



## **Cisco Unified SIP Phone 3905 Administration Guide for Cisco Unified Communications Manager 10.0**

**First Published:** 2013-10-17

**Last Modified:** 2017-01-12

### **Americas Headquarters**

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

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

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

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

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

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

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

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

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

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

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

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

© 2017 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### Preface

#### Preface ix

Overview ix

Audience ix

Guide Conventions ix

Related Documentation xi

    Cisco Unified SIP Phone 3905 Documentation xi

    Cisco Unified Communications Manager Documentation xi

Documentation, Support, and Security Guidelines xi

    Cisco Product Security Overview xi

---

### 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 4

    Network Port Connector 4

    Computer Port Connector 5

Phone Power Requirements 6

    Power Outage 7

Cisco Unified Communications Manager Interaction 7

Network Protocols 7

VLAN Interaction 10

External Devices 11

Phone Behavior During Times of Network Congestion 12

---

### CHAPTER 2

#### Cisco Unified SIP Phone Hardware 13

Cisco Unified SIP Phone 3905	13
Phone Connections	13
Buttons and Hardware	15
Terminology Differences	17

---

**PART II****Cisco Unified SIP Phone Installation 19**

---

**CHAPTER 3****Cisco Unified SIP Phone Installation 21**

Verify Network Setup	21
Enable Autoregistration for Phones	22
Install Cisco Unified SIP Phone	23
Set Up Phone from Setup Menus	24
Apply Phone Password	25
Text and Menu Entry from Phone	26
Configure Network Settings	26
Set Domain Name Field	30
Set Admin VLAN ID Field	30
Set PC VLAN Field	30
Set SW Port Setup Field	31
Set PC Port Setup Field	31
Set DHCP Enabled Field	31
Set IP Address Field	31
Set Subnet Mask Field	32
Set Default Router Field	32
Set DNS Server Field	32
Set Alternate TFTP Field	32
Set TFTP Server 1 Field	33
Set TFTP Server 2 Field	33
Set IPv6 Fields	33
Verify Phone Startup	35

---

**CHAPTER 4****Cisco Unified Communications Manager Phone Setup 37**

Phone Configuration Files	37
Set Up Cisco Unified SIP Phone	38
Determine Phone MAC Address	42

Phone Addition Methods	42
Add Phones Individually	43
Add Phones Using BAT Phone Template	43
Add Users to Cisco Unified Communications Manager	44
Add a User from an External LDAP Directory	44
Add User Directly to Cisco Unified Communications Manager	45
Add User to End User Group	45
Associate Phones with Users	46
Perform Final End User Configuration Steps	46

---

**CHAPTER 5****Self Care Portal Management 49**

Self Care Portal Overview	49
Set Up User Access to the Self Care Portal	49
Customize the Self Care Portal Display	50

---

**PART III****Hardware and Accessory Installation 51**

---

**CHAPTER 6****Cisco Unified SIP Phone Accessories 53**

Adjust footstand	53
Install Phone on Wall Mount Plate	53
Adjust the Handset Rest	57

---

**PART IV****Cisco Unified SIP Phone Administration 59**

---

**CHAPTER 7****Cisco Unified SIP Phone Security 61**

Cisco Unified SIP Phone Security Features	61
802.1X Authentication	62
Set Up SIP MD5 Digest Authentication	63
Set Device Authentication Field	64
Set Shared Secret Field	64

---

**CHAPTER 8****Phone Features and Setup 65**

Phone Features and Setup Overview	65
Cisco IP Phone User Support	65
Telephony Features	66

- Disable Speakerphone 72
- Control Phone Web Page Access 72
- Enable Paging Support on Cisco Unified Communications Manager 72
- Set the Label for a Line 73

---

**PART V**


---

**Cisco Unified IP Phone Troubleshooting 75**
**CHAPTER 9**
**Monitoring Phone Systems 77**

- Cisco Unified SIP Phone status 77
  - Display Model Information Window 77
    - Model Information Fields 78
  - Display Status Menu 78
  - Display Status Messages Window 79
    - Status Messages 79
  - Display Network Statistics Screen 83
    - Network Statistics Fields 83
  - Display Call Statistics Window 86
    - Call Statistics Fields 87
- Cisco IP Phone Web Page 88
  - Access Web Page for Phone 88
  - Device Information 89
  - Network Setup Page 90
  - Network Statistics 94
    - Ethernet Information Web Page 95
    - Network Information Fields 96
  - Device Logs 97
  - Streaming Statistics 101

---

**CHAPTER 10**
**Troubleshooting 105**

- Troubleshooting Overview 105
- Startup Problems 105
  - Cisco IP Phone Does Not Go Through the Normal Startup Process 106
  - Cisco IP Phone Does Not Register with Cisco Unified Communications Manager 106
  - Phone Displays Error Messages 107

Phone Cannot Connect to TFTP Server or to Cisco Unified Communications Manager	
<b>107</b>	
Phone Cannot Connect to TFTP Server	<b>107</b>
Phone Cannot Connect to Server	<b>107</b>
Cisco Unified Communications Manager and TFTP Services Are Not Running	<b>108</b>
Configuration File Corruption	<b>108</b>
Cisco Unified Communications Manager Phone Registration	<b>108</b>
Cisco IP Phone Cannot Obtain IP Address	<b>109</b>
Phone Reset Problems	<b>109</b>
Phone Cannot Connect to LAN	<b>109</b>
Phone Resets Due to Intermittent Network Outages	<b>109</b>
Phone Resets Due to DHCP Setting Errors	<b>110</b>
Phone Resets Due to Incorrect Static IP Address	<b>110</b>
Phone Resets During Heavy Network Usage	<b>110</b>
Phone Resets Due to Intentional Reset	<b>110</b>
Phone Resets Due to DNS or Other Connectivity Issues	<b>111</b>
Phone Does Not Power Up	<b>111</b>
Cisco IP Phone Security Problems	<b>111</b>
802.1X Authentication Problems	<b>111</b>
802.1X Enabled on Phone but Phone Does Not Authenticate	<b>112</b>
802.1X Not Enabled	<b>113</b>
Factory Reset of Phone Has Deleted 802.1X Shared Secret	<b>113</b>
Audio and Video Problems	<b>113</b>
No Speech Path	<b>114</b>
Choppy Speech	<b>114</b>
Poor Audio Quality with Calls that Route Outside Cisco Unified Communications Manager	<b>114</b>
Phone Display Is Wavy	<b>114</b>
General Telephone Call Problems	<b>115</b>
Phone Call Cannot Be Established	<b>115</b>
Phone Does Not Recognize DTMF Digits or Digits Are Delayed	<b>115</b>
Phone Bandwidth Restrictions	<b>116</b>
Troubleshooting Procedures	<b>116</b>
Check TFTP Settings	<b>116</b>
Check DHCP Settings	<b>117</b>

- Start Service **117**
- Create New Phone Configuration File **118**
- Determine DNS or Connectivity Issues **118**
- Identify 802.1X Authentication Problems **119**
- Verify DNS Settings **119**
- Additional Troubleshooting Information **120**

---

**CHAPTER 11**

**Maintenance 121**

- Basic Reset **121**
  - Reset the Phone to the Factory Settings from the Keypad **121**
  - Perform Factory Reset from Phone Menu **122**
- Voice Quality Monitoring **122**
  - Voice Quality Troubleshooting Tips **123**
- Cisco IP Phone Cleaning **124**

---

**CHAPTER 12**

**International User Support 125**

- Unified Communications Manager Endpoints Locale Installer **125**
- International Call Logging Support **125**
- Language Limitation **126**





## Preface

---

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

## Overview

*Cisco Unified SIP Phone 3905 Administration Guide for Cisco Unified Communications Manager* provides the information you need to understand, install, configure, manage, and troubleshoot the phones on a Voice-over-IP (VoIP) network.

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

## Audience

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

## Guide Conventions

This document uses the following conventions:

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

Convention	Description
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> .
[ ]	Elements in square brackets are optional.
{ x   y   z }	Alternative keywords are grouped in braces and separated by vertical bars.
[ x   y   z ]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in <code>screen font</code> .
input font	Information you must enter is in <code>input font</code> .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .
^	The symbol ^ represents the key labeled Control - for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters such as passwords are in angle brackets.



**Note**

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



**Caution**

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

Warnings use the following convention:



**Attention**

**IMPORTANT SAFETY INSTRUCTIONS**

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

SAVE THESE INSTRUCTIONS

## Related Documentation

Use the following sections to obtain related information.

### Cisco Unified SIP Phone 3905 Documentation

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

<http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-sip-phone-3900-series/tsd-products-support-series-home.html>

### Cisco Unified Communications Manager Documentation

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

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

## Documentation, Support, and Security Guidelines

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

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

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

### Cisco Product Security Overview

This product contains cryptographic features and is subject to 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 **I**

# About the Cisco Unified IP Phone

- [Technical Details](#) , page 3
- [Cisco Unified SIP Phone Hardware](#), page 13





## Technical Details

- [Physical and Operating Environment Specifications, page 3](#)
- [Cable Specifications, page 4](#)
- [Network and Computer Port Pinouts, page 4](#)
- [Phone Power Requirements, page 6](#)
- [Cisco Unified Communications Manager Interaction, page 7](#)
- [Network Protocols, page 7](#)
- [VLAN Interaction, page 10](#)
- [External Devices, page 11](#)
- [Phone Behavior During Times of Network Congestion, page 12](#)

### Physical and Operating Environment Specifications

The following table shows the physical and operating environment specifications for the Cisco Unified SIP Phone 3905.

**Table 1: Physical and Operating Environment Specifications for the Cisco Unified SIP Phone 3905**

Specification	Value or Range
Operating temperature	32° to 104°F (0° to 40°C)
Operating relative humidity	10% to 95% (noncondensing)
Storage temperature	14° to 140°F (-10° to 60°C)
Height	8.07 in. (20.5 cm)
Width	5.91 in. (15.0 cm)

Specification	Value or Range
Depth	2.11 in. (5.35 cm) - Excluding the handset
Weight	<ul style="list-style-type: none"> <li>• 0.987 lb (447.8 g) - Phone without handset</li> <li>• 0.347 lb (157.6 g) - Handset weight</li> </ul>
Power	<ul style="list-style-type: none"> <li>• 100-240 VAC, 50-60 Hz, 0.5 A - When using the AC adapter</li> <li>• 48 VDC, 0.2 A - When using the in-line power over the network cable</li> </ul>
Cables	Category 3/5/5e for 10-Mbps cables with 4 pairs Category 5/5e for 100-Mbps cables with 4 pairs <b>Note</b> Cables have 4 pairs of wires for a total of 8 conductors.
Distance Requirements	As supported by the Ethernet Specification, it is assumed that the maximum cable length between each Cisco Unified IP Phone and the switch is 100 meters (330 feet).

## Cable Specifications

- RJ-9 jack (4-conductor) for handset connection.
- RJ-45 jack for the LAN 10/100BaseT connection (labeled 10/100 SW on the Cisco Unified SIP Phone 3905).
- RJ-45 jack for a second 10/100BaseT compliant connection.
- 48-volt power connector.

## Network and Computer Port Pinouts

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

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

### Network Port Connector

The following table describes the network port connector pinouts.



**Table 2: Network Port Connector Pinouts**

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

## Computer Port Connector

The following table describes the computer port connector pinouts.

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

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

## Phone Power Requirements

The Cisco Unified SIP Phone 3905 can be powered with external power or with Power over Ethernet (PoE). External power is provided through a separate power supply. PoE is provided by a switch through the Ethernet cable attached to a phone.



### Note

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

The following table provides guidelines for powering the Cisco Unified SIP Phone 3905.

**Table 4: Cisco Unified SIP Phone 3905 power guidelines**

Power Type	Guidelines
External power: Provided through the Cisco Unified SIP Phone 3905 Power Adapter.	The Cisco Unified SIP Phone 3905 uses the Cisco Unified SIP Phone 3905 Power Adapter.
External power: Provided through the Cisco Unified IP Phone Power Injector.	The Cisco Unified IP Phone Power Injector may be used with any Cisco Unified IP Phone. Functioning as a midspan device, the injector delivers inline power to the attached phone. The Cisco Unified IP Phone Power Injector is connected between a switch port and the IP Phone, and supports a maximum cable length of 100m between the unpowered switch and the IP Phone.
PoE power: Provided by a switch through the Ethernet cable attached to the phone.	<ul style="list-style-type: none"> <li>• The Cisco Unified SIP Phone 3905 supports IEEE 802.3af Class 1 power on signal pairs and spare pairs.</li> <li>• To ensure uninterruptible operation of the phone, make sure that the switch has a backup power supply.</li> <li>• Make sure that the CatOS or IOS version running on your switch supports your intended phone deployment. Refer to the documentation for your switch for operating system version information.</li> </ul>
External power: Provided through inline power patch panel WS-PWR-PANEL	The inline power patch panel WS-PWR-PANEL is compatible with the Cisco Unified SIP Phone 3905.

## Power Outage

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

## 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.

---

## Network Protocols

Cisco Unified IP Phones support several industry-standard and Cisco network protocols required for voice communication. The following table provides an overview of the network protocols that the Cisco Unified SIP Phone 3905 support.

