed rapidly.

Troubleshooting Procedures
These procedures can be used to identify and correct problems.

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

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

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

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>On the phone, select <strong>Applications</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Navigate to the <strong>IPv4 Settings</strong> window.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Scroll to the Alternate TFTP option and set the field to <strong>Yes</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the TFTP Server 1 field, set the TFTP server address.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Save the changes.</td>
</tr>
</tbody>
</table>
Check TFTP Settings

**Procedure**

**Step 1**  You can determine the IP address of the TFTP server that the phone uses by pressing **Applications**, then selecting **Administrator Settings > Network Setup > Ethernet Setup > IPv4 Setup > TFTP Server 1**.

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

**Step 3**  If you are using DHCP, the phone obtains the address for the TFTP server from the DHCP server. Check that the IP address is configured in Option 150.

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

**Step 5**  If the local DHCP does not offer the correct TFTP address, enable the phone to use an alternate TFTP server. This is often necessary in VPN scenario.

**Related Topics**

   Phone Cannot Connect to TFTP Server, on page 304

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
   Determine the Phone MAC Address, on page 90
Check DHCP Settings

Procedure

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

Step 2 Select Administrator Settings > Network Setup > Ethernet Setup > IPv4 Setup, and look at the following options:

• DHCP Server: If you have assigned a static IP address to the phone, you do not need to enter a value for the DHCP Server option. However, if you are using a DHCP server, this option must have a value. If no value is found, check your IP routing and VLAN configuration. See the Troubleshooting Switch Port and Interface Problems document, available at this URL:

• IP Address, Subnet Mask, Default Router: If you have assigned a static IP address to the phone, you must manually enter settings for these options.

Step 3 If you are using DHCP, check the IP addresses that your DHCP server distributes. See the Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks document, available at this URL:

Related Topics

Phone Cannot Connect to Server, on page 305
Phone Resets Due to DHCP Setting Errors, on page 307

Create New Phone Configuration File

Note

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

Phone Addition Methods, on page 91

### Identify 802.1X Authentication Problems

Procedure

**Step 1**  Verify that you have properly configured the required components.

**Step 2**  Confirm that the shared secret is configured on the phone.

- If the shared secret is configured, verify that you have the same shared secret on the authentication server.
- If the shared secret is not configured on the phone, enter it, and ensure that it matches the shared secret on the authentication server.

### Verify DNS Settings

To verify DNS settings, follow these steps:

Procedure

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

**Step 2**  Select **Administrator Settings > Network Setup > Ethernet Setup > IPv4 Setup > DNS Server 1**.

**Step 3**  You should also verify that a CNAME entry was made in the DNS server for the TFTP server and for the Cisco Unified Communications Manager system.
You must also ensure that DNS is configured to do reverse lookups.

---

**Start Service**

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

**Procedure**

**Step 1**
From Cisco Unified Communications Manager Administration, choose **Cisco Unified Serviceability** from the Navigation drop-down list and click **Go**.

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

**Step 3**
Choose the primary Cisco Unified Communications Manager server from the Server drop-down list. The window displays the service names for the server that you chose, the status of the services, and a service control panel to start or stop a service.

**Step 4**
If a service has stopped, click the corresponding radio button and then click **Start**. The Service Status symbol changes from a square to an arrow.

---

**Control Debug Information from Cisco Unified Communications Manager**

If you are experiencing phone problems that you cannot resolve, Cisco TAC can assist you. You will need to turn debugging on for the phone, reproduce the problem, turn debugging off, and send the logs to TAC for analysis.

Because debugging captures detailed information, the communication traffic can slow down the phone, making it less responsive. After you capture the logs, you should turn debugging off to ensure phone operation.

The debug information may include a single digit code that reflects the severity of the situation. Situations are graded as follows:

- 0 - Emergency
- 1 - Alert
- 2 - Critical
- 3 - Error
- 4 - Warn
- 5 - Notification
- 6 - Information
- 7 - Debugging
Contact Cisco TAC for more information and assistance.

**Procedure**

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

- Device > Device settings > Common Phone Profile
- System > Enterprise Phone Configuration
- Device > Phone

**Step 2** Set the following parameters:

- Log Profile - values: Preset (default), Default, Telephony
- Remote Log - values: Disable (default), Enable
- IPv6 Log Server or Log Server - IP address (IPv4 or IPv6 address)

**Note** When the Log Server cannot be reached, the phone stops sending debug messages.

- The format for the IPv4 Log Server address is address:<port>@@base=<0-7>;pfs=<0-1>
- The format for the IPv6 Log Server address is [address]:<port>@@base=<0-7>;pfs=<0-1>
- Where:
  - the IPv4 address is separated with dot (.)
  - the IPv6 address is separated with colon (:)

---

**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:

CHAPTER 18

Maintenance

- Phone Reset Options, page 327
- Quality Report Tool, page 330
- Voice Quality Monitoring, page 330
- Video Metrics, page 331
- Cisco Unified IP Phone Cleaning, page 332

Phone Reset Options

Performing a reset of a Cisco Unified IP Phone provides a way to recover if the phone experiences an error and resets or restores various configuration and security settings. The following types of phone resets are available:

- Restart phone
- Reset the phone to the factory default settings using phone menu
- Reset the phone to the factory default settings using phone keypad
- Reset the network configuration for the phone
- Reset the user and network configuration for the phone
- Remove the CTL file from the phone

Before you perform a factory reset, ensure that the following conditions are met:

- The phone must be on a DHCP-enabled network.
- A valid TFTP server must be set in DHCP option 150 or option 66 on the DHCP server.

