Cisco DX Series Administration Guide, Release 10.2(4)

First Published: June 23, 2015

Last Modified: October 26, 2015

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)

The Bluetooth word mark and logo are registered trademarks owned by Bluetooth SIG, Inc., and any use of such marks by Cisco Systems, Inc., is under license.

Google, Google Play, Android and certain other marks are trademarks of Google Inc.

The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing LLC in the United States and other countries.

© 2015 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface xiii

Overview xiii

Guide Conventions xiii

Related Documentation xiv

Terminology Differences xv

Documentation, Support, and Security Guidelines xvi

Cisco Product Security Overview xvi

CHAPTER 1

Technical Specifications 1

Physical and Operating Environment Specifications 1

Network and Computer Port Pinouts 2

Network Port Connector Pinouts 3

Computer Port Connector Pinouts 3

Ports Used by Cisco DX Series Devices 4

Network Protocols 5

Power Requirements 9

Power Guidelines 10

Power Reduction 10

Power Save Mode 11

EnergyWise Mode 11

Power Negotiation Over LLDP 12

Additional Information About Power 12

External Devices 13

USB Port and USB Serial Console Data Information 13

Use USB Console 14

Behavior During Times of Network Congestion 15

CHAPTER 2 Device Descriptions 17

Cisco DX70 Hardware 17

Cisco DX70 Cable Installation 18

Cisco DX80 Hardware 19

Cisco DX80 Cable Installation 20

Cisco DX650 Hardware 21

Cisco DX650 Cable Installation 21

No Radio Hardware 22

CHAPTER 3 Wi-Fi Network Setup 23

Network Requirements 23

Wireless LAN 24

Wi-Fi Network Components 25

AP Channel and Domain Relationships 25

AP Interactions 25

Access Point Association 26

QoS in Wireless Network 26

Set Up Flexible DSCP 28

Cisco Unified Communications Manager Interaction 28

802.11 Standards for WLAN Communications 28

World Mode (802.11d) 29

Wireless Modulation Technologies 30

Radio Frequency Ranges 31

Security for Communications in WLANs 31

Authentication Methods 31

Authenticated Key Management 32

Encryption Methods 32

AP Authentication and Encryption Options 33

WLANs and Roaming 34

CHAPTER 4 Deployment 35

Configuration Files 35

Determine MAC Address 36

Cisco Unified Communications Manager Device Addition Methods 36

Autoregistration 37
Autoregistration and TAPS 37
Add Device in Cisco Unified Communications Manager 38
Add Device with Bulk Administration Tool Phone Template 38
Self-Provisioning 39
Enable Self-Provisioning 39
Cisco Unified Communications Manager User Addition 39
Add User Directly to Cisco Unified Communications Manager 40
Add User From External LDAP Directory 40
Identify Device Model 41
Configure Line Settings 41
Associate User with Device 42
Survivable Remote Site Telephony 43

CHAPTER 5 Installation 45
Install Cisco DX Series Device 45
Wireless LAN Setup 46
Wireless LAN Setup in Cisco Unified Communications Manager Administration 46
Provision Wireless LAN Profile 47
Provision Wireless LAN Profile Group 47
Network Settings Configuration 47
Configure IPv4 48
Renew IPv4 48
Configure IPv6 48
Renew IPv6 49
Configure Ethernet Web Proxy 49
Set Admin VLAN 49
Set SW Port Speed 50
Set PC Port Speed 50
Connect to Wi-Fi Network 50
Connect to Hidden Wi-Fi Network 51
Configure Wi-Fi Web Proxy 51
Configure Wi-Fi IP Settings 51
Set Wi-Fi Frequency Band 52
Mobile and Remote Access Through Expressway 52

Enable user Credential Persistence for Expressway 53
Convert a Device to Mobile and Remote Access through Expressway 53
Convert an Expressway Device to VPN 54
Convert an Off-Premise Device to On-Premise 54
Add Problem Report Tool Server to Expressway HTTP Allow List 54
Set the Allowed Authorization Request Rate 55
Enable Alternate TFTP Server 55
Set TFTP Server 1 55
Set TFTP Server 2 56
AnyConnect VPN 56
Add VPN Connection Profile 56
Connect to VPN 56
Optimize Video Call Experience Over VPN 57
Configure VPN in Cisco Unified Communications Manager 57
VPN Configuration Settings 58
VPN Authentication 60
Startup Process 60
Set TFTP Server Manually During Startup 62
Startup Verification 62

CHAPTER 6 **Contacts** 63
Contacts and Directories by Operating Mode 63
Local Contacts 64
Corporate Directory 64
Set Company Photo Directory 64
Contacts Search 65
Optimize Search Results 65
Application Dial Rules 65
Configure Application Dial Rules 66

CHAPTER 7 **Self Care Portal Management** 67
Self Care Portal Overview 67
Set Up Access to Self Care Portal 68
Customize Self Care Portal Display 68

CHAPTER 8 Accessories 69

Bluetooth Accessories 69

Bluetooth Device Profiles 69

Handsfree Profile 69

Phone Book Access Profile 70

Enable Device Profiles 70

Pair Bluetooth Accessory 71

Disable Bluetooth 71

Cable Lock 71

External Cameras 71

External Camera Settings 72

Perform External Camera Postinstallation Checks 72

External Speakers and Microphone 72

Headsets 72

Bluetooth Wireless Headsets 73

Add Bluetooth Wireless Headset 74

Remove Bluetooth Headset 74

USB Headsets 75

Enable USB Headset 75

Disable USB Headset 75

Wired Headsets 75

Connect to Wired Headset 75

Disable Wired Headset 75

Video Displays 76

Cisco DX650 Wall-Mount Kit 76

Before You Begin 76

Wall-Mount Components 77

Install Wall-Mount 77

CHAPTER 9 Security Features 83

Device Security 83

Overview of Security Features 83

Security Profiles 86

SE Android 86

Upgrades and SE Android 86
SE Android Troubleshooting 87
Diagnose SE Android Policy Issues 87
ADB Shell Limitations 87
SE Android Log Collection 87
Set Up Locally Significant Certificate 88
SHA-256 Manufacturing Installed Certificate 88
Secure Phone Calls 89
Secure Phone Call Identification 90
Secure Conference Call Identification 90
Call Security Interactions and Restrictions 90
Check Device Security Information Remotely 92
Encryption for Barge 92
802.1X Authentication Support 92
Required Network Components 92
Best Practices 93
Screen Lock and Automatic Lock Setup 93
Set Up Screen Unlock/Password Reset 94

CHAPTER 10 **Features and Services** 95
Available Telephony Features 95
Agent Greeting 96
Enable Agent Greeting 96
All Calls 96
All Calls on Primary Line 96
AutoAnswer 96
Auto Dial 97
Barge 97
Busy Lamp Field 97
Call Forward 97
Calling Line Identification 98
Calling Line Identification Presentation 98
Cisco Extension Mobility 98
Extension Mobility Multi-User 98
Set Up Cisco Extension Mobility 99

Cisco Mobility 100
Conference 100
Secure Conference 100
Divert 100
Do Not Disturb 101
Gateway Recording 101
Hold Status 101
Hold and Resume 101
Music on Hold 101
Ignore 101
Message Waiting Indicator 102
Mute 102
Plus Dialing 102
Protected Calling 102
Ringtone Setting 102
Ringtone 102
Secure and Nonsecure Indication Tone 103
Serviceability 103
Shared Line 103
Speed Dial 103
Transfer 104
Uniform Resource Identifier Dialing 104
Video Toggle 104
Voice Messaging System 104
Set Up Visual Voicemail 104
Set Up Visual Voicemail for Specific User or Group 105
Feature Buttons 105
Set Up Feature Control Policies 107
Feature Control Policy Default Values 107
Phone Button Templates 108
Modify Phone Button Templates 108
Configure Product-Specific Options 109
Video Transmit Resolution Setup 120
Instant Messaging and Presence Setup 121
Application Setup 122

Enable Cisco UCM App Client 122
Create End User to Log In to UCM App 122
Subscribe User with UCM App 123
Push Android APK Files Through Cisco Unified Communications Manager 123
Add Android Service in Cisco Unified Communications Manager Administration 124
Subscribe Device to Android Phone Service 124

CHAPTER 11 Customization 127
Wideband Codec Setup 127
Operating Modes 128
Set Operating Mode 128
Default Wallpaper 129
Assign Wallpaper Control 129
Specify Default Wallpaper (DX70 and DX80) 129
Specify Default Wallpaper (DX650) 130
SSH Access 130
Unified Communications Manager Endpoints Locale Installer 131
International Call Logging Support 131

CHAPTER 12 Maintenance 133
Reset Device 133
Reset Options and Load Upgrades 135
Remote Lock 135
Remote Lock Device 135
Remote Wipe 136
Remote Wipe Device 136
Boot Alternate Image for Cisco DX70 136
Boot Alternate Image for Cisco DX80 137
Boot Alternate Image for Cisco DX650 137
Data Migration 137
Debugging Log Profiles 137
Set Debugging Log Profile for Call Processing 138
Reset Debugging Log Profile to Default 138
User Support 138
Problem Report Tool 138

Configure Customer Support Upload URL 139
Take Screenshot From Web Browser 140
Take Screenshot From Device 140
Application Support 140

CHAPTER 13 Model Information Status and Statistics 141
Model Information 141
Device Status 142
Status Messages 143
Ethernet Statistics 147
WLAN Statistics 148
Audio Call Statistics 149

CHAPTER 14 Remote Monitoring 151
Enable and Disable Web Page Access 151
Access Device Web Page 152
Device Information 153
Network Setup 154
Security Information 159
Ethernet Statistics 161
WLAN Setup 163
Device Logs 165
Streaming Statistics 165

APPENDIX A Certificate Authority Trust List 171
Certificate Authority Trust List 171

Preface

- Overview, page xiii
- Guide Conventions, page xiii
- Related Documentation, page xiv
- Documentation, Support, and Security Guidelines, page xvi

Overview

This book provides the information you need to understand, install, configure, and manage Cisco DX Series devices on a network.

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

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 on other network devices.

Guide Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.

Convention	Description
[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 `screen` font.
input font	Information you must enter is in input font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	The symbol ^ represents the key labeled Control - for example, the key combination ^D in a 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

Cisco DX Series

All Cisco DX Series documentation is available at the following URL:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/tsd-products-support-series-home.html

User-oriented documents are available at the following URL:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-user-guide-list.html

Administrator-oriented documentation is available at the following URL:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html

The *Cisco DX Series Wireless LAN Deployment Guide* is available at the following URL:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-implementation-design-guides-list.html

Translated publications are available at the following URL:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/tsd-products-support-translated-end-user-guides-list.html

Open Source license information is available as the following URL:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-licensing-information-listing.html

Regulatory Compliance and Safety Information is available at the following URL:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-installation-guides-list.html

Cisco Unified Communications Manager

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

Cisco Business Edition 6000

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

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

Cisco and the Environment

Related publications are available at the following URL:

http://www.cisco.com/go/ptrdocs

Terminology Differences

The following table highlights some of the differences in terminology found in the Cisco DX Series user guides, the *Cisco DX Series Administration Guide*, and the *Cisco Unified Communications Manager Administration Guide*.