**Table 5: Supported Network Protocols**

Network Protocol	Purpose	Usage Notes
Cisco Discovery Protocol (CDP)	<p>CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment.</p> <p>Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.</p>	The phone uses CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.
Dynamic Host Configuration Protocol (DHCP)	<p>DHCP dynamically allocates and assigns an IP address to network devices.</p> <p>DHCP enables you to connect an IP phone into the network and have the phone become operational without your needing to manually assign an IP address or to configure additional network parameters.</p>	<p>DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, gateway, and a TFTP server on each phone locally.</p> <p>Cisco recommends that you use DHCP custom option 150. With this method, you configure the TFTP server IP address as the option value. For additional supported DHCP configurations, go to the “Dynamic Host Configuration Protocol” chapter and the “Cisco TFTP” chapter in the <i>Cisco Unified Communications Manager System Guide</i>.</p> <p><b>Note</b> If you cannot use option 150, you may try using DHCP option 66.</p>
Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	The DHCPv6 server assigns an IPv6 address to the phone.	You must disable DHCPv6 to edit IPv6 Setup menu options.
Hypertext Transfer Protocol (HTTP)	HTTP is the standard way of transferring information and moving documents across the Internet and the web.	Cisco Unified IP Phones use HTTP for troubleshooting purposes.
IEEE 802.1X	<p>The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports.</p> <p>Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.</p>	<p>The Cisco Unified IP Phone implements the IEEE 802.1X standard by providing support for the MD5 authentication method.</p> <p>When 802.1X authentication is enabled on the phone, you should disable the voice VLAN.</p>

Network Protocol	Purpose	Usage Notes
Internet Control Message Protocol for IPv6 (ICMPv6)		
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets across the network.	<p>To communicate using IP, network devices must have an assigned IP address, subnet, and gateway.</p> <p>IP addresses, subnets, and gateways identifications are automatically assigned if you are using the Cisco Unified IP Phone with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each phone locally.</p> <p>The Cisco Unified IP Phone supports IPv6 addresses. For more information, see <i>Cisco Unified Communications Manager Features and Services Guide</i>, "Internet Protocol Version 6 (IPv6)" chapter.</p>
Link Layer Discovery Protocol (LLDP)	LLDP is a standardized network discovery protocol (similar to CDP) that is supported on some Cisco and third-party devices.	The Cisco Unified IP Phone supports LLDP on the switch and PC port.
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED is an extension of the LLDP standard developed for voice products.	<p>The Cisco Unified IP Phone supports LLDP-MED on the SW port to communicate information such as:</p> <ul style="list-style-type: none"> <li>• Voice VLAN configuration</li> <li>• Device discovery</li> <li>• Power management</li> <li>• Inventory management</li> </ul> <p>For more information about LLDP-MED support, see the LLDP-MED and "Cisco Discovery Protocol" white paper:  <a href="http://www.cisco.com/en/US/technologies/tk652/tk701/technologies_white_paper0900aecd804cd46d.html">http://www.cisco.com/en/US/technologies/tk652/tk701/technologies_white_paper0900aecd804cd46d.html</a></p>
Real-Time Transport Protocol (RTP)	RTP is a standard protocol for transporting real-time data, such as interactive voice and video, over data networks.	Cisco Unified IP Phones use the RTP protocol to send and receive real-time voice traffic from other phones and gateways.

Network Protocol	Purpose	Usage Notes
Real-Time Control Protocol (RTCP)	RTCP works in conjunction with RTP to provide QoS data (such as jitter, latency, and round trip delay) on RTP streams.	RTCP is disabled by default, but you can enable it on a per phone basis by using Cisco Unified Communications Manager.
Session Initiation Protocol (SIP)	SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP is an ASCII-based application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints.	Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.  Cisco Unified IP Phones support the SIP protocol when the phones are operating in IPv6 address, IPv4 address, or dual-stack mode.
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	Cisco Unified IP Phones use TCP to connect to Cisco Unified Communications Manager.
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network.  On the Cisco Unified IP Phone, TFTP enables you to obtain a configuration file specific to the phone type.	TFTP requires a TFTP server in your network, which can be automatically identified from the DHCP server. If you want a phone to use a TFTP server other than the one specified by the DHCP server, you must manually assign the IP address of the TFTP server by using the Network Configuration menu on the phone.  For more information, go to the “Cisco TFTP” chapter in the <i>Cisco Unified Communications Manager System Guide</i> .
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data packets.	Cisco Unified IP Phones transmit and receive RTP streams, which utilize UDP.

### Related Topics

[Cisco Unified Communications Manager Interaction, on page 7](#)

## VLAN Interaction

The Cisco Unified SIP Phone 3905 has an internal Ethernet switch, enabling forwarding of packets to the phone, and to the access port and the network port on the back of the phone.

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

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

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

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

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

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

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

## External Devices

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

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

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

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



---

**Caution**

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

---

## Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect 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





## CHAPTER 2

# Cisco Unified SIP Phone Hardware

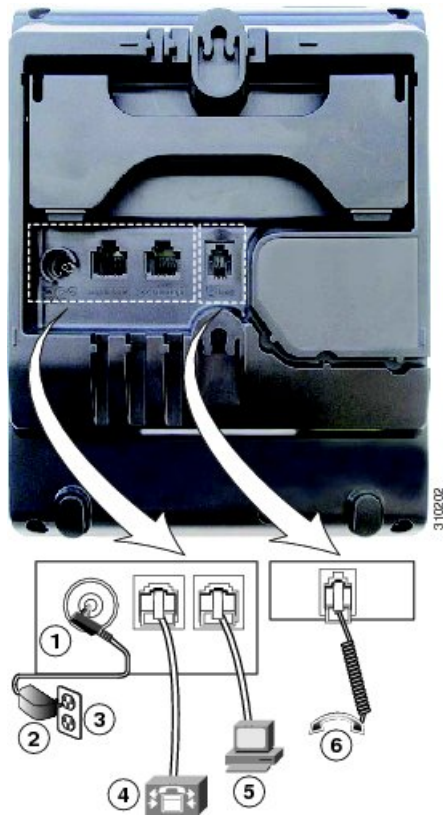
---

- [Cisco Unified SIP Phone 3905, page 13](#)
- [Terminology Differences, page 17](#)

## Cisco Unified SIP Phone 3905

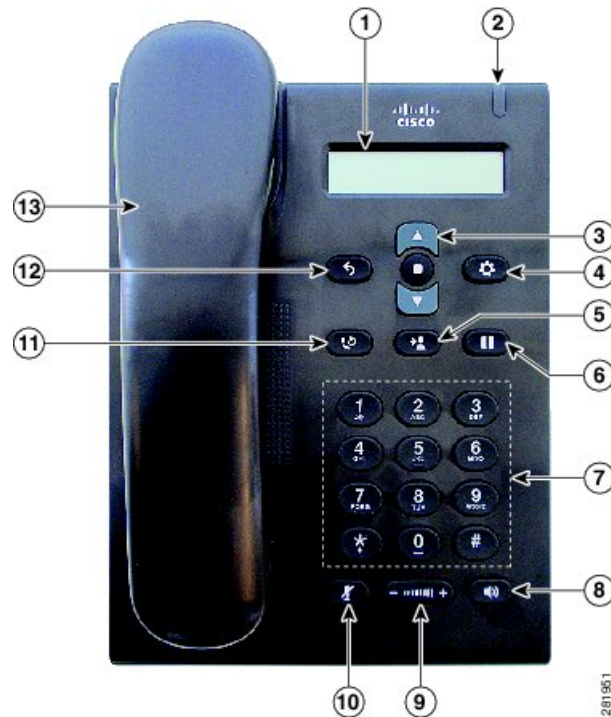
### Phone Connections

Use the following figure to connect the phone to the network.











1	DC adapter port (DC 4.2V).	4	Network port (10/100 SW) connection. IEEE 802.3af power enabled.
2	AC-to-DC power supply (optional).	5	Access port (10/100 PC) connection.
3	AC power wall connection.	6	Handset connection.

## Buttons and Hardware



1	Phone screen	Shows information about your phone such as directory number, active call, and phone menu listings.
2	Light strip	Indicates an incoming call (flashing red) or new voice message (steady red).
3	Navigation bar and Select/Feature button	<p>The Navigation bar allows you to scroll through menus and highlight items. The Select button (in the middle of the Navigation bar) allows you to select a highlighted item.</p> <p>When the phone is off-hook, the Select button functions as the Feature button. You can access these features:</p> <ul style="list-style-type: none"> <li>• Call Forward All: Allows you to forward a call.</li> <li>• Voice Mail: Allows you access voice mails.</li> <li>• Call Pickup: Allows you to answer a call that is ringing on a co-worker's phone.</li> <li>• Group Call Pickup: Allows you to answer a call that is ringing in another call group.</li> </ul>

4	Applications button 	Opens or closes the Applications menu. Use it to access call history, user preferences, phone settings, and phone model information.
5	Transfer button 	Transfers a call.
6	Hold/Resume button 	Places an active call on hold or resumes a held call.
7	Keypad	Allows you to dial phone numbers.
8	Speakerphone button 	Selects the speakerphone as the default audio path and initiates a new call, picks up an incoming call, or ends a call. The speakerphone audio path does not change until a new default audio path is selected (for example, by picking up the handset).
9	Volume button 	Controls the handset and speakerphone volume (off-hook) and the ringer volume (on hook).
10	Mute button 	Toggles the microphone on or off.
11	Redial button 	Dials the last dialed number.
12	Back button 	Returns to the previous screen or menu.
13	Handset	Phone handset.

## Terminology Differences

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

- *Cisco Unified SIP Phone 3905 User Guide for Cisco Unified Communications Manager*
- *Cisco Unified SIP Phone 3905 Administration Guide for Cisco Unified Communications Manager*
- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager System Guide*

<b>User Guide</b>	<b>Administration and System Guides</b>
Auto Barge	cBarge
Message Indicators	Message Waiting Indicator (MWI) or Message Waiting Lamp
Voicemail System	Voice Messaging System





## PART **II**

# Cisco Unified SIP Phone Installation

- [Cisco Unified SIP Phone Installation, page 21](#)
- [Cisco Unified Communications Manager Phone Setup, page 37](#)
- [Self Care Portal Management, page 49](#)







## Cisco Unified SIP Phone Installation

---

- [Verify Network Setup, page 21](#)
- [Enable Autoregistration for Phones, page 22](#)
- [Install Cisco Unified SIP Phone, page 23](#)
- [Set Up Phone from Setup Menus, page 24](#)
- [Configure Network Settings, page 26](#)
- [Verify Phone Startup, page 35](#)

### Verify Network Setup

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

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



**Note**

---

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

---

#### Procedure

---

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

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

## Enable Autoregistration for Phones

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

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

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

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

Autoregistration is disabled by default. In some cases, you might not want to use autoregistration; for example, if you want to assign a specific directory number to the phone, or if you want to use a secure connection with Cisco Unified Communications Manager. For information about enabling autoregistration, see the documentation for your particular Cisco Unified Communications Manager release. When you configure the cluster for mixed mode through the Cisco CTL client, autoregistration is automatically disabled. 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 select the Autoregister check box.
  - Step 3** In **Auto-registration Information**, configure Universal Device Template, Universal Line Template, Starting Directory Number, and Ending Directory Number.
  - Step 4** Click **Save**.
- 

### Related Topics

[Phone Addition Methods](#), on page 42

## Install Cisco Unified SIP Phone

The following steps provide an overview and checklist of installation tasks for the Cisco Unified SIP Phone 3905. The list presents a suggested order to guide you through the phone installation. Some tasks are optional, depending on your system and user needs. For detailed procedures and information, refer to the sources in the list.

### Procedure

---

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

Determines how the phone receives power. For more information, see [Phone Power Requirements](#), on page 6.
- Step 2** Connect the handset to the Handset port.
- Step 3** (Optional) Connect the power supply to the Cisco DC Adapter port. See [Phone Addition Methods](#), on page 42 for guidelines.
- Step 4** Connect a straight-through Ethernet cable from the switch to the network port labeled Network on the Cisco Unified SIP Phone 3905. Each phone ships with one Ethernet cable in the box. You can use either Category 3, 5, or 5e cabling for 10-Mbps connections, but you must use Category 5 or 5e for 100 Mbps connections.
- Step 5** Connect a straight-through Ethernet cable from another network device, such as a desktop computer, to the access port labeled Computer. You can connect another network device later if you do not connect one now. You can use either Category 3, 5, or 5e cabling for 10-Mbps connections, but you must use Category 5 or 5e for 100 Mbps connections.
- Step 6** Monitor the phone startup process. This step associates directory numbers to the phone and verifies that phone is configured properly.

For more information, see [Verify Phone Startup](#), on page 35.

**Step 7** If you are configuring the network settings on the phone, you can set up an IP address for the phone by either using DHCP or manually entering an IP address.

- Using DHCP: Verify that DHCP is enabled. You can set an alternate TFTP by entering the IP address for the TFTP.

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

- Without DHCP: Verify that DHCP is disabled. You must then configure the IP address, subnet mask, TFTP server, and default router locally.

For more information, see [Configure Network Settings](#), on page 26.

**Step 8** Set up security on the phone. This step provides protection against data tampering threats and identity theft of phones.

For more information, see [Cisco Unified SIP Phone Security](#), on page 61.

**Step 9** Upgrade the phone to the current firmware image.

**Step 10** Make calls with the phone. This step verifies that the phone and features work correctly.

For more information, see the *Cisco Unified SIP Phone 3905 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 phones.

For more information, see [Cisco IP Phone User Support](#), on page 65.