The following events occur on the phone when you perform a factory reset:

- User configuration settings reset to default values.
- Network configuration settings reset to default values.
- Call histories get erased.
• Locale information resets to default values.
• Phone application gets erased, and the phone recovers by using the image in the inactive partition of flash to boot up.
• Security settings reset to default values. This includes deleting the CTL file, deleting the MD5 secret, and changing the 802.1x Device Authentication parameter to "Disabled."

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

**Related Topics**
[Text and Menu Entry from Phone, on page 65](#)

**Reset the Phone to the Factory Settings from the Keypad**
You can reset the phone to the factory settings. The reset clears all the phone parameters.

**Procedure**

**Step 1**
Remove power from the phone in one of these ways:
- Unplug the power adapter.
- Unplug the LAN cable.

**Step 2**
Press the pound (#) key and plug the phone in.

**Step 3**
When the mute button is red and the top left and right line buttons are amber, enter the following key sequence:
123456789*0#

The phone resets.

**Perform Factory Reset from Phone Menu**
To perform a factory reset of a phone,

**Procedure**

**Step 1**
Press Applications.

**Step 2**
Choose Administrator Settings > Reset Settings > All.
If required, unlock the phone options.
Related Topics

Apply a Phone Password, on page 64

Perform Network Configuration Reset

Resets network configuration settings to their default values and resets the phone. This method causes DHCP to reconfigure the IP address of the phone.

Procedure

### Step 1
From the Administrator Settings menu, if required, unlock phone options.

### Step 2
Choose Reset Settings > Network Settings.

Related Topics

Apply a Phone Password, on page 64

Perform User and Network Configuration Reset

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

Procedure

### Step 1
From the Administrator Settings menu, if required, unlock phone options.

### Step 2
Choose Reset Settings > Reset Device.

Related Topics

Apply a Phone Password, on page 64

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.
Quality Report Tool

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

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

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

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

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.

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 50: Changes to Voice Quality Metrics**

<table>
<thead>
<tr>
<th>Metric change</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conceal Ratio and Conceal Seconds increase significantly</td>
<td>Network impairment from packet loss or high jitter.</td>
</tr>
</tbody>
</table>
| 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. |
| MOS LQK scores decrease significantly               | Network impairment from packet loss or high jitter levels:                  
  • Average MOS LQK decreases may indicate widespread and uniform impairment.  
  • Individual MOS LQK decreases may indicate bursty impairment.  
  Cross-check the conceal ratio and conceal seconds for evidence of packet loss and jitter. |
| MOS LQK scores increase significantly               | • Check to see if the phone is using a different codec than expected (RxType and TxType).  
  • Check to see if the MOS LQK version changed after a firmware upgrade. |

**Note**
Voice quality metrics do not account for noise or distortion, only frame loss.

**Video Metrics**

The phones do not support video metrics. This means that you can't see the following information about the video portion of a call:
- videoContentType
- videoDuration
- numberVideoPacketsSent
• numberVideoOctetsSent
• numberVideoPacketsReceived
• numberVideoOctetsReceived
• numberVideoPacketsLost
• videoAverageJitter

Cisco Unified IP Phone Cleaning

To clean your Cisco Unified IP Phone, use only a dry soft cloth to gently wipe the phone and the phone screen. Do not apply liquids or powders directly to the phone. As with all nonweatherproof electronics, liquids and powders can damage the components and cause failures.

When the phone is in sleep mode, the touchscreen is blank and the Select button is not lit. When the phone is in this condition, you can clean the screen, as long as you know that the phone will remain asleep until after you finish cleaning. If the phone is likely to wake up during cleaning, wake it up or wait until it is awake before following the preceding cleaning instructions.
International User Support

- Unified Communications Manager Endpoints Locale Installer, page 333
- International Call Logging Support, page 333
- Language Limitation, page 334

Unified Communications Manager Endpoints Locale Installer

By default, Cisco IP Phones are set up for the English (United States) locale. To use the Cisco IP Phones in other locales, you must install the locale-specific version of the Unified Communications Manager Endpoints Locale Installer on every Cisco Unified Communications Manager server in the cluster. The Locale Installer installs the latest translated text for the phone user interface and country-specific phone tones on your system so that they are available for the Cisco IP Phones.

To access the Locale Installer required for a release, access http://software.cisco.com/download/navigator.html?mdfid=286037605&flowid=46245, navigate to your phone model, and select the Unified Communications Manager Endpoints Locale Installer link.

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

Note

The latest Locale Installer may not be immediately available; continue to check the website for updates.

International Call Logging Support

If your phone system is configured for international call logging (calling party normalization), the call logs, redial, or call directory entries may display a plus (+) symbol to represent the international escape code for your location. Depending on the configuration for your phone system, the + may be replaced with the correct international dialing code, or you may need to edit the number before dialing to manually replace the + with the international escape code for your location. In addition, while the call log or directory entry may display the full international number for the received call, the phone display may show the shortened local version of the number, without international or country codes.
Language Limitation

There is no localized Keyboard Alphanumeric Text Entry (KATE) support for the following Asian locales:

- Chinese (China)
- Chinese (Hong Kong)
- Chinese (Taiwan)
- Japanese (Japan)
- Korean (Korea Republic)

The default English (United States) KATE is presented to the user instead.

For example, the phone screen will show text in Korean, but the 2 key on the keypad will display a b c 2 A B C.