Table 1: Terminology Differences

User Guides	Administration Guides
Line Status	Busy Lamp Field (BLF)
Message Indicators	Message Waiting Indicator (MWI) or Message Waiting Lamp
Voicemail System	Voice Messaging System

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:

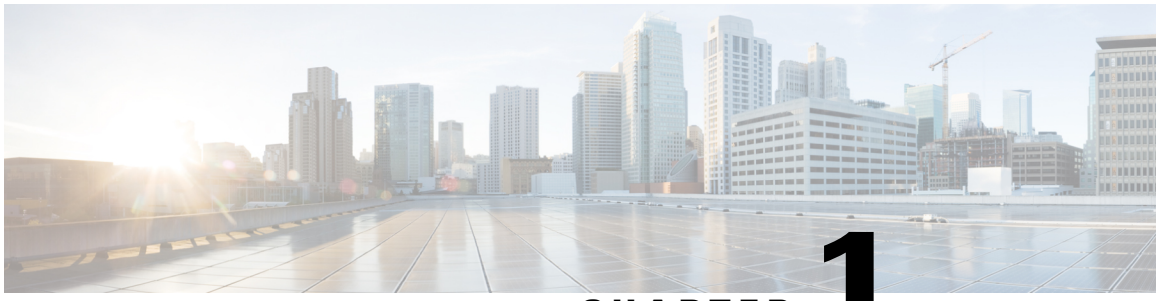
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

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.



CHAPTER 1

Technical Specifications

- Physical and Operating Environment Specifications, page 1
- Network and Computer Port Pinouts, page 2
- Network Protocols, page 5
- Power Requirements, page 9
- External Devices, page 13
- USB Port and USB Serial Console Data Information, page 13
- Behavior During Times of Network Congestion, page 15

Physical and Operating Environment Specifications

Table 2: Physical and Operating Specifications for Cisco DX Series Devices

Specification	Value or Range
Physical dimensions (H x W x D)	Cisco DX70: 14.84 in. (377.1 mm) x 13.91 in. (353.1 mm) x 2.45 in. (62.3 mm) Cisco DX80: 20.2 in. (51 2mm) x 22.2 in. (565 mm) x 3.5 in. (89 mm) Cisco DX650: 8.46 in. (215 mm) x 10.35 in. (263 mm) x 8.19 in. (208 mm)
Weight	Cisco DX70: 8.5 lb (3.9 kg) Cisco DX80: 15.65 lb (7.1 kg) Cisco DX650: 3.81 lb (1.73 kg)
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)

Specification	Value or Range
Power, Cisco DX70	Rated: 3.5A at 12V maximum Low Power Standby mode Integrated EnergyWise support
Power, Cisco DX80	Rated: 60 W maximum Low Power Standby mode Integrated EnergyWise support
Power, Cisco DX650	IEEE 802.3af (Class 3) or IEEE 802.3at (Class 4) Power over Ethernet (PoE) standards are supported. Compatible with both Cisco Discovery Protocol and Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) PoE switch blades. Power budget: 13.7W (Cisco Discovery Protocol) or 15.1W (LLDP) for 802.3AF and low-power USB peripheral support; greater than 15.4W and 802.3AT required for high-power USB peripheral support.
Connectivity	Internal 2-port Cisco Ethernet switch IEEE 802.11 a/b/g/n Wi-Fi
Audio codec support	Narrowband audio compression codecs: G.711a, G.711u, G.729a, G.729ab, and Internet Low Bitrate Codec (iLBC) Wideband audio compression codecs: G.722, Internet Speech Audio Codec (iSAC), iLBC, and AAC-LD audio compression codecs.
Operating System	Android™ 4.1.1 (Jellybean)
Processor	Cisco DX70: TI OMAP 4470 1.5GHz dual-core ARM Cortex-A9 processor Cisco DX80: TI OMAP 4470 1.5GHz dual-core ARM Cortex-A9 processor Cisco DX650: TI OMAP 4460 1.5-GHz dual-core ARM Cortex-A9 processor
Memory	2-GB RAM; Low Power Double Data Rate Synchronous Dynamic Random-Access Memory (LPDDR2 SDRAM)
Storage	8-GB eMMC NAND Flash memory (embedded multimedia card; nonvolatile)

Network and Computer Port Pinouts

Cisco DX Series devices include network and computer (access) ports, which are used for network connectivity. They serve different purposes and have different port pinouts.

- The network port is the 10/100/1000 SW port.
- The computer (access) port is the 10/100/1000 PC port.

Network Port Connector Pinouts

Table 3: 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-
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 Pinouts

Table 4: 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-

Pin Number	Function
7	BI_DC+
8	BI_DC-

Note BI stands for *bidirectional*, while DA, DB, DC and DD stand for *Data A*, *Data B*, *Data C* and *Data D*, respectively.

Ports Used by Cisco DX Series Devices

The following table describes the ports that Cisco DX Series devices use. For additional information, see the *TCP and UDP Port Usage Guide for Cisco Unified Communications Manager*.

Table 5: Cisco DX Series Device Ports

Source Port	Remote Device Port	Underlying Protocol	Protocol/Service	Notes
68	67	-	DHCP client	DHCP support to obtain dynamic IP addresses
49152-53248	53	UDP	DNS client	DNS support for name resolution
49152-53248	69	UDP	TFTP client	TFTP support is required to obtain various configuration and image files from a central server.
49152-53248	80	TCP/UDP	HTTP client	
80	Server configured	TCP/UDP	HTTP server	
123	123	UDP	NTP client	Network Time Protocol to obtain time-of-day
49152-53248	Server configured	TCP	HTTP client	
49152-53248	6970	TCP	TFTP client	TFTP support is required to obtain various configuration and image files from a central server.
49152-53248	5060	TCP	SIP/TCP	Default is 5060; administrator can change.
49152-53248	5061	TCP	SIP/TLS	Default is 5061; administrator can change.

Source Port	Remote Device Port	Underlying Protocol	Protocol/Service	Notes
16384- 32767	Receiver Range	UDP	RTP	Administrator can configure port range.
16384- 32767	Receiver Range	UDP	RTCP	RTCP port is RTP +1.
4224	PC Dynamic Range	TCP		
22	Server configured	TCP	Secure shell	
4051		TCP		Load upgrades
4052		RDP		Load upgrades
4061				Special debugs
8443				Contacts search

Network Protocols

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

Table 6: Supported Network Protocols

Network Protocol	Purpose	Usage Notes
Binary Floor Control Protocol (BFCP)	BFCP allows users to share a presentation within an ongoing video conversation.	BFCP is automatically enabled.
Bluetooth	Bluetooth is a wireless personal area network (WPAN) protocol that specifies how devices communicate over short distances.	The devices support Bluetooth 3.0. The devices support Hands-Free Profile (HFP), Advanced Audio Distribution (A2DP) Profile, Human Interface Device Profile (HID), Object Push Profile (OPP), and Phone Book Access Profile (PBAP).
Bootstrap Protocol (BootP)	BootP enables a network device to discover certain startup information, such as the IP address.	—

Network Protocol	Purpose	Usage Notes
Cisco Discovery Protocol (CDP)	CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment. Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.	The device uses CDP to communicate information, such as auxiliary VLAN ID, per-port power management details, and Quality of Service (QoS) configuration information, with the Cisco Catalyst switch.
Cisco Peer-to-Peer Distribution Protocol (CPPDP)	CPPDP is a Cisco proprietary protocol that is used to form a peer-to-peer hierarchy of devices. This hierarchy is used to distribute firmware files from peer devices to their neighboring devices.	The Peer Firmware Sharing feature uses CPPDP.
Dynamic Host Configuration Protocol (DHCP)	DHCP dynamically allocates and assigns an IP address to network devices. DHCP enables you to connect a device into the network and for that device to become operational without the need to manually assign an IP address or to configure additional network parameters.	DHCP is enabled by default. If it is disabled, you must manually configure the IP address, subnet mask, gateway, and a TFTP server on each device locally. Cisco recommends that you use DHCP custom option 150. With this method, you configure the TFTP server IP address as the option value. For additional supported DHCP configurations, see the "Dynamic Host Configuration Protocol" chapter and the "Cisco TFTP" chapter in the *Cisco Unified Communications Manager System Guide*. **Note** If you cannot use option 150, you may try using DHCP option 66.
Hypertext Transfer Protocol (HTTP)	HTTP is the standard way of transferring information and moving documents across the Internet and the web.	Devices use HTTP for XML services and for troubleshooting purposes.
Hypertext Transfer Protocol Secure (HTTPS)	Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of servers.	Web applications with both HTTP and HTTPS support have two URLs configured. Devices that support HTTPS choose the HTTPS URL.

Network Protocol	Purpose	Usage Notes
IEEE 802.1X	The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication succeeds, normal traffic can pass through the port.	Devices implement the IEEE 802.1X standard by providing support for the following authentication methods: EAP-FAST and EAP-TLS. When 802.1X authentication is enabled on the device, you should disable the PC port and voice VLAN.
IEEE 802.11a/b/g/n	The IEEE 802.11 standard specifies how devices communication over a wireless local area network (WLAN). 802.11a operates at the 5 GHz band, and 802.11b and 802.11g operate at the 2.4 GHz band. 802.11.n operates in either 2.4 GHz or 5Ghz band.	The 802.11 interface is a deployment option for cases when Ethernet cabling is unavailable or undesirable.
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets across the network.	To communicate using IP, network devices must have an assigned IP address, domain name, gateway, and netmask. IP addresses, subnets, and gateway identifications are automatically assigned if you are using the device with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each device locally. The device supports IPv6 addresses. For more information, see the *Features and Services Guide for Cisco Unified Communications Manager*, "Internet Protocol Version 6 (IPv6)" chapter.
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 device supports LLDP on the PC port.