## Set Up Phone from Setup Menus

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

The phone includes the following setup menus:

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

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



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


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

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

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

To display a configuration menu, follow these steps:

### Procedure

- 
- Step 1** Press **Applications** .
- Step 2** Select **Admin Settings**.
- Step 3** Select **Network** or **Security**.
- Note** For information about the Reset Settings menu, see [Maintenance](#), on page 121.
- Step 4** Enter your user ID and password, if required, then press **Select**.
- Step 5** Perform one of these actions to display the desired menu:
- Use the navigation arrows to select the desired menu and then press **Select**.
  - Use the keypad on the phone to enter the number that corresponds to the menu.
- Step 6** To display a submenu, repeat step 5.
- Step 7** To exit a menu, press **Back**.
- 

## Apply 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 using **Device > Device Settings > Common Phone Profile**.
- Step 2** Enter a password in the Local Phone Unlock Password option.
- Step 3** Apply the password to the common phone profile that the phone uses.
- 

## Text and Menu Entry from Phone

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

- Use the arrows on the navigation pad to highlight the field that you wish to edit, then press **Select** in the navigation pad to activate that field. You can also double-tap on an editable field to activate it for editing. 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.
- To delete a character to the left of the cursor, use the **Hold/Resume** button.
- Press the arrow button  to cancel or save your update.
- To enter an IP address, use the star (\*) key to input:
  - the period (.) in IPv4 addresses
  - the colon (:) in IPv6 addresses




---

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

---

### Related Topics

- [Apply Phone Password, on page 25](#)
- [Basic Reset, on page 121](#)

## Configure Network Settings

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

- IP address
- IP subnet information

- IPv6 addresses
- Default Router
- TFTP server IP address

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

**Table 6: Network Setup Menu Options**

Option	Description	To Change
IPv4	In the IPv4 Setup submenu, you can do the following: <ul style="list-style-type: none"> <li>• Enable or disable the phone to use the IP address that is assigned by the DHCP server.</li> <li>• Manually set the IP Address, Subnet Mask, Default Routers, DNS Server, and Alternate TFTP servers.</li> </ul>	Scroll to IPv4 Setup and press Select.
IPv6	In the IPv6 Setup submenu, you can do the following: <ul style="list-style-type: none"> <li>• Enable or disable the phone to use the IPv6 address that is assigned by the DHCPv6 server.</li> <li>• Manually set the IPv6 Address, IPv6 Prefix Length, Default Routers, DNS Server, and Alternate TFTP servers.</li> </ul> <p>See <a href="#">Set IPv6 Fields</a>, on page 33.</p>	Scroll to IPv6 Setup and press Select.
MAC Address	Unique Media Access Control (MAC) address of the phone	Display only - Cannot configure.
Host Name	Unique host name that the DHCP server assigned to the phone.	Display only - Cannot configure.
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides.	See <a href="#">Set Domain Name Field</a> , on page 30.
Operational VLAN ID	Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch in which the phone is a member.  If the phone has not received an auxiliary VLAN, this option indicates the Administrative VLAN.  If neither the auxiliary VLAN nor the Administrative VLAN are configured, this option defaults to a VLAN ID of 4095.	Display only - Cannot configure.  The phone obtains its Operational VLAN ID via Cisco Discovery Protocol (CDP) from the switch to which the phone is attached. To assign a VLAN ID manually, use the Admin VLAN ID option.

Option	Description	To Change
Admin. VLAN ID	<p>Auxiliary VLAN in which the phone is a member. Used only if the phone does not receive an auxiliary VLAN from the switch; otherwise it is ignored.</p>	<p>See <a href="#">Set Admin VLAN ID Field, on page 30.</a></p>
PC VLAN	<p>Allows the phone to interoperate with 3rd party switches that do not support a voice VLAN. The Admin VLAN ID option must be set before you can change this option.</p>	<p>See <a href="#">Set PC VLAN Field, on page 30.</a></p>
SW Port Setup	<p>Speed and duplex of the network port. Valid values:</p> <ul style="list-style-type: none"> <li>• Auto Negotiate</li> <li>• 100 Half: 100-BaseT/half duplex</li> <li>• 100 Full: 100-BaseT/full duplex</li> <li>• 10 Half: 10-BaseT/half duplex</li> <li>• 10 Full: 10-BaseT/full duplex</li> </ul> <p>If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to auto-negotiate.</p> <p>If you change the setting of this option, you must change the PC Port Configuration option to the same setting.</p>	<p>See <a href="#">Set SW Port Setup Field, on page 31.</a></p>
PC Port Setup	<p>Speed and duplex of the access port. Valid values:</p> <ul style="list-style-type: none"> <li>• Auto Negotiate</li> <li>• 100 Half: 100-BaseT/half duplex</li> <li>• 100 Full: 100-BaseT/full duplex</li> <li>• 10 Half: 10-BaseT/half duplex</li> <li>• 10 Full: 10-BaseT/full duplex</li> </ul> <p>If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to auto-negotiate.</p> <p>If you change the setting of this option, you must change the SW Port Configuration option to the same setting.</p>	<p>See <a href="#">Set PC Port Setup Field, on page 31.</a></p>

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



**Table 7: IPv4 Setup menu options**

Option	Description	To Change
DHCP Enabled	Indicates whether the phone has DHCP enabled or disabled.  When DHCP is enabled, the DHCP server assigns the phone an IP address. When DHCP is disabled, the administrator must manually assign an IP address to the phone.	See <a href="#">Set DHCP Enabled Field</a> , on page 31.
IP Address	Internet Protocol (IP) address of the phone.  If you assign an IP address with this option, you must also assign a subnet mask and default router. See the Subnet Mask and Default Router options in this table.	See <a href="#">Set IP Address Field</a> , on page 31.
Subnet Mask	Subnet mask used by the phone.	See <a href="#">Set Subnet Mask Field</a> , on page 32.
Default Router 1	Default router used by the phone (Default Router 1).	See <a href="#">Set Default Router Field</a> , on page 32.
DNS Server 1	Primary Domain Name System (DNS) server (DNS Server 1) used by the phone.	See <a href="#">Set DNS Server Field</a> , on page 32.
Alternate TFTP	Indicates whether the phone is using an alternative TFTP server.	See <a href="#">Set Alternate TFTP Field</a> , on page 32.
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the phone. If you are not using DHCP in your network and you want to change this server, you must use the TFTP Server 1 option.  If you set the Alternate TFTP option to yes, you must enter a non-zero value for the TFTP Server 1 option.	See <a href="#">Set TFTP Server 1 Field</a> , on page 33.
TFTP Server 2	Optional backup TFTP server that the phone uses if the primary TFTP server is unavailable.	See <a href="#">Set TFTP Server 2 Field</a> , on page 33.
DHCP Address Released	Releases the IP address assigned by DHCP.	Scroll to the DHCP Address Released option and press Select, then select Yes to release the DHCP Address.

### Procedure

---

- Step 1** On the phone, press **Applications**.
  - Step 2** Select **Admin Settings** and login if required.
  - Step 3** Select **Network**.
  - Step 4** To access the IPv4 setup fields, scroll to IPv4 and press **Select**.
  - Step 5** To access the IPv6 setup fields, scroll to IPv6 and press **Select**.  
For more information, see [Set IPv6 Fields, on page 33](#).
- 

## 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 **Select**.
- 

## Set Admin VLAN ID Field

### Procedure

---

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

## Set PC VLAN Field

### Procedure

---

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

## Set SW Port Setup Field

### Procedure

---

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

## Set PC Port Setup Field

### Procedure

---

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

## Set DHCP 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 **Select**.
-

## Set Subnet Mask Field

### Procedure

---

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

## Set Default Router Field

### Procedure

---

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

## Set DNS Server Field

### Procedure

---

- Step 1** Set the DHCP Enabled option to **No**.
  - Step 2** Scroll to the appropriate DNS Server option, press **Select**, and enter a new DNS server IP address.
  - Step 3** Press **Select**.
- 

## Set Alternate TFTP Field

### Procedure

---

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

## Set TFTP Server 1 Field

### Procedure

---

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

## Set TFTP Server 2 Field

### Procedure

---

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

## Set IPv6 Fields



**Note** If DHCPv6 Enabled is set to Yes, some IPv6 Setup menu options cannot be edited. If you need to change a setting and it is not available, check the value of the DHCPv6 Enabled option.

---

The following table describes supported IPv6 menu options.

**Table 8: IPv6 Setup Menu Options**

Option	Default value	Description
IPv6 Address	::	<p>Displays the current IPv6 address of the phone or allows the user to enter a new IPv6 address.</p> <p>Two address formats are supported:</p> <ul style="list-style-type: none"> <li>• Eight sets of hexadecimal digits separated by colons X:X:X:X:X:X:X:X</li> <li>• Compressed format to collapse a single run of consecutive zero groups into a single group represented by a double colon.</li> </ul> <p>If the IP address is assigned with this option, you must also assign the IPv6 prefix length and the default router.</p>
IPv6 Prefix Length	0	<p>Displays the current prefix length for the subnet or allows the user to enter a new prefix length.</p> <p>The subnet prefix length is a decimal value from 1-128.</p>
IPv6 Default Router 1	::	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 Alternate TFTP	Disabled	Allows the user to enable the use of an alternate (secondary) IPv6 TFTP server.
IPv6 TFTP Server 1	::	Displays the primary IPv6 TFTP server used by the phone or allows the user to set a new primary TFTP server.
IPv6 TFTP Server 2	::	Displays the secondary, optional, IPv6 TFTP server used if the primary IPv6 TFTP server is unavailable or allows the user to set a new secondary TFTP server.
IPv6 Addr. Released	Disabled	Allows the user to release IPv6 related information.

## Procedure

- 
- Step 1** Press **Applications**.
- Step 2** Select **Admin Settings > Network > IPv6**.
- Step 3** Select the option to edit or to toggle.
- Step 4** To enter IPv6 addresses,
- a) Click in the input field.

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

The following table describes the address formats.

Format	Description
X:X:X:X:X:X:X	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
Compressed	Collapse a single run of consecutive zero groups into a single group represented by a double colon. Example: 2001:db8::52:0:1

- 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**.

**Step 5** Change toggle fields using these steps:

- If an option is set to No, press **Yes** to enable it. If the option is set to Yes, press **No** to disable it.
- In the confirmation request window, press **Yes** to save your change, or **No** to discard it.

**Step 6** In the confirmation request window, press **Yes** to save your change, or **No** to discard it.

## Verify Phone Startup

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

### Procedure

**Step 1** If you are using Power over Ethernet, plug the LAN cable into the Network port.

**Step 2** If you are using the power cube, connect the cube to the phone and plug the cube into an electrical outlet. The buttons flash amber and then green in sequence during the various stages of bootup as the phone checks the hardware.

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

### Related Topics

[Startup Problems, on page 105](#)

[Cisco IP Phone Does Not Go Through the Normal Startup Process, on page 106](#)





# CHAPTER 4

## Cisco Unified Communications Manager Phone Setup

---

- [Phone Configuration Files](#), page 37
- [Set Up Cisco Unified SIP Phone](#), page 38
- [Determine Phone MAC Address](#), page 42
- [Phone Addition Methods](#), page 42
- [Add Users to Cisco Unified Communications Manager](#), page 44
- [Add User to End User Group](#), page 45
- [Associate Phones with Users](#), page 46
- [Perform Final End User Configuration Steps](#), page 46

### 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

## Set Up Cisco Unified SIP 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 *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
- Associated directory number (DN) to assign to the phone
- Cisco Unified Communications Manager user to associate with the phone

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.

For more information, see the “Cisco Unified IP Phones” chapter in the *Cisco Unified Communications Manager System Guide* and [Telephony Features](#), on page 66.

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

For more information, go to the “License Unit Report” chapter in the *Cisco Unified Communications Manager Administration Guide*.

**Step 3** Define the phone button templates that determine the configuration of buttons on a phone. Select **Device > Device Settings > Phone Button Template** to create and update the templates.

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

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

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

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

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

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

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

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

- d) In the Extension Information area, check the Enable Extension Mobility check box if this phone supports Cisco Extension Mobility.

- e) Click **Save**.

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

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

**Note** This field should contain the same number that appears in the Telephone Number field in the End User Configuration window.
- d) From the Route Partition drop-down list, choose the partition to which the directory number belongs. If you do not want to restrict access to the directory number, choose <None> for the partition.
- e) From the Calling Search Space drop-down list, choose the appropriate calling search space. The value that you choose applies to all devices that are using this directory number.
- f) In the Call Forward and Call Pickup Settings area, choose the items (for example, Forward All, Forward Busy Internal) and corresponding destinations to which calls should be sent.

**Example:**

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

- g) In the Line 1 on Device pane, configure the following fields:
- Display (Internal Caller ID field): You can enter the first name and last name of the user of this device so that this name displays for all internal calls. Leave this field blank to have the system display the phone extension.
  - External Phone Number Mask: Indicate phone number (or mask) that is used to send Caller ID information when a call is placed from this line. You can enter a maximum of 24 numeric and “X” characters. The Xs represent the directory number and must appear at the end of the pattern.

**Example:**

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

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

- h) Select **Save**.

For more information, see the “Directory number setup” chapter in the *Cisco Unified Communications Manager Administration Guide* and see [Telephony Features](#), on page 66.

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

- a) Use **Find** in conjunction with the Search fields to locate the user.
- b) check the box next to the user name, and click **Add Selected**.  
The user name and user ID appears in the Users Associated With Line pane of the Directory Number Configuration window.
- c) Select **Save**.
- d) Select **Save**.

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

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

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

- a) Choose **User Management > End User**.
- b) Use the search boxes and **Find** to locate the user you have added.
- c) Click on the user ID.
- d) In the Directory Number Associations area of the screen, set the Primary Extension from the drop-down list.
- e) In the Mobility Information area, check the Enable Mobility box.
- f) In the Permissions Information area, use the **Add to Access Control Group** buttons to add this user to any user groups.  
For example, you may want to add the user to a group that is defined as a Standard CCM End User Group.
- g) To view the details of a group, select the group and click **View Details**.
- h) In the Extension Mobility area, check the Enable Extension Mobility Cross Cluster box if the user can use for Extension Mobility Cross Cluster service.
- i) In the Device Information area, click **Device Associations**.
- j) Use the Search fields and **Find** to locate the device that you want to associate to the user.
- k) Select the device, and click **Save Selected/Changes**.
- l) Click **Go** next to the “Back to User” Related link in the upper right corner of the screen.
- m) Select **Save**.

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

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

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

**Step 13** Configure Cisco IP Phone services and assign services. Select **Device > Device Settings > Phone Services**. Provides IP Phone services to the phone.

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

**Step 14** (Optional) Assign services to programmable buttons. Select **Device > Device Settings > Phone Button Profile**.

Provides access to an IP phone service or URL.

**Step 15** Add user information to the global directory for Cisco Unified Communications Manager. Select **User Management > End User** and configure the required fields. Required fields are indicated by an asterisk (\*); for example, User ID and last name.

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

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

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

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

**Step 16** Associate a user with a user group. Select **User Management > User Settings > Access Control Group**. Assigns users a common list of roles and permissions that apply to all users in a user group. Administrators can manage user groups, roles, and permissions to control the level of access (and, therefore, the level of security) for system users. For more information, see [Add User to End User Group, on page 45](#).

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


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

## Determine Phone MAC Address

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

### Procedure

Perform one of the following actions:

- On the phone, press **Applications** , 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 individually or using BAT require you to identify the MAC address for the phone. For more information, see [Determine Phone MAC Address, on page 42](#).

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 22

## Add Phones Individually

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

### Procedure

---

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

## Add Phones 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 tasks:

- Access the corporate directory and other customized directories from a Cisco IP Phone.
- Create a personal directory.
- 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 45.
- Step 2** To add users in batches, use the Bulk Administration Tool. This method also enables you to set an identical default password for all users.
- For more information, see the documentation for your particular Cisco Unified Communications Manager release.
- 

## Add a User from an External LDAP Directory

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



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

---

### Procedure

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



## Add User Directly to Cisco Unified Communications Manager

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



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

### Procedure

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

## Add 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**.

---

## Perform Final End User Configuration Steps

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

In the End User configuration window, do the following:

## Procedure

---

- Step 1** In the Directory Number Associations pane of the screen, set the primary extension from the drop-down list.
- Step 2** In the Mobility Information pane, check the Enable Mobility box.
- Step 3** In the Permissions Information pane, 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 has been defined as a Standard CCM End User Group. To view all configured user groups, choose **User Management > User Group**.
- Step 4** Click **Save**.
-





## Self Care Portal Management

---

- [Self Care Portal Overview, page 49](#)
- [Set Up User Access to the Self Care Portal, page 49](#)
- [Customize the Self Care Portal Display, page 50](#)

### 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** 

# **Hardware and Accessory Installation**

- [Cisco Unified SIP Phone Accessories, page 53](#)







## Cisco Unified SIP Phone Accessories

---

- [Adjust footstand, page 53](#)
- [Install Phone on Wall Mount Plate, page 53](#)
- [Adjust the Handset Rest, page 57](#)

### Adjust footstand

#### Procedure

The Cisco Unified IP Phone 3905 has a foldable footstand. Unfold the footstand to give the phone an elevated viewing angle.

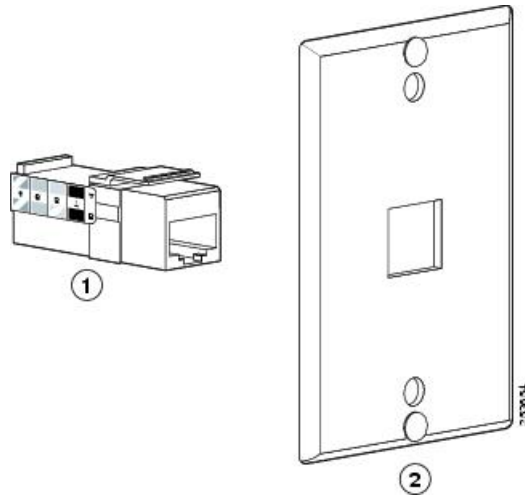
### Install Phone on Wall Mount Plate

#### Before You Begin

You can mount the Cisco Unified SIP Phone 3905 on the wall by using a standard telephone wall plate with an opening for an RJ-45 connector. Cisco recommends that you use Leviton Wall Mount plate (Leviton type number: 4108W-0SP) to wall mount the Cisco Unified SIP Phone 3905. 3905 on the wall using the Leviton Wall Mount plate.

The following figure shows a list of items required to mount the Cisco Unified SIP Phone

**Figure 1: Leviton Wall Mount Plate**



1	RJ45 Connector	2	Leviton Wall Mount Plate
---	----------------	---	--------------------------

## Procedure

- Step 1** Plug the telephone line cord (RJ45 connector) into the phone jack at the base of the phone as shown in the following image:

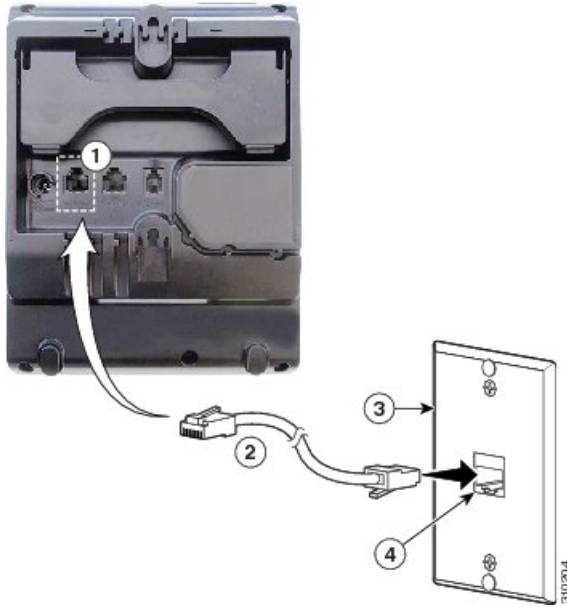
*Figure 2: RJ45 Connector in the Phone Jack*



1	Network Port on the Phone
2	RJ45 Connector

**Step 2** Plug the RJ45 connector into the wall mount phone jack as shown in the following image:

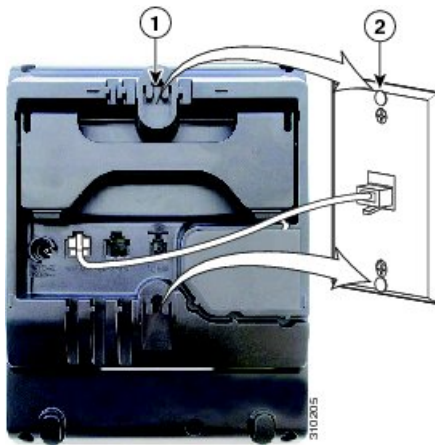
**Figure 3: RJ45 Connector in the Wall Mount Jack**



1	Network Port on the Phone	3	Wall Mount Plate
2	RJ45 Connector	4	Network Port on the Wall Mount Plate

**Step 3** Slip the mounting holes on the base of the wall mount plate and over the wall mount pins as shown in the following image:

**Figure 4: Mounting Holes**



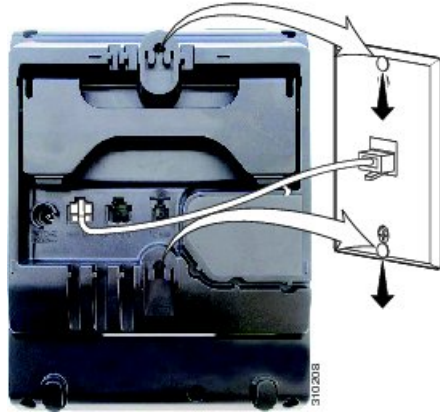
1	Mounting Hole on the Phone
---	----------------------------

2

Wall Mount Pin on the Wall Mount Plate

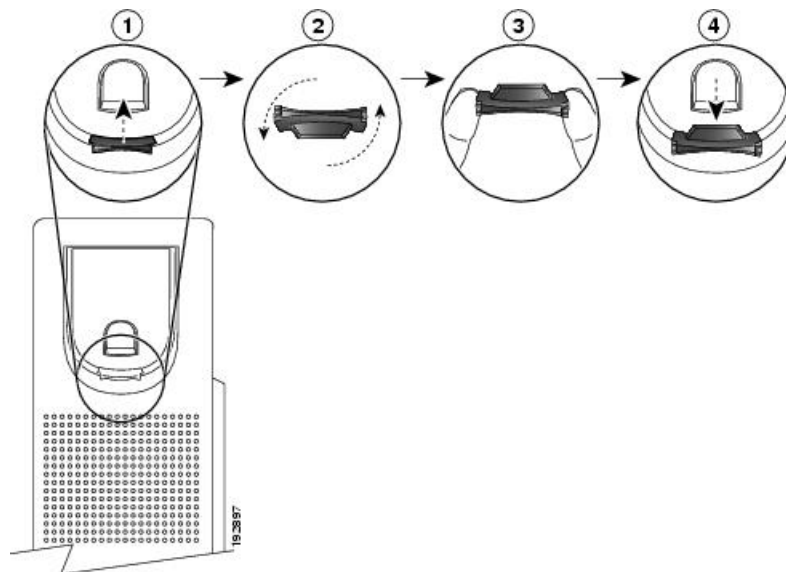
**Step 4** Firmly slide the IP phone down into place as shown in the following image:

**Figure 5: Sliding the IP Phone**



## 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.
-



# PART **IV**

## **Cisco Unified SIP Phone Administration**

- [Cisco Unified SIP Phone Security, page 61](#)
- [Phone Features and Setup , page 65](#)







# Cisco Unified SIP Phone Security

- [Cisco Unified SIP Phone Security Features](#), page 61
- [Set Up SIP MD5 Digest Authentication](#) , page 63
- [Set Device Authentication Field](#), page 64
- [Set Shared Secret Field](#), page 64

## Cisco Unified SIP Phone Security Features

The following table provides an overview of the security features that the Cisco Unified SIP Phone 3905 supports. For more information about these features and about Cisco Unified Communications Manager and phone security, see the *Cisco Unified Communications Manager Security Guide*.

**Table 9: Phone and Cisco Unified Communications Manager Security Topics**

Topic	Reference
Detailed explanation of security, including set up, configuration, and troubleshooting information for Cisco Unified Communications Manager and Cisco Unified IP Phones	See the <i>Troubleshooting Guide for Cisco Unified Communications Manager</i> .
Security and the phone startup process	See <a href="#">Verify Phone Startup</a> , on page 35.
Security and phone configuration files	See <a href="#">Phone Addition Methods</a> , on page 42.
Disabling access to a phone web pages	See <a href="#">Control Phone Web Page Access</a> , on page 72.
Troubleshooting	<ul style="list-style-type: none"> <li>• See <a href="#">Troubleshooting</a> , on page 105</li> <li>• See the <i>Troubleshooting Guide for Cisco Unified Communications Manager</i></li> </ul>
Resetting or restoring the phone	See <a href="#">Basic Reset</a> , on page 121.

Topic	Reference
802.1X Authentication for Cisco Unified IP Phones	See these sections: <ul style="list-style-type: none"> <li>• <a href="#">802.1X Authentication</a>, on page 62</li> <li>• <a href="#">Troubleshooting</a>, on page 105</li> </ul>
SIP MD5 Digest Authentication	See <a href="#">Set Up SIP MD5 Digest Authentication</a> , on page 63.

## 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-MD5 option for network authentication.
- Cisco Secure Access Control Server (ACS) (or other third-party authentication server): The authentication server and the phone must both be configured with a shared secret that authenticates the phone.
- Cisco Catalyst Switch (or other third-party switch): The switch must support 802.1X, so it can act as the authenticator and pass the messages between the phone and the authentication server. After the exchange completes, the switch grants or denies the phone access to the network.

You must perform the following actions to configure 802.1X.

- Configure the other components before you enable 802.1X Authentication on the phone.
- Configure PC Port: The 802.1X standard does not consider VLANs and thus recommends that only a single device should be authenticated to a specific switch port. However, some switches (including Cisco Catalyst switches) support multidomain authentication. The switch configuration determines whether you can connect a PC to the PC port of the phone.
  - Enabled: If you are using a switch that supports multidomain authentication, you can enable the PC port and connect a PC to it. In this case, Cisco IP Phones support proxy EAPOL-Logoff to monitor the authentication exchanges between the switch and the attached PC. For more information

about IEEE 802.1X support on the Cisco Catalyst switches, see the Cisco Catalyst switch configuration guides at:

[http://www.cisco.com/en/US/products/hw/switches/ps708/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html)

- Disabled: If the switch does not support multiple 802.1X-compliant devices on the same port, you should disable the PC Port when 802.1X authentication is enabled. If you do not disable this port and subsequently attempt to attach a PC to it, the switch denies network access to both the phone and the PC.
- Configure Voice VLAN: Because the 802.1X standard does not account for VLANs, you should configure this setting based on the switch support.
  - Enabled: If you are using a switch that supports multidomain authentication, you can continue to use the voice VLAN.
  - Disabled: If the switch does not support multidomain authentication, disable the Voice VLAN and consider assigning the port to the native VLAN.

## Set Up SIP MD5 Digest Authentication

You can challenge SIP phones for MD5 digest authentication credentials before they can connect to your network. For more information, see *Cisco Unified Communications Manager Security Guide*.

### Procedure

---

**Step 1** Access one of the following Cisco Unified Communications Manager Administration windows:

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

**Step 2** Set the Enable Digest Authentication parameter to Enabled or Disabled. The default is Disabled.

---

## Set Device Authentication Field

### Procedure

---

- Step 1** Press **Applications**.
  - Step 2** Choose **Admin Settings > Security > 802.1X Authentication > Device Authentication**.
  - Step 3** Press **Select**.
  - Step 4** Set the Device Authentication option to Enabled or Disabled.
  - Step 5** Press **Select** to confirm.
- 

## Set Shared Secret Field

Choose a password to use on the phone and on the authentication server. The password must be between 6 and 32 characters, consisting of any combination of numbers or letters.



**Note** If you disable 802.1X authentication or perform a factory reset of the phone, the shared secret is deleted.

---

### Procedure

---

- Step 1** Press **Applications**.
  - Step 2** Choose **Admin Settings > Security > 802.1X Authentication > EAP-MD5 > Shared Secret**.
  - Step 3** Press **Select**.
  - Step 4** Enter the shared secret.
  - Step 5** Press **Select** to confirm.
-



## Phone Features and Setup

---

- [Phone Features and Setup Overview](#), page 65
- [Cisco IP Phone User Support](#), page 65
- [Telephony Features](#), page 66
- [Disable Speakerphone](#), page 72
- [Control Phone Web Page Access](#), page 72
- [Enable Paging Support on Cisco Unified Communications Manager](#), page 72
- [Set the Label for a Line](#), page 73

### 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.

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

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

For suggestions about how to provide users with information about features, and what information to provide, see [Cisco IP Phone User Support](#), on page 65.