Network Protocol	Purpose	Usage Notes
Link Layer Discovery Protocol - Media Endpoint Devices (LLDP-MED)	LLDP-MED is an extension of the LLDP standard for voice products.	The device supports LLDP-MED on the SW port to communicate information such as: • Voice VLAN configuration • Device discovery • Power management • Inventory management For more information about LLDP-MED support, see the LLDP-MED and Cisco Discovery Protocol white paper: http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml
Real-Time Transport Protocol (RTP)	RTP is a standard protocol for transporting real-time data, such as interactive voice and video, over data networks.	The device uses the RTP protocol to send and receive real-time voice traffic from other phones and gateways.
Real-Time Control Protocol (RTCP)	RTCP works in conjunction with RTP to provide QoS data (such as jitter, latency, and round-trip delay) on RTP streams. RTCP is also used to synchronize the audio and video stream in order to provide a better video experience.	RTCP for audio calls is disabled by default. RTCP for video calls (including both audio streams and video streams in the video call) is enabled by default. You can enable or disable RTCP on individual devices from Cisco Unified Communications Manager Administration.
Session Description Protocol (SDP)	SDP is the portion of the SIP protocol that determines which parameters are available during a connection between two endpoints. Conferences are established by using only the SDP capabilities that all endpoints in the conference support.	SDP capabilities, such as codec types, DTMF detection, and comfort noise, are normally configured on a global basis by Cisco Unified Communications Manager or Media Gateway in operation. Some SIP endpoints may allow configuration of these parameters on the endpoint itself.

Network Protocol	Purpose	Usage Notes
Session Initiation Protocol (SIP)	SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP is an ASCII-based application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints.	Like other VoIP protocols, SIP addresses the functions of signaling and session management within a packet telephony network. Signaling allows transportation of call information across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.
Telepresence Interoperability Protocol (TIP)/Multiplex (MUX)	TIP/MUX is an IP protocol that is used to negotiate audio and video media options between endpoints prior to reception or transmission of media.	TIP/MUX is invoked for multiparticipant conferences and enables content sharing.
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	The device uses TCP to connect to Cisco Unified Communications Manager and to access XML services.
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	Upon security implementation, the device uses the TLS protocol when securely registering with Cisco Unified Communications Manager.
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network. On the device, TFTP enables you to obtain a configuration file specific to the device type.	TFTP requires a TFTP server in your network that the DHCP server can automatically identify. If you want a device to use a TFTP server other than the one that the DHCP server specifies, you must manually assign the IP address of the TFTP server by using the Settings application on the device. For more information, see the "Cisco TFTP" chapter in the *Cisco Unified Communications Manager System Guide*.
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data packets.	UDP is used only for RTP streams. SIP signaling on the devices does not support UDP.

Power Requirements

Cisco DX Series devices are powered with external power. A separate power supply provides external power.

Cisco DX650 can also be powered with Power over Ethernet (PoE). The switch can provide PoE through an Ethernet cable.

Note When you install a device 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 device. When you remove a device that is powered with external power, disconnect the Ethernet cable from the device before you disconnect the power supply.

Power Guidelines

To power the Cisco DX70 and the Cisco DX80, use the provided Lite-On PA-1600-2A-LF power supply or FSP075-DMAA1. To power the Cisco DX650, see the table below.

Table 7: Guidelines for Cisco DX650 Power

Power Type	Guidelines
External power: Provided through the CP-PWR-CUBE-4= external power supply	The device uses the CP-PWR-CUBE-4 power supply. **Note** You must use the CP-PWR-CUBE-4 when you deploy the device on a wireless network.
External power—Provided through the Cisco Unified IP Phone Power Injector	The Cisco Unified IP Phone Power Injector may be used with any Cisco DX650. Functioning as a midspan device, the injector delivers inline power to the attached phone. The Cisco Unified IP Phone Power Injector connects between a switch port and the phone, and supports a maximum cable length of 100m between the unpowered switch and the phone.
PoE power—Provided by a switch through the Ethernet cable that is attached to the phone	Cisco DX650 supports IEEE 802.3af Class 3 power on signal pairs and spare pairs. These devices support IEEE 802.3at for external add-on devices. To ensure uninterruptible operation of the phone, make sure that the switch has a backup power supply. Make sure that the CatOS or IOS version that runs on your switch supports your intended phone deployment. See the documentation for your switch for operating system version information. Support for NG-PoE+: The devices can draw more power than IEEE 802.3at, as long as there is NG-PoE+ switch support.

Power Reduction

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

Power Save Mode

In Power Save mode, the backlight on the screen is not lit when the device is not in use. The device remains in Power Save mode for the scheduled duration or until the user lifts the handset or presses any button. In the Product Specific Configuration area of the **Phone Configuration** window on Cisco Unified Communications Manager, configure the following parameters:

Days Display Not Active

Specifies the days that the backlight remains inactive.

Display on Time

Schedules the time of day that the backlight automatically activates.

Display on Duration

Indicates the length of time that the backlight is active after the backlight is enabled by the programmed schedule.

EnergyWise Mode

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

Set up each device to enable or disable the EnergyWise settings. If EnergyWise is enabled, configure a sleep and wake time, as well as other parameters. These parameters are sent to the device as part of the configuration XML file. In the **Phone Configuration** window in Cisco Unified Communications Manager, configure the following parameters:

Enable Power Save Plus

Selects the schedule of days for which the device powers down.

Phone On Time

Determines when the device automatically turns on for the days that are selected in the **Enable Power Save Plus** field.

Phone Off Time

Determines the time of day that the device powers down for the days that are selected in the **Enable Power Save Plus** field.

Phone Off Idle Timeout

Determines the length of time that the device must be idle before it powers down.

Enable Audio Alert

When enabled, instructs the device to play an audible alert that starts 10 minutes before the time that the **Phone Off Time** field specifies.

EnergyWise Domain

Specifies the EnergyWise domain that the device is in.

EnergyWise Secret

Specifies the security secret password that is used to communicate within the EnergyWise domain.

Allow EnergyWise Overrides

Determines whether you allow the EnergyWise domain controller policy to send power-level updates to the devices.

When a device is sleeping, the power sourcing equipment (PSE) provides minimal power to the device to illuminate the **Power/Lock** button, and the **Power/Lock** button can be used to wake up the device when it is sleeping.

Power Negotiation Over LLDP

The device and the switch negotiate the power that the device consumes. Devices operate at multiple power settings, which lowers power consumption when less power is available.

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

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

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

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

Additional Information About Power

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

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

Document Topic	URL
Cisco Unified IP Phones Power Injector	http://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-power-injector/index.html

Document Topic	URL
PoE Solutions	http://www.cisco.com/c/en/us/solutions/enterprise-networks/power-over-ethernet-solutions/index.html
Cisco Catalyst Switches	http://www.cisco.com/cisco/web/psa/default.html?mode=prod http://www.cisco.com/c/en/us/products/switches/index.html
Integrated Service Routers	http://www.cisco.com/c/en/us/products/routers/index.html
Cisco IOS Software	http://www.cisco.com/c/en/us/products/ios-nx-os-software/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].

USB Port and USB Serial Console Data Information

Cisco DX Series devices include USB ports, and sometimes a micro-USB port. The devices support connection of a maximum of ten accessories to the USB ports. Each accessory that connects to the devices is included in the maximum count. Supported accessories include USB serial cable, USB mouse, USB keyboard, USB-powered hub, and USB memory stick.

Note Because all USB hubs need to be powered, keyboards that include one or more hubs are not allowed on these devices, because they contain a nonpowered hub.

You can also use a USB connection for Android Debug Bridge (ADB) access. Use the micro-USB ports on Cisco DX650, and Cisco DX70, and the USB type B port on Cisco DX80 for ADB access. For more information about using ADB, see http://developer.android.com/index.html.

The USB Serial Console allows a USB port to be used as a console, thus eliminating the need for a serial port. The following table shows the settings for the USB console.

Table 8: USB Console Settings

Parameter	Setting
Baud rate	115200
Data	8 bit
Parity	none
Stop	1 bit
Flow control	none

Note Because the device comes preloaded with drivers, Cisco supports only a limited number of cable types. Cisco recommends use of the IOGEAR USB-serial adapter.

Use USB Console

The USB console cable has a USB interface on one end and a serial interface on the other. The USB interface may be plugged in to any of the USB ports on the device. The serial interface connects to the serial port on the PC.

For Cisco DX650, use either the side or rear USB type A port. For Cisco DX70 and Cisco DX80 use the micro-USB port.

Tip If you do not have a serial port on your PC/laptop, two USB console cables can be connected back to back, with a null modem cable between them.

Procedure

Step 1 In Cisco Unified Communications Manager, set credentials on the device page.

Step 2 Enable USB debugging in the Product Specific Configuration Layout portion of the window.

Step 3 Connect a USB serial cable to the device. The device console output appears on your terminal screen.

Step 4 After output stops, tap **Return** to sign in.

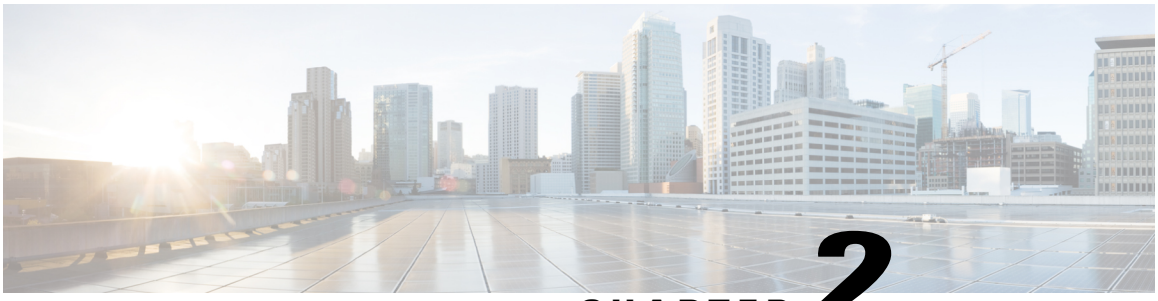
Step 5 After $ prompt screen, you can use tools such as debugsh to diagnose problems.

Behavior During Times of Network Congestion

Anything that degrades network performance can affect 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

To reduce or eliminate any adverse effects, schedule administrative network tasks during a time when the devices are not being used or exclude the devices from testing.