For information about setting up phones in non-English environments, see [International User Support](#), on page 125.

### Cisco IP Phone User Support

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

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

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

Cisco Unified IP Phones provide traditional telephony functionality, such as call forwarding and transferring, redialing, 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, but if your network requires it, you can manually configure an IP address, TFTP server, subnet information, and so on.

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 modify additional settings for the Cisco Unified IP Phone from Cisco Unified Communications Manager Administration. Use Cisco Unified Communications Manager Administration to set up phone registration criteria and calling search spaces, among other tasks. See the “Telephony Features” section in this document and the Cisco Unified Communications Manager documentation for additional information.

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

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

For information about using most of these features on the phone, see the *Cisco Unified SIP Phone 3905 User Guide for Cisco Unified Communications Manager*.

**Note**

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

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

**Table 10: Telephony Features**

Feature	Description
Audible Message Waiting Indicator (AMWI)	A stutter tone from the handset or speakerphone indicates that a user has one or more new voice messages on a line.  See the <i>Cisco Unified Communications Manager System Guide</i> , “Cisco Unified IP Phone” chapter.
Auto Answer	Connects incoming calls automatically after a ring or two.  Auto Answer works with the speakerphone.  See the <i>Cisco Unified Communications Manager Administration Guide</i> , “Directory Number Configuration” chapter.
Block External to External Transfer	Prevents users from transferring an external call to another external number.  See the <i>Cisco Unified Communications Manager Features and Services Guide</i> , “External Call Transfer Restrictions” chapter.
Call Forward	Allows users to redirect incoming calls to another number. The Call Forward All option is supported. Users hear a stutter tone after going off-hook if the Call Forward All feature is configured on the phone.  See: <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Directory Number Configuration” chapter</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone” chapter</li> <li>• <a href="#">Customize the Self Care Portal Display</a>, on page 50</li> </ul>
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 the <i>Cisco Unified Communications Manager System Guide</i> , “Cisco Unified IP Phone” chapter.

Feature	Description
Call Forward All Loop Prevention	<p>Prevents a user from configuring a Call Forward All destination directly on the phone that creates a Call Forward All loop or that creates a Call Forward All chain with more hops than the existing Forward Maximum Hop Count service parameter allows.</p> <p>See the <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone” chapter.</p>
Call Forward Destination Override	<p>Allows you to override Call Forward All (CFA) in cases where the CFA target places a call to the CFA initiator. This feature allows the CFA target to reach the CFA initiator for important calls. The override works whether the CFA target phone number is internal or external.</p> <p>See the <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Directory Numbers” chapter.</p>
Call Pickup	<p>Allows users to answer a call that is ringing on a co-worker's phone by redirecting the call to their phone</p> <p>You can configure an audio alert for the primary line on the phone. This alert notifies the users that a call is ringing in their pickup group.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Call Pickup” chapter.</p>
Call Waiting	<p>Indicates (and allows users to answer) an incoming call that rings while on another call.</p> <p>The phone sounds the call waiting tone (single beep) and the phone screen displays the second incoming call.</p> <p>See <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Directory Numbers” chapter.</p>
cBarge	<p>Allows a user to join a non-private call on a shared phone line. cBarge adds a user to a call and converts it into a conference, allowing the user and other parties to access conference features.</p> <p>For more information, see the <i>Cisco Unified Communications Manager Features and Services Guide</i> “Barge and Privacy” chapter.</p>
Conference	<ul style="list-style-type: none"> <li>• Allows a user to talk simultaneously with multiple parties by calling each participant individually.</li> <li>• Allows a non-initiator in a standard (ad hoc) conference to add participants; also allows any conference participant to join together two standard conferences on the same line.</li> </ul> <p>The service parameter, Advance Adhoc Conference, (disabled by default in Cisco Unified Communications Manager Administration) allows you to enable these features.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• Cisco Unified Communications Manager System Guide, “Conference Bridges” chapter.</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phone” chapter.</li> </ul> <p><b>Note</b> Be sure to inform your users whether these features are activated.</p>



Feature	Description
Forced Authorization Codes (FAC)	<p>Controls the types of calls that certain users can place.</p> <p>For more information, see the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Client Matter Codes” and “Forced Authorization Codes” chapters.</p>
Group Call Pickup	<p>Allows a user to answer a call that is ringing on a directory number in another group.</p> <p>For more information, see the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Call Pickup” chapter.</p>
Hold/Resume	<p>Allows the user to move a connected call from an active state to a held state by using the Hold/Resume button. The user resumes a held call by pressing the Hold/Resume button, speaker button, or going off-hook.</p> <p>No configuration required unless you want to use music on hold. See “Music-On-Hold” in this table for information.</p>
Hookflash Timer	<p>Controls the length of time before the hookflash indicates a timeout (or call disconnect).</p> <p>See <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter.</p>
IPv6 Support	<p>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.</p> <p>See <a href="#">Set IPv6 Fields</a>, on page 33.</p>
IPv6 Ready Logo (SIP)	<p>Ensures that IP addressing on Cisco SIP No configuration required. Phones passes component level conformance and interoperability testing as identified in the TAHI Project.</p> <p>No configuration required.</p>
Line Text Label	<p>Sets a text label for a phone line instead of the directory number.</p> <p>See <a href="#">Set the Label for a Line</a>, on page 73.</p>
Message Waiting	<p>Defines directory numbers for message-waiting on and message-waiting off indicator. 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.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Message Waiting Configuration” chapter</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Voice Mail Connectivity to Cisco Unified Communications Manager” chapter.</li> </ul>

Feature	Description
Message Waiting Indicator	<p>A light on the phone that indicates that a user has one or more new voice messages.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Message Waiting Configuration” chapter</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Voice Mail Connectivity to Cisco Unified Communications Manager” chapter</li> </ul>
Multiple Date Display Formats	<p>Displays one of three date formats controlled by the CUCM. Available formats include:</p> <ul style="list-style-type: none"> <li>• Day, Month, Year (DD/MM/YYYY)</li> <li>• Month, Day, Year (MM/DD/YYYY)</li> <li>• Year, Month, Day (YYYY/MM/DD)</li> </ul> <p>See <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter.</p>
Music On Hold	<p>Plays music while callers are on hold.</p> <p>See the <i>Cisco Unified Communications Manager Features and Services Guide</i>, “Music On Hold” chapter.</p>
Mute	<p>Mutes the microphone from the handset or speakerphone.</p> <p>No configuration required.</p>
On-hook Call Transfer	<p>Allows a user to press the Transfer button and then go on-hook to complete a call transfer.</p> <p>See the <i>Cisco Unified Communications Manager System Guide</i>, “Cisco Unified IP Phones” chapter.</p>
Plus Dialing	<p>Allows the user to dial E.164 numbers prefixed with a + sign.</p> <p>To dial the + sign, the user needs to press and hold the * key for at least 1 second. This applies to dialing the first digit for both on-hook or off-hook calls.</p> <p>Requires no configuration.</p>
Private Line Automated Ringdown (PLAR)	<p>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 can be useful for phones that are designated for calling emergency or <i>hotline</i> numbers.</p> <p>See the <i>Cisco Unified Communications Manager Administration Guide</i>, “Directory Number Configuration” chapter.</p>
Redial	<p>Allows users to call the most recently dialed phone number by pressing the Redial button.</p> <p>No configuration required.</p>

Feature	Description
Shared Line	<p>Allows a user to have multiple phones that share the same phone number or allows a user to share a phone number with a coworker.</p> <p>See the <i>Cisco Unified Communications Manager System Guide</i>, “Understanding Directory Numbers” chapter.</p>
SIP MD5 Digest Authentication	<p>Allows you to enable or disable MD5 digest authentication for SIP.</p> <p>See <a href="#">Set Up SIP MD5 Digest Authentication</a> , on page 63.</p>
Telnet	<p>You can use Telnet to connect to your Cisco Unified IP Phone for use in troubleshooting and phone maintenance.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Unified IP Phone Configuration” chapter</li> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “SIP Profile Configuration Settings” chapter</li> </ul>
Time-of-Day Routing	<p>Restricts access to specified telephony features by time period.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Time Period Configuration” chapter</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Time-of-Day Routing” chapter</li> </ul>
Time Zone Update	<p>Updates the Cisco Unified IP Phone with time zone changes.</p> <p>See the <i>Cisco Unified Communications Manager Administration Guide</i>, “Time Group Configuration” chapter.</p>
Transfer	<p>Allows users to redirect connected calls from their phones to another number.</p> <p>No configuration required.</p>
Voice Messaging System	<p>Enables callers to leave messages if calls are unanswered.</p> <p>See:</p> <ul style="list-style-type: none"> <li>• <i>Cisco Unified Communications Manager Administration Guide</i>, “Cisco Voice-Mail Port Configuration” chapter</li> <li>• <i>Cisco Unified Communications Manager System Guide</i>, “Voice Mail Connectivity to Cisco Unified Communications Manager” chapter</li> </ul>

## 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**.
- 

## 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**.
- 

## Enable Paging Support on Cisco Unified Communications Manager

You enable the Paging Support on Cisco Unified Communications Manager feature for IP phones by selecting basic HTTP authentication. The default is Disabled.

For more information, see [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cucm/singlewire/InformaCastBasicPaging.pdf](http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/singlewire/InformaCastBasicPaging.pdf).

### Before You Begin

Paging phones must have access to the Singlewire InformaCast server.

### Procedure

---

- Step 1** To enable Paging Support for a single phone,
- In Cisco Unified Communications Manager Administration, choose one of the following windows:
    - **Device > Device Settings > Common Phone Profile > External Data Locations Information**
    - **Device > Phone > Phone Configuration > External Data Locations Information**
  - Set the Authentication Server parameter.
  - Select **Save**.
- Step 2** To enable Paging Support for a group of phones,
- In the Cisco Unified Communications Manager Administration application, choose **System > Enterprise Phone Configuration > External Data Locations Information**.
  - Set the Authentication Server parameter.
  - Select **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 share the line, check the Update Shared Device Settings check box and click **Propagate Selected**.
- Step 5** Select **Save**.
-





# PART **V**

## **Cisco Unified IP Phone Troubleshooting**

- [Monitoring Phone Systems, page 77](#)
- [Troubleshooting , page 105](#)
- [Maintenance, page 121](#)
- [International User Support, page 125](#)







## Monitoring Phone Systems

---

- [Cisco Unified SIP Phone status, page 77](#)
- [Cisco IP Phone Web Page, page 88](#)

### Cisco Unified SIP Phone status

This section describes how to use the following menus on the Cisco Unified SIP Phone 3905 to view model information, status messages, and network statistics for the phone:

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

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

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

For more information about troubleshooting the Cisco Unified SIP Phone 3905, see [Troubleshooting](#), on [page 105](#)

### Display Model Information Window

To display the Model Information screen, follow these steps.

#### Procedure

---

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

**Step 2** Select **Phone Information**.

If the user is connected to a secure or authenticated server, a corresponding icon (lock or certificate) displays in the Phone Information Screen to the right of the server option. If the user is not connected to a secure or authenticated server, no icon appears.

**Step 3** To exit the Model Information screen, press **Back**.

### Related Topics

[Cisco IP Phone Web Page](#), on page 88

### Model Information Fields

The following table describes the Model Information Settings fields.

**Table 11: Model Information Settings fields**

Option	Description	To Change
Model Number	Model number of the phone.	Display only - cannot configure.
MAC Address	MAC address of the phone.	Display only - cannot configure.
Active Load ID	Version of firmware currently installed on the phone.	Display only - cannot configure.
Boot Load ID	Identifier of the factory-installed load running on the phone.	Display only - cannot configure.
IP Address	IPv4 address of the phone.  This option is only displayed when the phone is configured in IPv4-only mode or in dual-stack mode.	See <a href="#">Configure Network Settings</a> , on page 26.
IPv6 Address	IPv6 address of the phone.  This option is only displayed when the phone is configured in IPv6-only mode or in dual-stack mode.	See <a href="#">Set IPv6 Fields</a> , on page 33.
Active Server	IP address or name of the server to which the phone is registered.	Display only - cannot configure.
Stand-by Server	Name of the stand-by server for the phone.  This option is displayed whether the phone is configured in IPv6-only mode, IPv4-only mode, or dual-stack mode.	Display only - cannot configure.


### Display Status Menu

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

- Network Statistics: Displays the Network Statistics screen, which shows Ethernet traffic statistics
- Call Statistics: Displays counters and statistics for the current call.

### Procedure

---

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

## Display Status Messages Window

To display the Status Messages screen,

### Procedure

---

- Step 1** Press **Applications**.
- Step 2** Select **Admin Settings > Status Messages**.  
For information on the messages, see [Status Messages](#), on page 79.
- Step 3** To exit the Status Messages screen, press **Back**.
- 

### Related Topics

[Phone Displays Error Messages](#), on page 107

## Status Messages

The Status Messages web page displays up to 30 of the most recent status messages that the phone has generated since it was last powered up. You can access the Status Messages web page even if the phone is not running. The following table describes the status messages. This table also includes possible explanations and actions to troubleshoot errors.

**Table 12: Status Messages on the Cisco Unified SIP Phone 3905**

Message	Description	Possible Explanation and Action
CFG file not found	The name-based and default configuration file was not found on the TFTP Server.	<p>The configuration file for a phone is created when the phone is added to the Cisco Unified Communications Manager database. If the phone has not been added to the Cisco Unified Communications Manager database, the TFTP server generates a CFG File Not Found response.</p> <ul style="list-style-type: none"> <li>• Phone is not registered with Cisco Unified Communications Manager. You must manually add the phone to Cisco Unified Communications Manager if you are not allowing phones to auto-register. See <a href="#">Phone Addition Methods</a>, on page 42 for details.</li> <li>• If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server.</li> <li>• If you are using static IP addresses, check the TFTP server configuration.</li> </ul>
CFG TFTP Size Error	The configuration file is too large for the file system on the phone.	Power cycle the phone.
Checksum Error	Downloaded software file is corrupted.	Obtain a new copy of the phone firmware and place it in the TFTPPath directory. You should only copy files into this directory when the TFTP server software is shut down, otherwise the files may be corrupted.
DHCP timeout	DHCP server did not respond.	<ul style="list-style-type: none"> <li>• Network is busy. The errors should resolve themselves when the network load reduces.</li> <li>• No network connectivity between the DHCP server and the phone. Verify the network connections.</li> <li>• DHCP server is down. Check the DHCP server configuration.</li> <li>• Errors persist. Consider assigning a static IP address.</li> </ul>

Message	Description	Possible Explanation and Action
DNS timeout	DNS server did not respond.	<ul style="list-style-type: none"> <li>• Network is busy. The errors should resolve themselves when the network load reduces.</li> <li>• No network connectivity between the DNS server and the phone. Verify the network connections.</li> <li>• DNS server is down. Check the DNS server configuration.</li> </ul>
DNS unknown host	DNS could not resolve the name of the TFTP server or Cisco Unified Communications Manager.	<ul style="list-style-type: none"> <li>• Verify that the host names of the TFTP server or Cisco Unified Communications Manager are configured properly in DNS.</li> <li>• Consider using IP addresses rather than host names.</li> </ul>
Duplicate IP	Another device is using the IP address assigned to the phone.	<ul style="list-style-type: none"> <li>• If the phone has a static IP address, verify that you have not assigned a duplicate IP address.</li> <li>• If you are using DHCP, check the DHCP server configuration.</li> </ul>
File not found	The phone cannot locate, on the TFTP server, the phone load file that is specified in the phone configuration file.	From Cisco Unified Operating System Administration, make sure that the phone load file is on the TFTP server, and that the entry in the configuration file is correct.
IP address released	The phone has been configured to release its IP address.	The phone remains idle until it is power cycled or you reset the DHCP address.
Load ID incorrect	Load ID of the software file is of the wrong type.	Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose <b>Device &gt; Phone</b> ). Verify that the load ID is entered correctly.
Load rejected HC	The application that was downloaded is not compatible with the phone's hardware.	Occurs if you were attempting to install a version of software on this phone that did not support hardware changes on this newer phone.  Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose <b>Device &gt; Phone</b> ). Re-enter the load displayed on the phone.


Message	Description	Possible Explanation and Action
No default router	DHCP or static configuration did not specify a default router.	<ul style="list-style-type: none"> <li>• If the phone has a static IP address, verify that the default router has been configured.</li> <li>• If you are using DHCP, the DHCP server has not provided a default router. Check the DHCP server configuration.</li> </ul>
No DNS server IP	A name was specified but DHCP or static IP configuration did not specify a DNS server address.	<ul style="list-style-type: none"> <li>• If the phone has a static IP address, verify that the DNS server has been configured.</li> <li>• If you are using DHCP, the DHCP server has not provided a DNS server. Check the DHCP server configuration.</li> </ul>
TFTP access error	TFTP server is pointing to a directory that does not exist.	<ul style="list-style-type: none"> <li>• If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server.</li> <li>• If you are using static IP addresses, check the TFTP server configuration.</li> </ul>
TFTP error	The phone does not recognize an error code provided by the TFTP server.	Contact the Cisco TAC.
TFTP file not found	The requested load file (.bin) was not found in the TFTPPath directory.	Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose <b>Device &gt; Phone</b> ). Verify that the TFTPPath directory contains a .bin file with this load ID as the name.
TFTP timeout	TFTP server did not respond.	<ul style="list-style-type: none"> <li>• Network is busy. The errors should resolve themselves when the network load reduces.</li> <li>• No network connectivity between the TFTP server and the phone. Verify the network connections.</li> <li>• TFTP server is down. Check the TFTP server configuration.</li> </ul>
Timed Out	Supplicant attempted 802.1X transaction but timed out due to the absence of an authenticator.	Authentication typically times out if 802.1X is not configured on the switch.

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

## Display Network Statistics Screen

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

### Procedure

- 
- Step 1** Press **Applications**.
  - Step 2** Select **Admin Settings**.
  - Step 3** Select **Status**.
  - Step 4** Select **Network Statistics**. [Network Statistics Fields](#), on page 83 describes the information that appears in this screen.
  - Step 5** To exit the Network Statistics screen, press **Back** .
- 

### Network Statistics Fields

The following table lists the Network Statistics Message information.

**Table 13: Network Statistics Message Information for the Cisco Unified SIP Phone 3905**

Item	Description
Rx Frames	Number of packets received by the phone
Tx Frames	Number of packets sent by the phone
Rx Broadcasts	Number of broadcast packets received by the phone

Item	Description
Restart Cause	<p>Cause of the last reset of the phone - One of these values:</p> <ul style="list-style-type: none"> <li>• Hardware Reset (Power-on reset)</li> <li>• Software Reset (memory controller also reset)</li> <li>• Software Reset (memory controller not reset)</li> <li>• Watchdog Reset</li> <li>• Unknown</li> </ul>
Port 1	Link state and connection of the PC port (for example, Auto 100 Mb Full-Duplex means that the PC port is in a link-up state and has auto-negotiated a full-duplex, 100-Mbps connection)
Port 2	Link state and connection of the Network port
DHCP state (IPv4 / IPv6)	<ul style="list-style-type: none"> <li>• In IPv4 mode, displays only the DHCPv4 state, such as DHCP BOUND.</li> <li>• In IPv6 mode, displays only the DHCPv6 state, such as ROUTER ADVERTISE, (GOOD IP).</li> <li>• In dual-stack mode, displays both DHCPv4 and DHCPv6 state information.</li> </ul> <p>For more information, see the following DHCPv4 network statistics and DHCPv6 network statistics tables.</p>

**Table 14: DHCPv4 Network Statistics**

DHCPv4 State	Description
CDP INIT	CDP is not bound or WLAN is not in service
DHCP BOUND	DHCPv4 is BOUND
DHCP DISABLED	DHCPv4 is disabled
DHCP INIT	DHCPv4 is INIT
DHCP INVALID	DHCPv4 is INVALID; this is initial state
DHCP RENEWING	DHCPv4 is RENEWING
DHCP REBINDING	DHCPv4 is REBINDING
DHCP REBOOT	DHCPv4 is init-reboot



<b>DHCPv4 State</b>	<b>Description</b>
DHCP REQUESTING	DHCPv4 is requesting
DHCP RESYNC	DHCPv4 is RESYNCH
DHCP WAITING COLDBOOT TIMEOUT	DHCPv4 is booting
DHCP UNRECOGNIZED	Unrecognized DHCPv4 state
DISABLED DUPLICATE IP	Duplicated IPv4 Address
DHCP TIMEOUT	DHCPv4 Timeout
IPV4 STACK TURNED OFF	Phone is in IPv6-only mode with IPv4 Stack turned off
ILLEGAL IPV4 STATE	Illegal IPv4 state and should not happen

**Table 15: DHCPv6 Network Statistics**

<b>DHCPv6 State</b>	<b>Description</b>
CDP INIT	CDP is initializing
DHCP6 BOUND	DHCPv6 is BOUND
DHCP6 DISABLED	DHCPv6 is DISABLED
DHCP6 RENEW	DHCPv6 is renewing
DHCP6 REBIND	DHCPv6 is rebinding
DHCP6 INIT	DHCPv6 is initializing
DHCP6 SOLICIT	DHCPv6 is soliciting
DHCP6 REQUEST	DHCPv6 is requesting
DHCP6 RELEASING	DHCPv6 is releasing
DHCP6 RELEASED	DHCPv6 is released
DHCP6 DISABLING	DHCPv6 is disabling
DHCP6 DECLINING	DHCPv6 is declining
DHCP6 DECLINED	DHCPv6 is declined

DHCPv6 State	Description
DHCP6 INFOREQ	DHCPv6 is INFOREQ
DHCP6 INFOREQ DONE	DHCPv6 is INFOREQ DONE
DHCP6 INVALID	DHCPv6 is INVALID; this is initial state
DISABLED DUPLICATE IPV6	DHCP6 is DISABLED, but DUPLICATE IPV6 DETECTED
DHCP6 DECLINED DUPLICATE IP	DHCP6 is DECLINED -- DUPLICATE IPV6 DETECTED
ROUTER ADVERTISE., (DUPLICATE IP)	Duplicated autoconfigured IPv6 address
DHCP6 WAITING COLDBOOT TIMEOUT	DHCPv6 is booting
DHCP6 TIMEOUT USING RESTORED VAL	DHCPv6 timeout, using the value saved in flash memory
DHCP6 TIMEOUT CANNOT RESTORE	DHCP6 timeout and there is no backup from flash memory
IPV6 STACK TURNED OFF	Phone is in IPv4-only mode with IPv6 Stack turned off
ROUTER ADVERTISE., (GOOD IP)	
ROUTER ADVERTISE., (BAD IP)	
UNRECOGNIZED MANAGED BY	IPv6 Address is not from router or DHCPv6 server
ILLEGAL IPV6 STATE	Illegal IPv6 state and should not happen

## 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 not available on the phone. For more information about remote monitoring, see [Cisco IP Phone Web Page, on page 88](#).

A single call can have multiple voice streams, but data is captured for only the last voice stream. A voice stream is a packet stream between two endpoints. If one endpoint is put on hold, the voice stream stops even

though the call is still connected. When the call resumes, a new voice packet stream begins, and the new call data overwrites the former call data.

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

### Procedure

- 
- Step 1** Press **Applications**.
- Step 2** Select **Admin Settings**.
- Step 3** Select **Status**.
- Step 4** Select **Call Statistics**.  
[Call Statistics Fields](#), on page 87 describes the information that appears in this window.
- Step 5** To exit the Call Statistics window, press **Back** .
- 

### Call Statistics Fields

The following table contains the fields in the Call Statistics screen.

**Table 16: Call Statistics Items for the Cisco Unified SIP Phone 3905**

Item	Description
Rcvr Codec	Type of voice stream received (RTP streaming audio from codec): G.729, G.711 u-law, G.711 A-law.
Sender Codec	Type of voice stream transmitted (RTP streaming audio from codec): G.729, G.711 u-law, G.711 A-law.
Avg Jitter	Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network) observed since the receiving voice stream was opened.
Max Jitter	Maximum jitter observed since the receiving voice stream was opened.
Voice Quality Metrics	
MOS LQK	Objective estimate of the Mean Opinion Score (MOS) for Listening Quality (LQK) that ranks audio quality from 5 (excellent) to 1 (bad). This score is based on audible-concealment events due to a frame loss in the preceding 8 seconds of the voice stream.  <b>Note</b> The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.
Avg MOS LQK	Average MOS LQK score for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score from the start of the voice stream.

Item	Description
Max MOS LQK	Baseline or highest MOS LQK score from the start of the voice stream. The following codecs provide the corresponding maximum MOS LQK scores under normal conditions with no frame loss: <ul style="list-style-type: none"> <li>• G.711: 4.5</li> <li>• G729A/AB: 3.7</li> </ul>
MOS LQK Version	Version of the Cisco-proprietary algorithm used to calculate the MOS LQK scores.
Latency	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.

## 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 Model Information Window, on page 77](#)
- [Control Phone Web Page Access, on page 72](#)

## Access Web Page for Phone

To access the web page for a Cisco Unified IP Phone, perform these steps.



### Note

If you cannot access the web page, it may be disabled. See [Control Phone Web Page Access, on page 72](#) for more information.

## Procedure

- 
- Step 1** Obtain the IP address of the Cisco Unified IP Phone using one of these methods:
- Search for the phone in Cisco Unified Communications Manager by choosing **Device > Phone**. Phones registered with Cisco Unified Communications Manager display the IP address on the **Find and List Phones** window and at the top of the **Phone Configuration** window.
  - On the Cisco Unified IP Phone, press **Applications**, choose **Network > IPv4**, 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`
- 

## Device Information

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

To display the Device Information area, access the web page for the phone as described in [Access Web Page for Phone](#), on page 88, and click the **Device Information** hyperlink.

**Table 17: Device Information Area Items**

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

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

## Network Setup Page

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

You can view and set many of these items from the Network Setup Menu and the Phone Information Menu on the Cisco Unified IP Phone. For more information, see [Cisco Unified SIP Phone Installation](#), on page 21

To display the Network Setup area, access the web page for the phone as described in the [Access Web Page for Phone](#), on page 88, and click the Network Configuration hyperlink.

**Table 18: Network Setup Area items**

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

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

<b>Item</b>	<b>Description</b>
SW Port Setup Auto Negotiate	Indicates if switch port is set to auto negotiate.
PC Port Setup Auto Negotiate	Indicates if PC port is set to auto negotiate.
User Locale	User locale associated with the phone user. Identifies a set of detailed information to support users, including language, font, date and time formatting, and alphanumeric keyboard text information.
Network Locale	Network locale associated with the phone user. Identifies a set of detailed information to support the phone in a specific location, including definitions of the tones and cadences used by the phone.
User Locale Version	Version of the user locale loaded on the phone.
Network Locale Version	Version of the network locale loaded on the phone.
PC Port Disabled	Indicates if the PC port on the phone is enabled or disabled.
Speaker Enabled	Indicates if the speakerphone is enabled on the phone.
GARP Enabled	Indicates if the phone learns MAC addresses from Gratuitous ARP responses.
Voice VLAN Enabled	Indicates if the phone allows a device attached to the PC port to access the Voice VLAN.
DSCP for Call Control	DSCP IP classification for call control signaling.
DSCP for Configuration	DSCP IP classification for any phone configuration transfer.
DSCP for Services	DSCP IP classification for phone-based services.
Web Access Enabled	Indicates if web access is enabled (Yes) or disabled (No) for the phone.
Span to PC Port	Indicates if the phone forwards packets transmitted and received on the network port to the access port.
PC VLAN	VLAN used to identify and remove 802.1P/Q tags from packets sent to the PC.