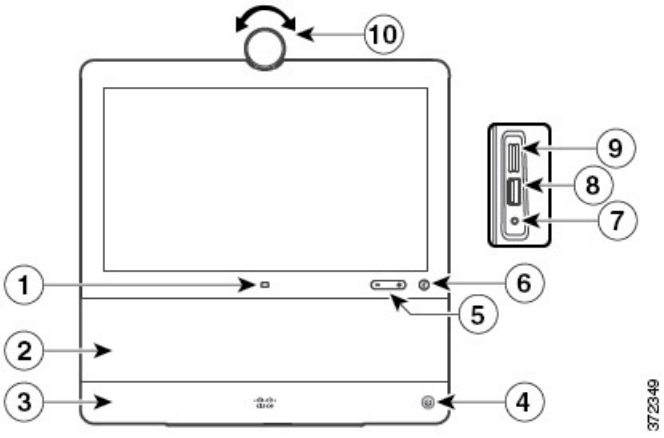


CHAPTER 2

Device Descriptions

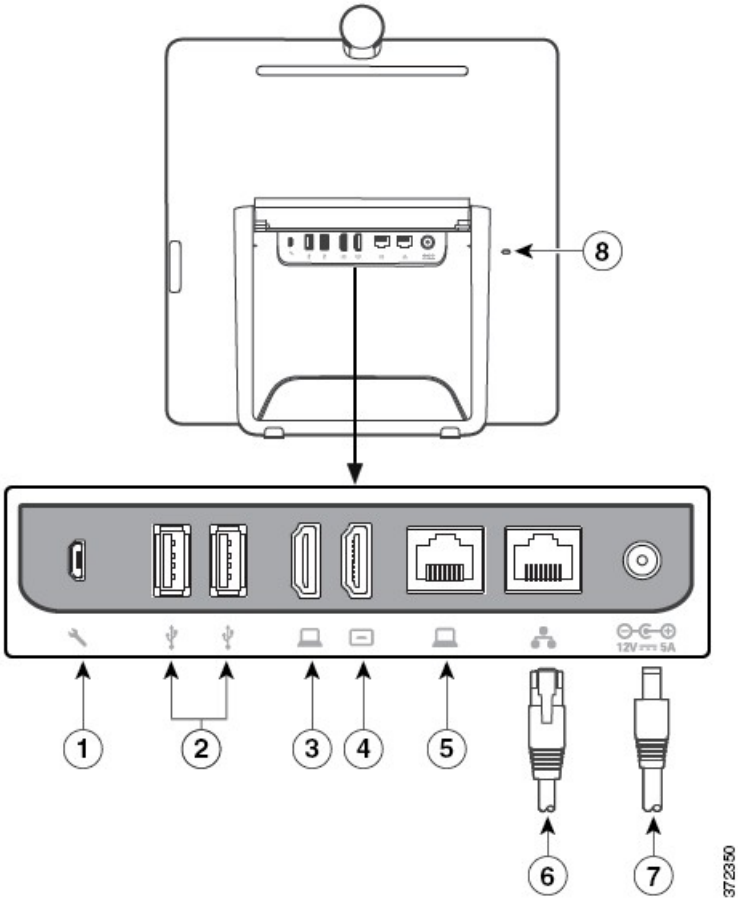
- Cisco DX70 Hardware, page 17
- Cisco DX80 Hardware, page 19
- Cisco DX650 Hardware, page 21
- No Radio Hardware, page 22

Cisco DX70 Hardware



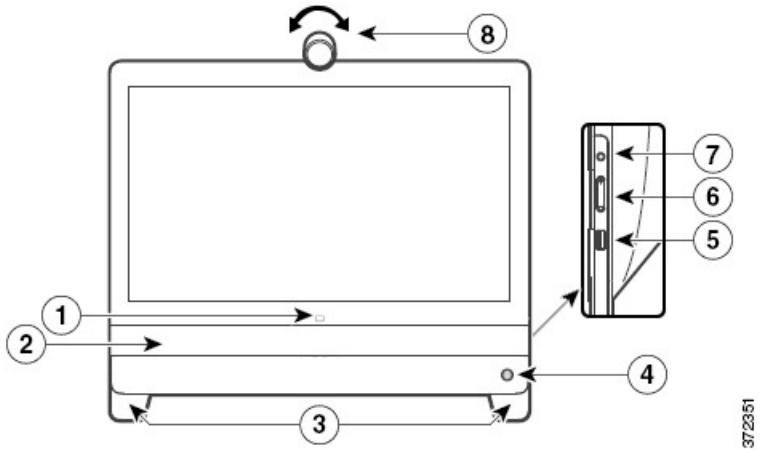
1	Source button	6	Mute button
2	Speaker	7	Mini jack 3.5 mm output
3	Microphone	8	USB charging port
4	Power button	9	microSD card slot
5	Volume button	10	Camera with privacy shutter

Cisco DX70 Cable Installation



1	micro-B USB port	5	Computer port
2	USB ports	6	Network port
3	HDMI in	7	Power port
4	HDMI out		

Cisco DX80 Hardware

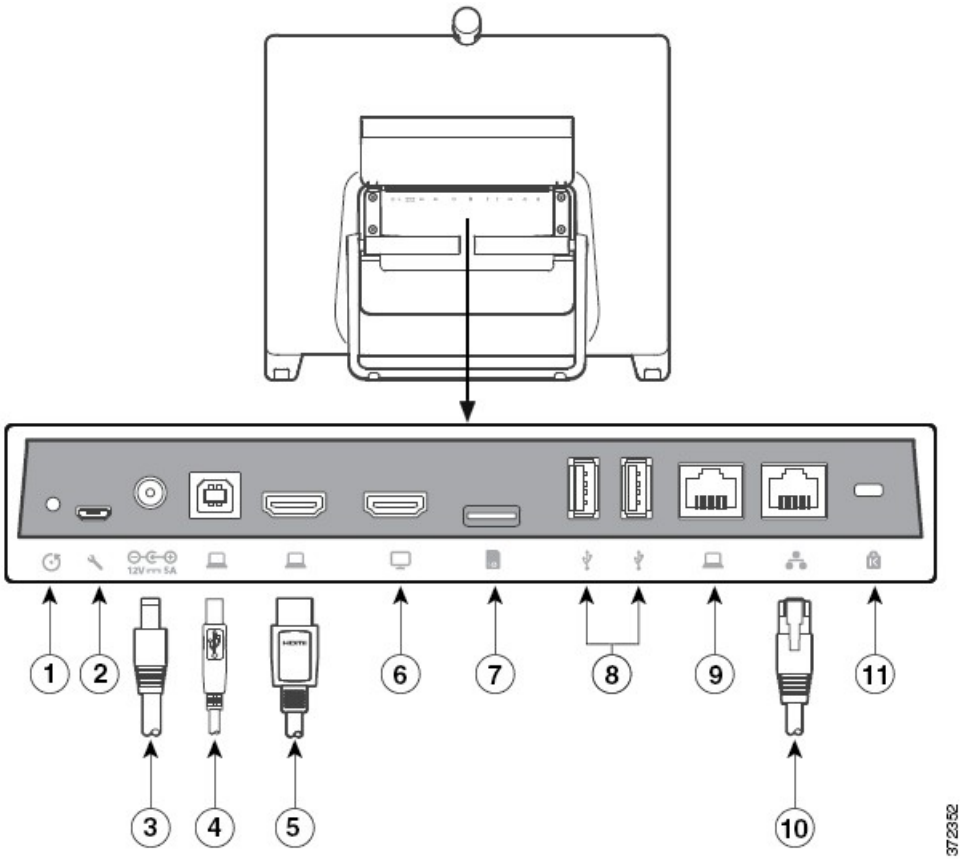


1	Source button	5	USB port
2	Speaker	6	Volume button
3	Microphones in each leg	7	Mute button
4	Power button	8	Camera with privacy shutter

Cisco DX80 includes an Acoustic Echo Canceller (AEC) and laptop shadowing. Users at the far end of a call experience clear audio quality even if the user puts an obstacle, such as a laptop, in front of one of the microphones. If the current microphone is blocked by an object, the device automatically switches to the other microphone array in the other foot.

Cisco DX80 also includes two microphone array beam forming. If the user moves out of the beam (that is, out of the camera view), the sound sent to the far end weakens. All sound sources that are not located within the pickup beam (in front of the unit) attenuate.

Cisco DX80 Cable Installation

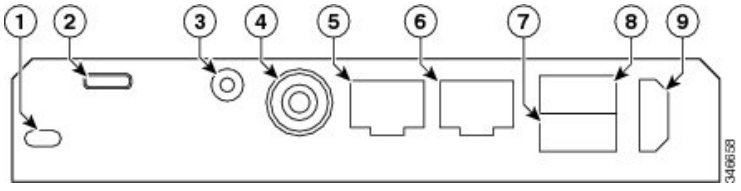


1	Factory reset pinhole	7	microSD card slot
2	micro-B USB port	8	USB ports
3	Power port	9	Computer port
4	USB type B port	10	Network port
5	HDMI in	11	Kensington Security Slot (K-Slot)
6	HDMI out		

Cisco DX650 Hardware

1	Privacy shutter slide switch	10	Conference button
2	Camera	11	Transfer button
3	Touchscreen	12	Volume button
4	12 key dial pad	13	Speaker button
5	Micro Secure Digital Standard Capacity (HDSC) slot	14	Stop Video button
6	Lock button	15	Headset button
7	USB port	16	Mute button
8	End call button	17	Handset with light strip
9	Hold button		

Cisco DX650 Cable Installation

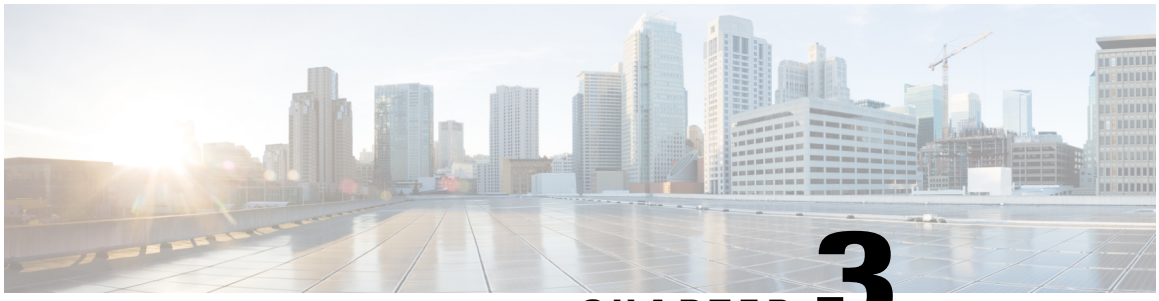


1	Kensington Security Slot (K-Slot)	6	Computer port

2	micro-B USB port	7	Auxiliary port
3	3.5-mm stereo line in/out jack	8	USB 2.0 port
4	Power port	9	HDMI type A port
5	Network port		

No Radio Hardware

The No Radio (NR) hardware versions of Cisco DX70 and Cisco DX80 do not support Wi-Fi or Bluetooth features.