Item	Description
CDP: PC Port	<p>Indicates if CDP is supported on the PC port (default is enabled).</p> <p>Enable CDP on the PC port when Cisco VT Advantage/Unified Video Advantage (CVTA) is connected to the PC port. CVTA does not work without CDP interaction with the phone.</p> <p>When CDP is disabled in Cisco Unified Communications Manager, a warning is displayed, indicating that disabling CDP on the PC port prevents CVTA from working.</p> <p>The current PC and switch port CDP values are shown on the Settings menu.</p>
CDP: SW Port	<p>Indicates if CDP is supported on the switch port (default is enabled).</p> <p>Enable CDP on the switch port for VLAN assignment for the phone, power negotiation, QoS management, and 802.1x security.</p> <p>Enable CDP on the switch port when the phone is connected to a Cisco switch.</p> <p>When CDP is disabled in Cisco Unified Communications Manager, a warning is presented, indicating that CDP should be disabled on the switch port only if the phone is connected to a non-Cisco switch.</p> <p>The current PC and switch port CDP values are shown on the Settings menu.</p>
IP Addressing Mode	Type of addressing - IPv4 only, IPv6 only, or dual stack
IP Preference Mode Control	
IPv6 Auto Configuration	
DHCPv6	IP address of the IPv6 DHCP server from which the phone obtains its IPv6 address.
IPv6 Address	IPv6 address of the phone.
IPv6 Prefix Length	Current prefix length for the subnet.
IPv6 Default Router 1	Default IPv6 router used by the phone.
IPv6 DNS Server 1	Primary IPv6 DNS server used by the phone.
IPv6 Alternate TFTP	Indicates if the phone is using an alternative IPv6 TFTP server.
IPv6 TFTP Server 1	Primary IPv6 Trivial File Transfer Protocol (TFTP) server used by the phone.
IPv6 TFTP Server 2	Secondary IPv6 Trivial File Transfer Protocol (TFTP) server used by the phone.
IPv6 Address Released	

## Network Statistics

The following table lists the Network Statistics information.

**Table 19: Network Statistics information**

Item	Description
Rx Frames	Number of packets received by the phone
Tx Frames	Number of packets sent by the phone
Rx Broadcasts	Number of broadcast packets received by the phone
Restart Cause	Cause of the last reset of the phone - One of these values: <ul style="list-style-type: none"> <li>• Hardware Reset (Power-on reset)</li> <li>• Software Reset (memory controller also reset)</li> <li>• Software Reset (memory controller not reset)</li> <li>• Watchdog Reset</li> <li>• Unknown</li> </ul>
Port 1	Link state and connection of the Network port
Port 2	Link state and connection of the PC port (for example, Auto 100 Mb Full-Duplex means that the PC port is in a link-up state and has auto-negotiated a full-duplex, 100-Mbps connection)
DHCPv4 State DHCPv6 State	<ul style="list-style-type: none"> <li>• In IPv4 mode, displays only the DHCPv4 state, such as DHCP BOUND.</li> <li>• In IPv6 mode, displays only the DHCPv6 state, such as ROUTER ADVERTISE, (GOOD IP).</li> <li>• In dual-stack mode, displays both DHCPv4 and DHCPv6 state information.</li> </ul> <p>For more information, see the following DHCPv4 network statistics and DHCPv6 network statistics tables.</p>

**Table 20: DHCPv4 network statistics**

DHCPv4 State	Description
CDP INIT	CDP is not bound or WLAN is not in service
DHCP BOUND	DHCPv4 is BOUND

DHCPv4 State	Description
DHCP DISABLED	DHCPv4 is disabled
DHCP INIT	DHCPv4 is INIT
DHCP INVALID	DHCPv4 is INVALID; this is initial state
DHCP RENEWING	DHCPv4 is RENEWING
DHCP REBINDING	DHCPv4 is REBINDING
DHCP REBOOT	DHCPv4 is init-reboot
DHCP REQUESTING	DHCPv4 is requesting
DHCP RESYNC	DHCPv4 is RESYNCH
DHCP WAITING COLDBOOT TIMEOUT	DHCPv4 is booting
DHCP UNRECOGNIZED	Unrecognized DHCPv4 state
DISABLED DUPLICATE IP	Duplicated IPv4 Address
DHCP TIMEOUT	DHCPv4 Timeout
IPV4 STACK TURNED OFF	Phone is in IPv6-only mode with IPv4 Stack turned off
ILLEGAL IPV4 STATE	Illegal IPv4 state and should not happen

### Ethernet Information Web Page

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

**Table 21: Ethernet Information Items**

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

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

### Network Information Fields

The following table describes the information in the Network Area web page.

**Table 22: Network Items on the Cisco Unified SIP Phone 3905**

Item	Description
Tx Frames	Total number of packets transmitted by the phone
Tx broadcast	Total number of broadcast packets transmitted by the phone
Tx unicast	Total number of unicast packets transmitted by the phone
Rx Frames	Total number of packets received by the phone
Rx broadcast	Total number of broadcast packets received by the phone
Rx unicast	Total number of unicast packets received by the phone
Neighbor Device ID	Identifier of a device connected to this port discovered by CDP protocol or LLDP
Neighbor IP Address	IP address of the neighbor device discovered by CDP protocol
Neighbor Port	Neighbor device port to which the phone is connected discovered by CDP protocol
LLDP AgeoutsTotal	Total number of LLDP frames that have been time out in cache
LLDP FramesDiscardedTotal	Total number of LLDP frames that are discarded when any of the mandatory TLVs is missing or out of order or contains out of range string length
LLDP FramesInErrorsTotal	Total number of LLDP frames that received with one or more detectable errors
LLDP FramesInTotal	Total number of LLDP frames received on the phone
LLDP TLVDiscardedTotal	Total number of LLDP TLVs that are discarded

Item	Description
LLDP TLVUnrecognizedTotal	Total number of LLDP TLVs that are not recognized on the phone
Restart Cause	Reason for the last restart
Port 1-2	Speed and duplex information
IPv4	IPv4 Address
IPv6	IPv6 Address

## Device Logs

The following device logs hyperlinks on a phone web page provide information you can use to help monitor and troubleshoot the phone.

- **Console Logs:** Includes hyperlinks to individual log files. The console log files include debug and error messages received on the phone.
- **Core Dumps:** Includes hyperlinks to individual dump files. The core dump files include data from a phone crash.
- **Status Messages:** Displays up to the 30 most recent status messages that the phone has generated since it was last powered up. You can also see this information from the Status Messages screen on the Web page of the phone. The following table describes the status messages that may be displayed.
- **Debug Display:** Displays debug messages that might be useful to the Cisco Technical Assistance Center (TAC) if you require assistance with troubleshooting.

The Status Messages web page displays up to 30 of the most recent status messages that the phone has generated since it was last powered up. You can access the Status Messages web page even if the phone is not running. The following table describes the status messages. This table also includes possible explanations and actions to troubleshoot errors.

**Table 23: Status Messages**

Message	Description	Possible explanation and action
CFG file not found	The name-based and default configuration file was not found on the TFTP Server.	<p>The configuration file for a phone is created when the phone is added to the Cisco Unified Communications Manager database. If the phone has not been added to the Cisco Unified Communications Manager database, the TFTP server generates a <code>CFG File Not Found</code> response.</p> <ul style="list-style-type: none"> <li>• Phone is not registered with Cisco Unified Communications Manager. You must manually add the phone to Cisco Unified Communications Manager if you are not allowing phones to autoregister. See <a href="#">Phone Addition Methods</a>, on page 42 for details.</li> <li>• If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server.</li> <li>• If you are using static IP addresses, check the TFTP server configuration.</li> </ul>
CFG TFTP Size Error	The configuration file is too large for the file system on the phone.	Power cycle the phone.
Checksum Error	Downloaded software file is corrupted.	Obtain a new copy of the phone firmware and place it in the TFTPPath directory. You should only copy files into this directory when the TFTP server software is shut down, otherwise the files may be corrupted.
DHCP timeout	DHCP server did not respond.	<ul style="list-style-type: none"> <li>• Network is busy. The errors should resolve themselves when the network load reduces.</li> <li>• No network connectivity between the DHCP server and the phone. Verify the network connections.</li> <li>• DHCP server is down. Check the DHCP server configuration.</li> <li>• Errors persist. Consider assigning a static IP address.</li> </ul>

Message	Description	Possible explanation and action
DNS timeout	DNS server did not respond.	<ul style="list-style-type: none"> <li>• Network is busy. The errors should resolve themselves when the network load reduces.</li> <li>• No network connectivity between the DNS server and the phone. Verify the network connections.</li> <li>• DNS server is down. Check the DNS server configuration.</li> </ul>
DNS unknown host	DNS could not resolve the name of the TFTP server or Cisco Unified Communications Manager.	<ul style="list-style-type: none"> <li>• Verify that the host names of the TFTP server or Cisco Unified Communications Manager are configured properly in DNS.</li> <li>• Consider using IP addresses rather than host names.</li> </ul>
Duplicate IP	Another device is using the IP address assigned to the phone.	<ul style="list-style-type: none"> <li>• If the phone has a static IP address, verify that you have not assigned a duplicate IP address.</li> <li>• If you are using DHCP, check the DHCP server configuration.</li> </ul>
File not found	The phone cannot locate, on the TFTP server, the phone load file that is specified in the phone configuration file.	From Cisco Unified Operating System Administration, make sure that the phone load file is on the TFTP server, and that the entry in the configuration file is correct.
IP address released	The phone has been configured to release its IP address.	The phone remains idle until it is power cycled or you reset the DHCP address.
Load ID incorrect	Load ID of the software file is of the wrong type.	Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose <b>Device &gt; Phone</b> ). Verify that the load ID is entered correctly.
Load rejected HC	The application that was downloaded is not compatible with the phone's hardware.	Occurs if you were attempting to install a version of software on this phone that did not support hardware changes on this newer phone.  Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose <b>Device &gt; Phone</b> ). Re-enter the load displayed on the phone.

Message	Description	Possible explanation and action
No default router	DHCP or static configuration did not specify a default router.	<ul style="list-style-type: none"> <li>• If the phone has a static IP address, verify that the default router has been configured.</li> <li>• If you are using DHCP, the DHCP server has not provided a default router. Check the DHCP server configuration.</li> </ul>
No DNS server IP	A name was specified but DHCP or static IP configuration did not specify a DNS server address.	<ul style="list-style-type: none"> <li>• If the phone has a static IP address, verify that the DNS server has been configured.</li> <li>• If you are using DHCP, the DHCP server has not provided a DNS server. Check the DHCP server configuration.</li> </ul>
TFTP access error	TFTP server is pointing to a directory that does not exist.	<ul style="list-style-type: none"> <li>• If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server.</li> <li>• If you are using static IP addresses, check the TFTP server configuration.</li> </ul>
TFTP error	The phone does not recognize an error code provided by the TFTP server.	Contact the Cisco TAC.
TFTP file not found	The requested load file (.bin) was not found in the TFTPPath directory.	Check the load ID assigned to the phone (from Cisco Unified Communications Manager, choose <b>Device &gt; Phone</b> ). Verify that the TFTPPath directory contains a .bin file with this load ID as the name.
TFTP timeout	TFTP server did not respond.	<ul style="list-style-type: none"> <li>• Network is busy. The errors should resolve themselves when the network load reduces.</li> <li>• No network connectivity between the TFTP server and the phone. Verify the network connections.</li> <li>• TFTP server is down. Check the TFTP server configuration.</li> </ul>
Timed Out	Supplicant attempted 802.1X transaction but timed out due to the absence of an authenticator.	Authentication typically times out if 802.1X is not configured on the switch.



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

## Streaming Statistics

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

The streaming statistics areas on a phone web page provide information about the streams. Cisco Unified SIP Phone 3905 use only Stream 1.

To display a Streaming Statistics area, access the web page for the phone as described in [Access Web Page for Phone](#), on page 88 and click the Stream 1 hyperlink.

**Table 24: Streaming Statistics Area Items**

Item	Description
Remote Address	IP address and UDP port of the destination of the stream.
Local Address	IP address and UDP port of the phone.
Start Time	Internal time stamp indicating when Cisco Unified Communications Manager requested that the phone start transmitting packets.
Stream Status	Indication of whether streaming is active or not.
Host Name	Unique, fixed name that is automatically assigned to the phone based on its MAC address.
Sender Packets	Total number of RTP data packets transmitted by the phone since starting this connection. The value is 0 if the connection is set to receive only mode.
Sender Octets	Total number of payload octets transmitted in RTP data packets by the phone since starting this connection. The value is 0 if the connection is set to receive only mode.
Sender Codec	Type of audio encoding used for the transmitted stream.
Sender Reports Sent	Number of times the RTCP Sender Report have been sent. When the RTCP Control Protocol is disabled, no data generates for this field and thus displays as 0.

Item	Description
Sender Report Time Sent	Internal time stamp indication when the last RTCP Sender Report was sent. When the RTCP Control Protocol is disabled, no data generates for this field and thus displays as 0.
Rcvr Lost Packets	Total number of RTP data packets that have been lost since starting receiving data on this connection. Defined as the number of expected packets less the number of packets actually received, where the number of received packets includes any that are late or duplicate. The value displays as 0 if the connection was set to send-only mode.
Avg Jitter	Estimate of mean deviation of the RTP data packet inter-arrival time, measured in milliseconds. The value displays as 0 if the connection was set to send-only mode.
Rcvr Codec	Type of audio encoding used for the received stream.
Rcvr Reports Sent	Number of times the RTCP Receiver Reports have been sent. When the RTCP Control Protocol is disabled, no data generates for this field and thus displays as 0.
Rcvr Report Time Sent	Internal time stamp indication when a RTCP Receiver Report was sent. When the RTCP Control Protocol is disabled, no data generates for this field and thus displays as 0.
Rcvr Packets	Total number of RTP data packets received by the phone since starting receiving data on this connection. Includes packets received from different sources if this is a multicast call. The value displays as 0 if the connection was set to send-only mode.
Rcvr Octets	Total number of payload octets received in RTP data packets by the device since starting reception on the connection. Includes packets received from different sources if this is a multicast call. The value displays as 0 if the connection was set to send-only mode.
MOS LQK	Objective estimate of the Mean Opinion Score (MOS) for Listening Quality (LQK) that ranks audio quality from 5 (excellent) to 1 (bad). This score is based on audible-concealment events due to a frame loss in the preceding 8 seconds of the voice stream.  <b>Note</b> The MOS LQK score can vary based on the type of codec that the Cisco Unified IP Phone uses.
Avg MOS LQK	Average MOS LQK score for the entire voice stream.
Min MOS LQK	Lowest MOS LQK score from the start of the voice stream.

Item	Description
Max MOS LQK	<p>Baseline or highest MOS LQK score from the start of the voice stream.</p> <p>The following codecs provide the corresponding maximum MOS LQK scores under normal conditions with no frame loss:</p> <ul style="list-style-type: none"> <li>• G.711: 4.5</li> <li>• G729A/AB: 3.7</li> </ul>
MOS LQK Version	Version of the Cisco-proprietary algorithm used to calculate the MOS LQK scores.
Cumulative Conceal Ratio	Total number of concealment frames divided by total number of speech frames received from start of the voice stream.
Interval Conceal Ratio	Ratio of concealment frames to speech frames in preceding 3-second interval of active speech. If using voice activity detection (VAD), a longer interval might be required to accumulate 3 seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from start of the voice stream.
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Secs	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.
Latency	<p>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.</p> <p>When the RTCP Control Protocol is disabled, no data generates for this field and thus displays as 0.</p>
Max Jitter	Maximum value of instantaneous jitter, in milliseconds.
Sender Size	RTP packet size, in milliseconds, for the transmitted stream.
Sender Reports Received	<p>Number of times RTCP Sender Reports have been received.</p> <p>When the RTCP Control Protocol is disabled, no data generates for this field and thus displays as 0.</p>
Sender Report Time Received	<p>Last time at which an RTCP Sender Report was received.</p> <p>When the RTCP Control Protocol is disabled, no data generates for this field and thus displays as 0.</p>
Revr Size	RTP packet size, in milliseconds, for the received stream.
Revr Discarded	RTP packets received from network but discarded from jitter buffers.

Item	Description
Rcvr Reports Received	Number of times RTCP Receiver Reports have been received. When the RTCP Control Protocol is disabled, no data generates for this field and thus displays as 0.
Rcvr Report Time Received	Last time at which an RTCP Receiver Report was received. When the RTCP Control Protocol is disabled, no data generates for this field and thus displays as 0.



# Troubleshooting

---

- [Troubleshooting Overview](#), page 105
- [Startup Problems](#), page 105
- [Phone Reset Problems](#), page 109
- [Cisco IP Phone Security Problems](#), page 111
- [Audio and Video Problems](#), page 113
- [General Telephone Call Problems](#), page 115
- [Troubleshooting Procedures](#), page 116
- [Additional Troubleshooting Information](#), page 120

## Troubleshooting Overview

This chapter provides information that can assist you in troubleshooting problems with your Cisco Unified IP Phone or with your IP telephony network. It also explains how to maintain your voice network and clean your phone.

If you need additional assistance to resolve an issue, see [Documentation, Support, and Security Guidelines](#), on page xi.

This chapter includes these topics:

## Startup Problems

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

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

### Related Topics

[Verify Phone Startup](#), on page 35

## 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

[Verify Phone Startup](#), on page 35

## 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 116 for more information.

## Phone Displays Error Messages

### Problem

Status messages display errors during startup.

### Solution

While the phone cycles through the startup process, you can access status messages that might provide you with information about the cause of a problem. See [Display Status Messages 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 79

## 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 116

## 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 117](#)

## 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 117](#).

## 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 42](#) to ensure that the phone is added to the Cisco Unified Communications Manager database.

To verify that the phone is in the Cisco Unified Communications Manager database, choose **Device > Phone** from Cisco Unified Communications Manager Administration. Click **Find** to search for the phone based on the MAC Address. For information about determining a MAC address, see [Determine Phone MAC Address, on page 42](#).



If the phone is already in the Cisco Unified Communications Manager database, the configuration file may be damaged. See [Configuration File Corruption, on page 108](#) for assistance.

## Cisco IP Phone Cannot Obtain IP Address

### Problem

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

### Solution

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

## Phone Reset Problems

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

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

## Phone Cannot Connect to LAN

### Problem

The physical connection to the LAN may be broken.

### Solution

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

## Phone Resets Due to Intermittent Network Outages

### Problem

Your network may be experiencing intermittent outages.

### Solution

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

## Phone Resets Due to DHCP Setting Errors

### Problem

The DHCP settings may be incorrect.

### Solution

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

### Related Topics

[Check DHCP Settings, on page 117](#)

## Phone Resets Due to Incorrect Static IP Address

### Problem

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

### Solution

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

## Phone Resets During Heavy Network Usage

### Problem

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

### Solution

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

## Phone Resets Due to Intentional Reset

### Problem

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

### Solution

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

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

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

## Phone Resets Due to DNS or Other Connectivity Issues

### Problem

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

### Solution

If the phone continues to reset, eliminate DNS or other connectivity errors by following the procedure in [Determine DNS or Connectivity Issues](#), on page 118.

## Phone Does Not Power Up

### Problem

The phone does not appear to be powered up.

### Solution

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

## Cisco IP Phone Security Problems

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

### 802.1X Authentication Problems

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

**Table 25: 802.1X Authentication Problem Identification**

If all the following conditions apply,	See
<ul style="list-style-type: none"> <li>• Phone cannot obtain a DHCP-assigned IP address.</li> <li>• Phone does not register with Cisco Unified Communications Manager.</li> <li>• Phone status displays <code>Configuring IP</code> or <code>Registering</code>.</li> <li>• 802.1X Authentication Status displays <code>Held</code>.</li> <li>• Status menu 802.1X status displays <code>Failed</code>.</li> </ul>	<a href="#">802.1X Enabled on Phone but Phone Does Not Authenticate, on page 112</a>
<ul style="list-style-type: none"> <li>• Phone cannot obtain a DHCP-assigned IP address.</li> <li>• Phone does not register with Cisco Unified Communications Manager.</li> <li>• Phone status displays <code>Configuring IP</code> or <code>Registering</code>.</li> <li>• 802.1X Authentication Status displays <code>Disabled</code>.</li> <li>• Status menu displays that the DHCP status has timed out.</li> </ul>	<a href="#">802.1X Not Enabled, on page 113</a>
<ul style="list-style-type: none"> <li>• Phone cannot obtain a DHCP-assigned IP address.</li> <li>• Phone does not register with Cisco Unified Communications Manager.</li> <li>• Phone status display as <code>Configuring IP</code> or <code>Registering</code>.</li> <li>• You are unable to access phone menus to verify 802.1X status.</li> </ul>	<a href="#">Factory Reset of Phone Has Deleted 802.1X Shared Secret, on page 113</a>

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

### Problem

The phone cannot authenticate.

**Cause**

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

**Solution**

To resolve this problem, check the 802.1X and shared secret configuration. See [Identify 802.1X Authentication Problems](#), on page 119.

## 802.1X Not Enabled

**Problem**

The phone does not have 802.1X configured.

**Cause**

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

**Solution**

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

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

**Problem**

After a reset, the phone does not authenticate.

**Cause**

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

**Solution**

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

**Related Topics**

[Basic Reset](#)

## Audio and Video Problems

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

## No Speech Path

**Problem**

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

**Solution**

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

## Choppy Speech

**Problem**

A user complains of choppy speech on a call.

**Cause**

There may be a mismatch in the jitter configuration.

**Solution**

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

## 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.

## 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.

## General Telephone Call Problems

The following sections help troubleshoot general telephone call problems.

### Phone Call Cannot Be Established

**Problem**

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

**Cause**

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

**Solution**

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

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

**Problem**

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

**Cause**

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

**Solution**

Keys should not be pressed rapidly.

## Phone Bandwidth Restrictions

### Problem

Users report frequent Not enough bandwidth messages on their phones.

### Cause

The Cisco Unified Communications Manager does not have adequate bandwidth to place the call or there are policy restrictions.

### Solution

For information on changing the Cisco Unified Communications Manager bandwidth, see the documentation for your particular version of Cisco Unified Communications Manager.

## Troubleshooting Procedures

These procedures can be used to identify and correct problems.

### Check TFTP Settings

#### Procedure

---

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

#### Related Topics


[Phone Cannot Connect to TFTP Server, on page 107](#)



## Check DHCP Settings

### Procedure

---

- Step 1** On the Cisco IP Phone, press **Applications** .
- Step 2** Select **Admin 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:  
[http://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod\\_tech\\_notes\\_list.html](http://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html)
  - **IP Address, Subnet Mask, Default Router:** If you have assigned a static IP address to the phone, you must manually enter settings for these options.
- Step 3** If you are using DHCP, check the IP addresses that your DHCP server distributes. See the *Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks* document, available at this URL:  
[http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_tech\\_note09186a00800f0804.shtml](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml)
- 

### Related Topics

- [Phone Cannot Connect to Server, on page 107](#)
- [Phone Resets Due to DHCP Setting Errors, on page 110](#)

## Start Service



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

---

To start a service, follow these steps:

### Procedure

---

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

---

## 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 42

## 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 Phone MAC Address, on page 42](#)

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

## Additional Troubleshooting Information

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

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



# Maintenance

- [Basic Reset](#), page 121
- [Voice Quality Monitoring](#), page 122
- [Cisco IP Phone Cleaning](#), page 124

## Basic Reset

Performing a basic reset of a Cisco IP Phone provides a way to recover if the phone experiences an error and provides a way to reset or restore various configuration and security settings.

The following table describes the ways to perform a basic reset. You can reset a phone after the phone has started up. Choose the operation that is appropriate for your situation.

**Table 26: Basic Reset Method**

Operation	Action	Explanation
Restart phone	Press <b>Services, Applications, or Directories</b> and then press <b>***#**</b> .	Resets any user and network setup changes that you have made, but that the phone has not written to its Flash memory, to previously saved settings, then restarts the phone.

## Reset 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

	Command or Action	Purpose
<b>Step 1</b>	Remove power from the phone in one of these ways: <ul style="list-style-type: none"> <li>• Unplug the power adapter.</li> </ul>	

	Command or Action	Purpose
	<ul style="list-style-type: none"> <li>Unplug the LAN cable.</li> </ul>	
<b>Step 2</b>	Press the pound (#) key and plug the phone in.	
<b>Step 3</b>	When prompted, 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 **Admin Settings > Reset All**.  
If required, unlock the phone options.
- Step 3** Choose **Yes** and press **Select**.
- 

### Related Topics

[Apply Phone Password, on page 25](#)

## Voice Quality Monitoring

To measure the voice quality of calls that are sent and received within the network, Cisco IP Phones use these statistical metrics that are based on concealment events. The DSP plays concealment frames to mask frame loss in the voice packet stream.

- Concealment Ratio metrics: Show the ratio of concealment frames over total speech frames. An interval conceal ratio is calculated every 3 seconds.
- Concealed Second metrics: Show the number of seconds in which the DSP plays concealment frames due to lost frames. A severely “concealed second” is a second in which the DSP plays more than five percent concealment frames.



### Note

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

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

## Voice Quality Troubleshooting Tips

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

**Table 27: Changes to Voice Quality Metrics**

Metric change	Condition
Conceal Ratio and Conceal Seconds increase significantly	Network impairment from packet loss or high jitter.
Conceal Ratio is near or at zero, but the voice quality is poor.	<ul style="list-style-type: none"> <li>Noise or distortion in the audio channel such as echo or audio levels.</li> <li>Tandem calls that undergo multiple encode/decode such as calls to a cellular network or calling card network.</li> <li>Acoustic problems coming from a speakerphone, handsfree cellular phone or wireless headset.</li> </ul> <p>Check packet transmit (TxCnt) and packet receive (RxCnt) counters to verify that voice packets are flowing.</p>
MOS LQK scores decrease significantly	<p>Network impairment from packet loss or high jitter levels:</p> <ul style="list-style-type: none"> <li>Average MOS LQK decreases may indicate widespread and uniform impairment.</li> <li>Individual MOS LQK decreases may indicate bursty impairment.</li> </ul> <p>Cross-check the conceal ratio and conceal seconds for evidence of packet loss and jitter.</p>
MOS LQK scores increase significantly	<ul style="list-style-type: none"> <li>Check to see if the phone is using a different codec than expected (RxType and TxType).</li> <li>Check to see if the MOS LQK version changed after a firmware upgrade.</li> </ul>



**Note**

Voice quality metrics do not account for noise or distortion, only frame loss.

## Cisco IP Phone Cleaning

To clean your Cisco IP Phone, use only a dry soft cloth to gently wipe the phone and the phone screen. Do not apply liquids or powders directly to the phone. As with all non-weatherproof electronics, liquids and powders can damage the components and cause failures.

When the phone is in sleep mode, the screen is blank and the Select button is not lit. When the phone is in this condition, you can clean the screen, as long as you know that the phone will remain asleep until after you finish cleaning.





## International User Support

---

- [Unified Communications Manager Endpoints Locale Installer](#), page 125
- [International Call Logging Support](#), page 125
- [Language Limitation](#), page 126

### 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 Alpha-Numeric 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.