CHAPTER 3

Wi-Fi Network Setup

- Network Requirements, page 23
- Wireless LAN, page 24
- Wi-Fi Network Components, page 25
- 802.11 Standards for WLAN Communications, page 28
- Security for Communications in WLANs, page 31
- WLANs and Roaming, page 34

Network Requirements

For the device to successfully operate as an endpoint in your network, your network must meet the following requirements:

- VoIP Network
  - 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.
- IP network that supports DHCP or manual assignment of IP address, gateway, and subnet mask

Note The device displays the date and time from Cisco Unified Communications Manager. If the user unchecks **Automatic Date & time** in the Settings application, the time may become out of sync with the server time.

- Wireless LAN
  - Access Points (APs) are configured to support voice and video over WLAN.
  - Controllers and switches are configured to support voice and video.
  - Security is implemented for authenticating wireless voice devices and users.

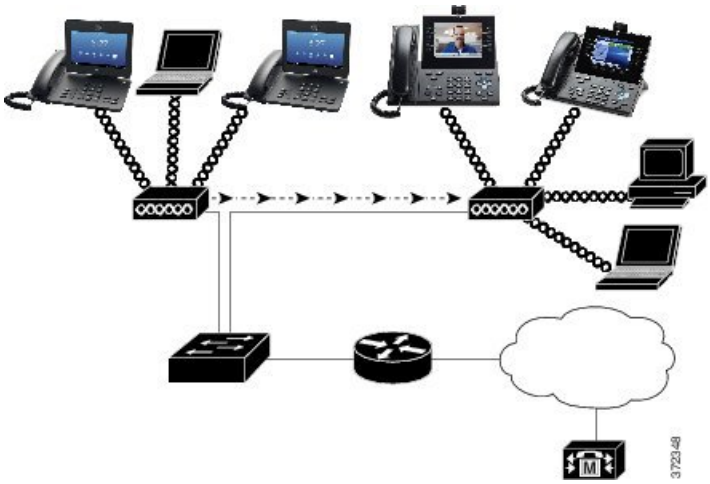
Wireless LAN

Note For instructions on deploying and configuring a wireless Cisco DX Series device, see the *Cisco DX Series Wireless LAN Deployment Guide*.

Devices with wireless capability can provide voice communication within the corporate WLAN. The device depends on and interacts with wireless access points (AP) and key Cisco IP Telephony components, including Cisco Unified Communications Manager Administration, to provide wireless voice communication.

Cisco DX Series devices exhibit Wi-Fi capabilities that can use 802.11a, 802.11b, 802.11g, and 802.11n Wi-Fi.

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



When a Cisco DX Series device powers on, it searches for and associates with an AP if the device wireless access is set to On. If remembered networks are not within range, you can select a broadcasted network or manually add a network.

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

APs are critical components in a WLAN because they provide the wireless links or hot spots to the network. In some WLANs, each AP has a wired connection to an Ethernet switch, such as a Cisco Catalyst 3750, that is configured on a LAN. The switch provides access to gateways and the Cisco Unified Communications Manager server to support wireless IP telephony.

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

For more information about Cisco Unified Wireless Networks, see http://www.cisco.com/c/en/us/products/wireless/index.html.

Wi-Fi Network Components

The device must interact with several network components in the WLAN to successfully place and receive calls.

AP Channel and Domain Relationships

Access points (APs) transmit and receive RF signals over channels within the 2.4 GHz or 5 GHz frequency band. To provide a stable wireless environment and reduce channel interference, you must specify nonoverlapping channels for each AP.

For more information about AP channel and domain relationships, see the "Designing the Wireless LAN for Voice" section in the *Cisco DX Series Wireless LAN Deployment Guide*.

AP Interactions

Cisco DX Series devices use the same APs as wireless data devices. However, voice traffic over a WLAN requires different equipment configurations and layouts than a WLAN that is used exclusively for data traffic. Data transmission can tolerate a higher level of RF noise, packet loss, and channel contention than voice transmission. Packet loss during voice transmission can cause choppy or broken audio and can make the call inaudible. Packet errors can also cause blocky or frozen video.

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

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

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

Note Packet loss occurs during roaming; however, the security mode and the presence of fast roaming determines how many packets are lost during transmission. Cisco recommends implementation of Cisco Centralized Key Management (CCKM) to enable fast roaming.

For more information about Voice QoS in a wireless network, see the *Cisco DX Series Wireless LAN Deployment Guide*.

Access Point Association

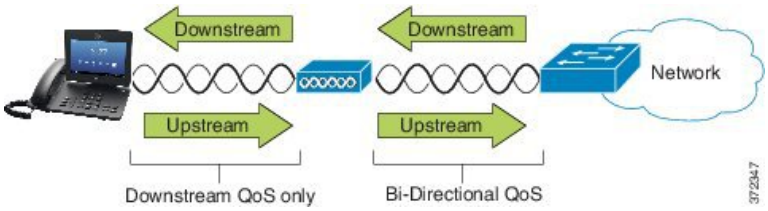
At startup, the device scans for APs with SSIDs and encryption types that it recognizes. The device builds and maintains a list of eligible APs and selects the best AP based on the current configuration.

QoS in Wireless Network

Voice and video traffic on the wireless LAN, like data traffic, is susceptible to delay, jitter, and packet loss. These issues do not impact the data end user, but can seriously impact a voice or video call. To ensure that voice and video traffic receives timely and reliable treatment with low delay and low jitter, you must use Quality of Service (QoS).

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

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



The Enhanced Distributed Coordination Function (EDCF) type of QoS has up to eight queues for downstream (toward the 802.11b/g clients) QoS. You can allocate the queues based on these options:

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

Although up to eight queues on the AP can be set up, you should use only three queues for voice, video, and signaling traffic to ensure the best possible QoS. Place voice in the Voice queue (UP6), video in the Video queue (UP5), signaling (SIP) traffic in the Video queue (UP4), and place data traffic in a best-effort queue (UP0). Although 802.11b/g EDCF does not guarantee that voice traffic is protected from data traffic, you should get the best statistical results by using this queuing model.

The queues are:

- Best Effort (BE) - 0, 3
- Background (BK) - 1, 2
- Video (VI) - 4, 5
- Voice (VO) - 6, 7

Note The device marks the SIP signaling packets with a DSCP value of 24 (CS3) and RTP packets with DSCP value of 46 (EF).

Note Call Control (SIP) is sent as UP4 (VI). Video is sent as UP5 (VI) when Admission Control Mandatory (ACM) is disabled for video (Traffic Specification [TSpec] disabled). Voice is sent as UP6 (VO) when ACM is disabled for voice (TSpec disabled).

The following table provides a QoS profile on the AP that gives priority to voice, video, and call control (SIP) traffic.

Table 9: QoS Profile and Interface Settings

Traffic Type	DSCP	802.1p	WMM UP	Port Range
Voice	EF (46)	5	6	UDP 16384-32767
Interactive Video	AF41 (34)	4	5	UDP 16384-32767
Call Control	CS3 (24)	3	4	TCP 5060-5061

To improve reliability of voice transmissions in a nondeterministic environment, the device supports the IEEE 802.11e industry standard and is Wi-Fi Multimedia (WMM) capable. WMM enables differentiated services for voice, video, best effort data and other traffic. For these differentiated services to provide sufficient QoS for voice packets, only a certain amount of voice bandwidth can be serviced or admitted on a channel at one time. If the network can handle “N” voice calls with reserved bandwidth, when the amount of voice traffic is increased beyond this limit (to N+1 calls), the quality of all calls suffers.

To help address issues with call quality, an initial Call Admission Control (CAC) scheme is required. With SIP CAC enabled on the WLAN, QoS is maintained in a network overload scenario by limiting the number of active voice calls so as not to exceed the configured limits on the AP. During times of network congestion, the system maintains a small bandwidth reserve so wireless device clients can roam into a neighboring AP, even when the AP is at “full capacity.” After the voice bandwidth limit is reached, the next call is load-balanced to a neighboring AP so as not to affect the quality of the existing calls on the channel.

Note Cisco DX Series devices use TCP for SIP communications, and Cisco Unified Communications Manager registrations can potentially be lost if an AP is at full capacity. Frames to or from a client that has not been "authorized" through the CAC can be dropped, leading to Cisco Unified Communications Manager deregistration. Therefore, Cisco recommends that you disable SIP CAC.

Note The DSCP, COS, and WMM UP markings correctly display for the optimum transmission of video frames. The device does not support Voice and Video CAC; Cisco recommends that you implement SOP CAC.

The devices use the Flexible DSCP and Video Promotion feature to resolve inconsistent QoS and inconsistent bandwidth accounting when a video occurs with a different type of device.

Set Up Flexible DSCP

Procedure

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

Step 2 In Clusterwide Parameters (System - Location and Region), set Use Video BandwidthPool for Immersive Video Calls to **False**.

Step 3 In Clusterwide Parameters (Call Admission Control), set Video Call QoS Marking Policy to **Promote to Immersive**.

Step 4 Save your changes.

Cisco Unified Communications Manager Interaction

Cisco Unified Communications Manager manages the components of the IP telephony system (the endpoints, access gateways, and the resources) for such features as call conferencing and route planning.

Cisco DX Series devices are supported by Cisco Unified Communications Manager Release 8.5(1), 8.6(2), 9.1(2), 10.5(1) and later.

Cisco Unified Communications Manager cannot recognize a device until the device is registered and configured in the database.

You can find more information about configuring Cisco Unified Communications Manager to work with IP devices in the *Cisco Unified Communications Manager Administration Guide*, the *Cisco Unified Communications Manager System Guide*, and the *Cisco DX Series Wireless LAN Deployment Guide*.

802.11 Standards for WLAN Communications

Wireless LANs must follow the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards that define the protocols that govern all Ethernet-based wireless traffic. Cisco DX Series devices support the following standards:

- 802.11a: Uses the 5 GHz band that provides more channels and improved data rates by using OFDM technology. Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) support this standard.
- 802.11b: Specifies the radio frequency (RF) of 2.4 Ghz for both transmission and receipt of data at lower data rates (1, 2, 5.5, 11 Mbps).
- 802.11d: Enables access points to advertise their currently supported radio channels and transmit power levels. The 802.11d-enabled client then uses that information to determine the channels and powers to use. The device requires World mode (802.11d) to determine which channels are legally allowed for any given country. For supported channels, see the table that follows. Ensure that 802.11d is properly configured on the Cisco IOS Access Points or Cisco Unified Wireless LAN Controller.

- 802.11e: Defines a set of Quality of Service (QoS) enhancements for wireless LAN applications.
- 802.11g: Uses the same unlicensed 2.4 Ghz band as 802.11b, but extends the data rates to provide greater performance by using Orthogonal Frequency Division Multiplexing (OFDM) technology. OFDM is a physical-layer encoding technology for transmission of signals through use of RF.
- 802.11h: 5 GHz spectrum and transmit power management. Provides DFS and TPC to the 802.11a Media Access Control (MAC).
- 802.11i: Specifies security mechanisms for wireless networks.
- 802.11n: Uses the radio frequency of 2.4 GHz or 5 GHz for both transmission and receipt of data, and enhances data transfer through the use of multiple input, multiple output (MIMO) technology, channel bonding, and payload optimization.

Note Cisco DX Series devices have a single antenna and use the Single Input Single Output (SISO) system, which supports MCS 0 to MCS 7 data rates only (72 Mbps with 20 MHz channels and 150 Mbps 40 MHz channels). Optionally, you can enable MCS 8 to MCS 15 if 802.11n clients are using MIMO technology that can take advantage of those higher data rates.

Table 10: Supported Channels for Cisco DX Series Devices

Band Range	Available Channels	Channel Set
2.412 - 2.472 GHz	13	1 - 13
5.180 - 5.240 GHz	4	36, 40, 44, 48
5.260 - 5.320 GHz	4	52, 56, 60, 64
5. 500 - 5.700 GHz	11	100 - 140
5.745 - 5.825 GHz	5	149, 153, 157, 161, 165

Note Channels 120, 124, 128 are not supported in the Americas, Europe, or Japan, but may be in other regions around the world.

For information about supported data rates, Tx power and Rx sensitivity for WLANs, see the *Cisco DX Series Wireless LAN Deployment Guide*.

World Mode (802.11d)

Cisco DX Series devices use 802.11d to determine the channels and transmit power levels to use. The device inherits its client configuration from the associated AP. Enable World mode (802.11d) on the AP to use the

device in World mode. For more information on enabling World mode, see the *Cisco DX Series Wireless LAN Deployment Guide*

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

Because all countries support these frequencies, you can attempt to scan these channels regardless of World mode (802.11d) support. For the countries that support 2.4GHz, see the *Cisco DX Series Wireless LAN Deployment Guide*.

Enable World mode (802.11d) for the corresponding country where the access point is located. World mode is enabled automatically for the Cisco Unified Wireless LAN Controller.

Wireless Modulation Technologies

Wireless communications use the following modulation technologies for signaling:

Direct-Sequence Spread Spectrum (DSSS)

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

Orthogonal Frequency Division Multiplexing (OFDM)

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

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

Table 11: Data Rates, Number of Channels, and Modulation Technologies by IEEE Standard

Item	802.11b	802.11g	802.11a	802.11n
Data rates	1, 2, 5.5, 11 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	• 20 MHz Channels: 7 - 72 Mbps • 40 MHz Channels: 15 - 150 Mbps
Nonoverlapping channels	3	3	Up to 24	Up to 24

Item	802.11b	802.11g	802.11a	802.11n
Wireless modulation	DSSS	OFDM	OFDM	OFDM

Radio Frequency Ranges

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

- 2.4 GHz: Many devices that use 2.4 GHz can potentially interfere with the 802.11b/g connection. Interference can produce a Denial of Service (DoS) scenario, which may prevent successful 802.11 transmissions.
- 5 GHz: This range divides into several sections called Unlicensed National Information Infrastructure (UNII) bands, each of which has four channels. The channels are spaced at 20 MHz to provide nonoverlapping channels and more channels than 2.4 GHz provides.

Security for Communications in WLANs

Because all WLAN devices that are within range can receive all other WLAN traffic, security of voice communications is critical in WLANs. To ensure that intruders do not manipulate or intercept voice traffic, the Cisco SAFE Security Architecture supports Cisco DX Series devices and Cisco Aironet APs. For more information about security in networks, see http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html.

Authentication Methods

The Cisco Wireless IP Telephony solution provides wireless network security that prevents unauthorized sign-ins and compromised communications through use of the following authentication methods that Cisco DX Series devices support:

WLAN Authentication

- WPA (802.1x authentication + TKIP or AES encryption)
- WPA2 (802.1x authentication + AES or TKIP encryption)
- WPA-PSK (Pre-Shared key + TKIP encryption)
- WPA2-PSK (Pre-Shared key + AES encryption)
- EAP-FAST (Extensible Authentication Protocol – Flexible Authentication via Secure Tunneling)
- EAP-TLS (Extensible Authentication Protocol – Transport Layer Security)
- PEAP (Protected Extensible Authentication Protocol) MS-CHAPv2 and GTC
- CCKM (Cisco Centralized Key Management)
- Open

WLAN Encryption

- AES (Advanced Encryption Scheme)
- TKIP / MIC (Temporal Key Integrity Protocol / Message Integrity Check)
- WEP (Wired Equivalent Protocol) 40/64 and 104/128 bit

Note Dynamic WEP with 802.1x authentication and Shared Key authentication are not supported.

For more information about authentication methods, see the "Wireless Security" section in the *Cisco DX Series Wireless LAN Deployment Guide*.

Authenticated Key Management

The following authentication schemes use the RADIUS server to manage authentication keys:

- WPA/WPA2: Uses RADIUS server information to generate unique keys for authentication. Because these keys are generated at the centralized RADIUS server, WPA/WPA2 provides more security than WPA pre-shared keys that are stored on the AP and device.
- Cisco Centralized Key Management (CCKM): Uses RADIUS server and a wireless domain server (WDS) information to manage and authenticate keys. The WDS creates a cache of security credentials for CCKM-enabled client devices for fast and secure reauthentication.

With WPA/WPA2 and CCKM, encryption keys are not entered on the device, but are automatically derived between the AP and device. But the EAP username and password that are used for authentication must be entered on each device.

Encryption Methods

To ensure that voice traffic is secure, Cisco DX Series devices support WEP, TKIP, and Advanced Encryption Standards (AES) for encryption. When these mechanisms are used for encryption, voice Real-Time Transport Protocol (RTP) packets are encrypted between the AP and the device.

WEP

When WEP is used in the wireless network, authentication happens at the AP through open or shared-key authentication. The WEP key that is set up on the device must match the WEP key that is configured at the AP for successful connections. The devices support WEP keys that use 40-bit encryption or a 128-bit encryption and remain static on the device and AP.

TKIP

WPA and CCKM use TKIP encryption, which has several improvements over WEP. TKIP provides per-packet key ciphering and longer initialization vectors (IVs) that strengthen encryption. In addition, a message integrity check (MIC) ensures that encrypted packets are not altered. TKIP removes the predictability of WEP that helps intruders decipher the WEP key.

AES

An encryption method used for WPA2 authentication. This national standard for encryption uses a symmetrical algorithm that has the same key for encryption and decryption.

For more information about encryption methods, see the “Wireless Security” section in the *Cisco DX Series Wireless LAN Deployment Guide*.

AP Authentication and Encryption Options

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

Note

- When you use WPA pre-shared key or WPA2 pre-shared key, the pre-shared key must be statically set on the device. These keys must match the keys that are on the AP.
- Cisco DX Series devices do not support auto EAP negotiation; to use EAP-FAST mode, you must specify it.

The following table provides a list of authentication and encryption schemes that are configured on the Cisco Aironet APs that the devices support. The table shows the network configuration option for the device that corresponds to the AP configuration.

Table 12: Authentication and Encryption Schemes

Cisco WLAN Configuration			**Cisco DX Series Configuration**
Authentication	Key management	Common encryption	Authentication
Open	None	None	None
Static WEP	None	WEP	WEP
EAP-FAST	WPA or WPA2 with optional CCKM	TKIP or AES	802.1x EAP > EAP-FAST
PEAP-MSCHAPv2	WPA or WPA2 with optional CCKM	TKIP or AES	802.1x EAP > PEAP > MSCHAPV2
PEAP-GTC	WPA or WPA2 with optional CCKM	TKIP or AES	802.1x EAP > PEAP > GTC
EAP-TLS	WPA or WPA2 with optional CCKM	TKIP or AES	802.1x EAP > TLS

Cisco WLAN Configuration			Cisco DX Series Configuration
WPA/WPA2-PSK	WPA-PSK or WPA2-PSK	TKIP or AES	WPA/WPA2 PSK

For additional information about Cisco WLAN Security, see http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1200-access-point/prod_brochure09186a00801f7d0b.html.

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

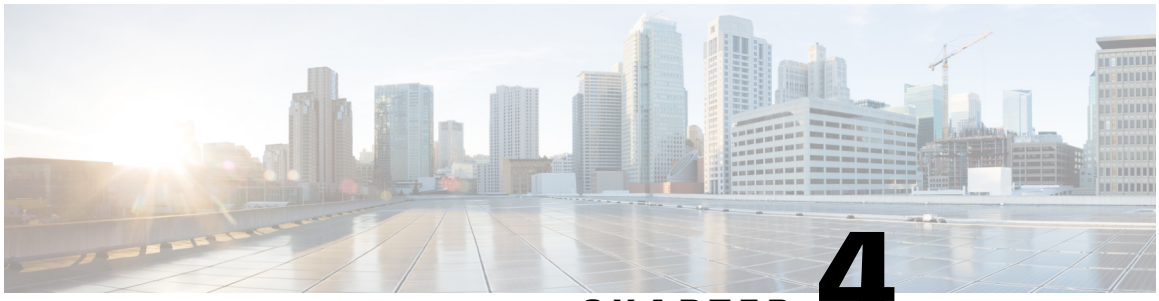
http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=278875243

WLANs and Roaming

Cisco DX Series devices support Cisco Centralized Key Management (CCKM), a centralized key management protocol that provides a cache of session credentials on the wireless domain server (WDS).

For details about CCKM, see the *Cisco Fast Secure Roaming Application Note* at:

http://www.cisco.com/en/US/products/hw/wireless/ps4570/prod_technical_reference09186a00801c5223.html



CHAPTER 4

Deployment

- Configuration Files, page 35
- Determine MAC Address, page 36
- Cisco Unified Communications Manager Device Addition Methods, page 36
- Cisco Unified Communications Manager User Addition, page 39
- Identify Device Model, page 41
- Configure Line Settings, page 41
- Associate User with Device, page 42
- Survivable Remote Site Telephony, page 43

Configuration Files

The TFTP server stores the device configuration files that define parameters for connection to Cisco Unified Communications Manager. In general, any time you make a change in Cisco Unified communications Manager that requires the device to be reset, a change is automatically made to the configuration file.

Configuration files also contain information about the image load that the device should be running. If this image load differs from the one that is currently loaded on a device, the device contacts the TFTP server to request the required load files. Due to the size of the image loads it is mandatory that TCP port 6970 be open between the device and the TFTP server.

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

- You enable autoregistration in Cisco Unified Communications Manager.
- You have not added the device to the Cisco Unified Communications Manager database.
- The device registers for the first time.

Note If the device security mode in the configuration file is set to Authenticated or Encrypted, but the device has not received a CTL or ITL file, the device makes four attempts to obtain the file so the device can register securely.

If autoregistration is not enabled and the device has not been added to the Cisco Unified Communications Manager database, the registration request will be rejected. The device displays `Out of service` on the screen.

Cisco DX Series devices access the configuration file, SEPmac_address.cnf.xml, where mac_address is the Ethernet MAC address of the device. The device will instead access the configuration file named SEPmac_address.cnf.xml.sgn if a CTL or ITL file is installed. The **Description** field in the **Phone Configuration** window of Cisco Unified Communications Manager Administration is prepopulated when the device is first configured. The MAC address identifies the device uniquely.

Determine MAC Address

You can determine the MAC address of a device in these ways:

- From the device, tap **Applications** > **Settings** > **About device** > **Status** and look at the **Ethernet MAC Address** field.
- Look at the MAC label on the back of the device.
- Display the web page for the device and click the **Device Information** hyperlink.

Cisco Unified Communications Manager Device Addition Methods

Before you install the device, you must choose a method for addition of endpoints to the Cisco Unified Communications Manager database.

The following table provides an overview of the methods for addition of devices to the Cisco Unified Communications Manager database.

Table 13: Methods for Adding Devices to the Cisco Unified Communications Manager

Method	Requires MAC Address?	Notes
Autoregistration	No	Results in automatic assignment of directory numbers.
Autoregistration with Tool for Autoregistered Phones Support (TAPS)	No	Requires autoregistration and the Bulk Administration Tool; updates information in the device and in Cisco Unified Communications Manager Administration.
Cisco Unified Communications Manager Administration	Yes	Requires devices to be added individually.

Method	Requires MAC Address?	Notes
Cisco Unified Communications Manager Bulk Administration Tool	Yes	Allows for simultaneous registration of multiple devices.
Self-Provisioning	No	Allows the user to provision their own device.

Autoregistration

By enabling autoregistration before you begin to install devices, you can:

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

Note Cisco recommends that you use autoregistration to add fewer than 100 devices to your network. To add more than 100 devices to your network, use the Bulk Administration Tool.

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 device, or if you want to use a secure connection with Cisco Unified Communications Manager as described in the *Cisco Unified Communications Manager Security Guide*. For information about enabling autoregistration, see the "Autoregistration Setup" section in the *Cisco Unified Communications Manager Security Guide*.

Autoregistration and TAPS

You can add devices with autoregistration and TAPS, the Tool for Autoregistered Phones Support, without prior collection of MAC addresses from devices.

TAPS works with the Bulk Administration Tool to update a batch of devices 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.

Note Cisco recommends that you use autoregistration and TAPS to add fewer than 100 devices to your network. To add more than 100 devices to your network, use the Bulk Administration Tool.

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

Autoregistration must be enabled in Cisco Unified Communications Manager Administration (**System** > **Cisco Unified CM**) for TAPS to function.

Note 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.

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

Add Device in Cisco Unified Communications Manager

You can add devices individually to the Cisco Unified Communications Manager database. To do so, you first must obtain the MAC address for each device.

Procedure

Step 1 After you collect MAC addresses, in Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 2 Click **Add New**.

Step 3 Choose the device type from the **Phone Type** drop-down list box.

Note Depending on the Cisco Unified Communications Manager version, when you add Cisco DX Series devices, you may need to install a Device Enabler before you install the firmware.

Step 4 Click **Next**.

Step 5 Enter the details of device-specific parameters (Device Pool, Device Security Profile, and so on).

Step 6 Click **Save**.
For more information, go to the "System Configuration Overview" chapter in the *Cisco Unified Communications Manager System Guide*.

Add Device with Bulk Administration Tool Phone Template

The Cisco Unified Communications Manager Bulk Administration Tool enables you to perform batch operations, such as registration of multiple devices.

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

Procedure

Step 1 Obtain the MAC address for each device.
Step 2 From Cisco Unified Communications Manager, choose **Bulk Administration** > **Phones** > **Phone Template**.
Step 3 Click **Add New**.
Step 4 Choose a Phone Type and select **Next**.
Step 5 Enter the details of device-specific parameters, such as Device Pool and Device Security Profile.
Step 6 Click **Save**.
Step 7 From Cisco Unified Communications Manager Administration, choose **Device** > **Phone** > **Add New** to add a device by using an existing Bulk Administration Tool template.

Self-Provisioning

Self-provisioning allows the user to set up their device with less administrator effort. When self-provisioning is enabled, the user enters their credentials during the device setup. The device MAC address and other configuration information is shared with the Cisco Unified Communications Manager server.

Self-provisioning requires Cisco Unified Communications Manager Release 10.0 or later. For more information, see the "Self-Provisioning" chapter of the *Cisco Unified Communications Manager Administration Guide*.

Enable Self-Provisioning

Procedure

Step 1 In Cisco Unified Communications Manager Administration, go to **User Management** > **User Setting** > **User Profile**.
Step 2 Set Self-provisioning to **Enabled**.
Step 3 Go to **User Management** > **End User**.
Step 4 Set the Self-Service User ID.
Step 5 Go to **User Management** > **Self Provisioning** and choose an authentication mode.

Cisco Unified Communications Manager User Addition

This section describes steps for adding a user to Cisco Unified Communications Manager. Follow one of the procedures in this section, depending on your operating system and the manner in which you are adding the user.

Add User Directly to Cisco Unified Communications Manager

If you are not using an LDAP directory, you can add a user directly to Cisco Unified Communications Manager.

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

Procedure

Step 1 Choose **User Management** > **End User**, then click **Add New**.
The **End User Configuration** window appears.

Step 2 In the User Information pane of this window, enter the following:

- User ID - Enter the end user identification name. Cisco Unified Communications Manager does not permit modification of the user ID after it is created. You may use the following special characters: =, +, <, >, #, ;, \," ", and blank spaces.
- 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.
- Telephone Number - Enter the primary directory number for the end user. End users can have multiple lines on their devices.

Step 3 Click **Save**.

Step 4 Proceed to Identify Device Model, on page 41.

Add User From External LDAP Directory

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

Procedure

Step 1 Sign in to Cisco Unified Communications Manager Administration.

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

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

Step 4 Click on the LDAP directory name.

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

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

Step 6 Proceed to Identify Device Model, on page 41.

Identify Device Model

Procedure

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

Step 2 Click **Add New**.

Step 3 Choose the device model from the **Phone Type** drop-down list, and then click **Next**.
The **Phone Configuration** window appears.

Step 4 Proceed to Configure Line Settings, on page 41.

Configure Line Settings

In the **Phone Configuration** window, you can use the default values for most of the fields.

Procedure

Step 1 On the **Phone Configuration** window, click **Line 1** on the left pane of the window. The **Directory Number Configuration** window appears.

Step 2 In the **Directory Number** field, enter the same number that appears in the **Telephone Number** field in the **User Configuration** window.

Step 3 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.

Step 4 From the **Calling Search Space** drop-down list (Directory Number Settings pane of the **Directory Number Configuration** window), choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that are called from this directory number. The value that you choose applies to all devices that use this directory number.

Step 5 In the **Call Forward Settings** pane of the **Directory Number Configuration** window, 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 be forwarded to the voice mail for this line, check the **Voice Mail** box in the Call Forward Settings pane.

Step 6 In the **Line 1** field in the Device pane of the **Directory Number Configuration** window, configure the following:

a) Display (**Internal Caller ID** field): You can enter the first name and last name of the user of this device so that this name will be displayed for all internal calls. You can also leave this field blank to have the system display the phone extension.

b) 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 number 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 555902XXXX, an external call from extension 6640 displays a caller ID number of 5559026640.

c) Click **Save**.

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

Step 7 Click **Associate End Users** at the bottom of the window to associate a user to the line that you are configuring.

a) Use the **Find** button in conjunction with the **Search** fields to locate the user.

b) Check the box next to the username, then choose **Add Selected**.
The username and user ID appear in the Users Associated With Line pane of the **Directory Number Configuration** window.

c) Click **Save**.
The user is now associated with Line 1 on the device.

Step 8 If the device has a second line, configure Line 2.

Step 9 Proceed to Associate User with Device, on page 42.

Associate User with Device

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, choose the link for the user.

Step 4 Choose **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.

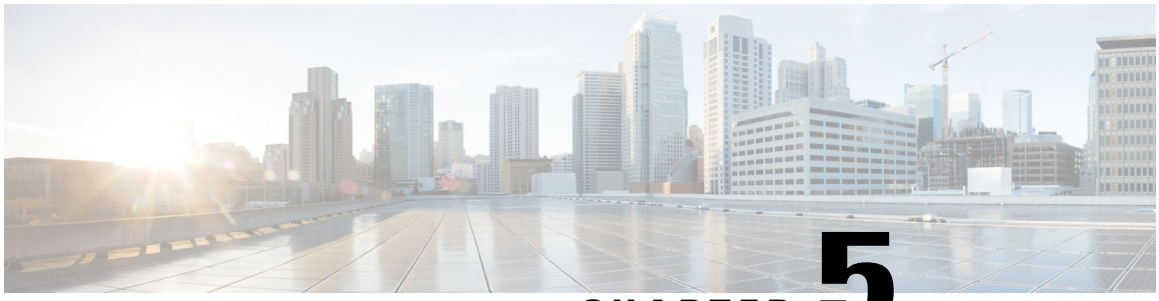
Step 8 From the **Related Links** drop-down list, choose **Back to User**, and click **Go**.
The **End User Configuration** window appears and the associated devices that you chose display in the Controlled Devices pane.

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

Survivable Remote Site Telephony

Survivable Remote Site Telephony (SRST) ensures that basic call functions remain accessible when communications with the controlling Cisco Unified Communications Manager are broken. In this scenario, the device can keep an in-progress call active, and the user can access a subset of the features available. When failover occurs, the user receives an alert message on the device. SRST requires Cisco IOS version 12.4(20) or above.

Note SRST does not support IPv6.



CHAPTER 5

Installation

- Install Cisco DX Series Device, page 45
- Wireless LAN Setup, page 46
- Network Settings Configuration, page 47
- Startup Process, page 60
- Startup Verification, page 62

Install Cisco DX Series Device

After you add devices to the Cisco Unified Communications Manager database, you can complete the device installation. You (or the users) can install the device at the user location.

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

http://software.cisco.com/download/release.html?mdfid=284721679&flowid=46173&softwareid=282074288

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

If you used autoregistration, you need to update the specific configuration information for the device, such as associate the device with a user, or change the directory number.

The following steps provide an overview and checklist of installation tasks for Cisco DX Series devices. The steps present a suggested order to guide you through the device installation. Some tasks are optional, depending on your system and user needs.

Procedure

Step 1 Choose the power source.

- External power supply
- [Cisco DX650-only] Power over Ethernet (PoE)

  Note With PoE+ 802.3at, accessories that are plugged in to the device, such as mouse or keyboard, negotiate for power. If not enough power is available for the accessory, an error message appears on the screen. The device requires an external power supply when it is used in a WLAN environment.

Step 2 Assemble the device and connect the network cable. If you use the device in a WLAN environment, see Step 5.
This step locates and installs the device in the network.

Step 3 Monitor the device startup process. This step adds primary and secondary directory numbers and features that are associated with directory numbers to the device, and verifies that the device is configured properly.

Step 4 If you choose to deploy the device on a wireless network, skip to Step 5.
If you are configuring the Ethernet network settings on the device for an IP network, you can set up an IP address for the device either by use of DHCP or by manual entry of an IP address.

Step 5 If you choose to deploy the device on the wireless network, you must perform the following:

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

Note The wireless LAN on the device does not activate when Ethernet cables are connected on the device.

Step 6 Make calls with the device to verify that the Call application and features work correctly.

Step 7 Provide information to end users about how to use and configure their devices.

Wireless LAN Setup

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

For complete wireless network configuration information, see the *Cisco DX Series Wireless LAN Deployment Guide*.

Wireless LAN Setup in Cisco Unified Communications Manager Administration

In Cisco Unified Communications Manager, you must enable a parameter called “Wi-Fi” for the device. You can enable this parameter in one of the following locations in Cisco Unified Communications Manager Administration:

- To enable wireless LAN on a specific device, choose **Enable** for the Wi-Fi parameter in the Product Specific Configuration Layout section (**Device** > **Phone**) for the specific device, and check **Override Common Settings**.

- To enable wireless LAN for a group of devices, choose **Enable** for the Wi-Fi parameter in a **Common Phone Profile Configuration** window (**Device** > **Device Settings** > **Common Phone Profile**), check **Override Common Settings**, then associate the device (**Device** > **Phone**) with that common phone profile.
- To enable wireless LAN for all WLAN-capable devices in your network, choose **Enable** for the Wi-Fi parameter in the **Enterprise Phone Configuration** window (**System** > **Enterprise Phone Configuration**), and check **Override Common Settings**.

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

Provision Wireless LAN Profile

Procedure

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

Step 2 Configure the Wireless LAN profile and click **Save**.

Provision Wireless LAN Profile Group

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Phone** > **Wireless LAN Profile Group**.

Step 2 Configure the Wireless LAN Profile Group and click **Save**.

Step 3 Choose **System** > **Device Pool** then add the Wireless LAN profile group to a device pool and click **Save**. Or, choose **Device** > **Phone** then add the Wireless LAN profile group to a specific device and click **Save**.

Network Settings Configuration

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

- IP address
- IP subnet information

- IPv6 addresses
- TFTP server IP address

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

Configure IPv4

Procedure

Step 1 In the Settings application, tap **Ethernet** > **IPv4 configuration**.

Step 2 Check **Use static IP**.

Step 3 Set the following options:

- IP address
- Gateway
- Netmask
- Domain name

  Note You can use option 15 to send multiple domain names to the device. Each domain name needs to be delimited by a space. Any other delimiter, such as a comma, is not supported. The domain names can also be entered manually if you are using a static IP address. Again, the space is the only valid delimiter. Currently, option 119 is not supported.

- DNS 1
- DNS 2

Renew IPv4

Procedure

In the Settings application, tap **Ethernet** > **Renew IPv4**.

Configure IPv6

Procedure

Step 1 In the Settings application, tap **Ethernet** > **IPv6 configuration**.

Step 2 Check **Use static IP**.

Step 3 Set the following options:

- IP address
- Default router
- Prefix length
- Domain name

  Note You can use option 15 to send multiple domain names to the device. Each domain name needs to be delimited by a space. Any other delimiter, such as a comma, is not supported. The domain names can also be entered manually if you are using a static IP address. Again, the space is the only valid delimiter. Currently, option 119 is not supported.

- DNS 1
- DNS 2

Renew IPv6

Procedure

In the Settings application, tap **Ethernet** > **Renew IPv6**.

Configure Ethernet Web Proxy

Procedure

Step 1 In the Settings application, tap **Ethernet** > **Proxy settings**.

Step 2 Choose the proxy setting type.

a) To set a manual proxy, enter the proxy hostname, proxy port, and any proxy bypasses. Check **Proxy requires authentication** if applicable.

b) To set an auto proxy, enter the PAC location, and any proxy bypasses. Check **Proxy requires authentication** if applicable.

Set Admin VLAN

Procedure

Step 1 In the Settings application, tap **Ethernet** > **Admin VLAN**.

Step 2 Enter an Admin VLAN ID value and tap **OK**.

Set SW Port Speed

Procedure

Step 1 In the Settings application, tap **Ethernet** > **SW port speed**.

Step 2 Select a port speed.
If the device is connected to a switch, configure the port on the switch to the same speed/duplex as the device, or configure both to autonegotiate. If you change the setting of this option, you must change the PC port speed to the same setting.

Set PC Port Speed

Procedure

Step 1 In the Settings application, tap **Ethernet** > **PC port speed**.

Step 2 Select a port speed.
If the device is connected to a switch, configure the port on the switch to the same speed/duplex as the device, or configure both to autonegotiate. If you change the setting of this option, you must change the SW port speed to the same setting.

Connect to Wi-Fi Network

Procedure

Step 1 In the Settings application, toggle **Wi-Fi** on.

Step 2 Tap **Wi-Fi**.

Step 3 Select a wireless network from the list of available networks.

Step 4 Enter the credentials and tap **Connect**.

Connect to Hidden Wi-Fi Network

Procedure

Step 1 In the Settings application, toggle **Wi-Fi** on.
Step 2 Tap **Wi-Fi**.
Step 3 Tap +.
Step 4 Enter the Network SSID, select the security type and credentials (if applicable).
Step 5 Tap **Save**.

Configure Wi-Fi Web Proxy

Procedure

Step 1 In the Settings application, tap **Wi-Fi**.
Step 2 Tap and hold a wireless network from the list of available networks.
Step 3 Tap **Modify network**.
Step 4 Check **Show advanced options**.
Step 5 Choose the proxy setting type.
a) To set a manual proxy, enter the proxy hostname, proxy port, and any proxy bypasses. Check **Proxy requires authentication** if applicable.
b) To set an auto proxy, enter the PAC location, and any proxy bypasses. Check **Proxy requires authentication** if applicable.
Step 6 Tap **Save**.

Configure Wi-Fi IP Settings

Procedure

Step 1 In the Settings application, tap **Wi-Fi**.
Step 2 Tap and hold a wireless network from the list of available networks.
Step 3 Tap **Modify network**.
Step 4 Check **Show advanced options**.
Step 5 Choose the IP settings type, and configure the following:

- IP address

- Gateway
- Network prefix length
- DNS 1
- DNS 2
- Domain name

Step 6 Tap **Save**.

Set Wi-Fi Frequency Band

Procedure

Step 1 In the Settings application, tap **Wi-Fi**.

Step 2 Tap **...**

Step 3 Tap **Wi-Fi frequency band** and choose a setting.

Mobile and Remote Access Through Expressway

Mobile and Remote Access through Expressway requires Cisco Expressway 8.6 or later and Cisco Unified Communications Manager 10.5.2 SU2 or Cisco Unified Communications Manager 11.0 or later.

Cisco Expressway provides a way for remote workers to easily and securely connect their Cisco DX Series devices into the corporate network without using a virtual private network (VPN) client tunnel. Expressway uses Transport Layer Security (TLS) to secure network traffic. For a DX Series device to authenticate an Expressway certificate and establish a TLS session, the Expressway certificate must be signed by a public Certificate Authority that is trusted by the DX Series firmware. It is not possible to install or trust other CA certificates on DX Series devices for authenticating an Expressway certificate. See Certificate Authority Trust List, on page 171 for the list of supported CA certificates.

To ensure that the users are able to use the Problem Report Tool, you must add the Problem Report Tool server address to the Expressway HTTP server allow list

When logging in to Expressway, the user is prompted for a Service Name, User ID, and Password. On first boot, off-premise users are prompted to log in to Expressway by the Setup Assistant. For devices that have previously been deployed, either on-premise or off-premise, you must convert the device to use Expressway.

With the **User Credentials Persistent for Expressway Sign In** parameter set in the Product Specific Options on Cisco Unified Communications Manager, the device stores a user's login credentials so that users do not need re-enter this information. User credentials stored on the device are encrypted.

For more information, see *Unified Communications Mobile and Remote Access via Cisco Expressway Deployment Guide*.

Mobile and Remote Access Limitations and Restrictions

- DX Series devices connected through Expressway cannot access web browsing, or email services hosted inside the enterprise network.
- The Off Hook/KPML Dialing, Mobility, DND, Call Back, and drop conference participants features are only supported with Expressway 8.6 and later.
- Busy Line Field features require Cisco Unified Communications Manager 11.0 or later.
- A device connected through Expressway cannot download APKs from an APK server inside the enterprise network. The device can download APKs from an APK server on a public network as long as the host is accessible.
- You do not have SSH access to the device from the corporate network.
- You do not have access to the device web page from the corporate network.
- Self-provisioning is not supported through Expressway.

Related Topics

http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html

Enable user Credential Persistence for Expressway

Procedure

Step 1 Go to the Product Specific Configuration Layout area of the individual device configuration window or **Common Phone Profile** window.

Step 2 Set **User Credentials Persistent for Expressway Sign In** to On.

Convert a Device to Mobile and Remote Access through Expressway

Before You Begin

The device must have firmware 10.2(4) or later.

Procedure

Step 1 In the Settings application, tap **More...**.

Step 2 Tap **Reset network settings**.

Step 3 Uncheck **Enable automatic local telephony discovery** and tap **Reset**.

The network connection is reset. If the device is connected to a wired network, it will reconnect automatically. If the device is deployed wirelessly, you need to connect to a Wi-Fi network. When the device connects to a network, the **Enter TFTP server** screen displays.

Step 4 Tap **Expressway**.

Step 5 Fill in the **Service domain**, **Username**, and **Password** fields.

Step 6 Tap **Sign in**.

Convert an Expressway Device to VPN

Procedure

Step 1 In the Settings application, tap **More...**.

Step 2 Tap **Reset network settings**.

Step 3 Connect to a network.

Step 4 Enter TFTP server settings.

Step 5 Add a VPN profile and connect to it.

Convert an Off-Premise Device to On-Premise

Procedure

Connect a device to an enterprise network.
The enterprise network is detected, and the phone registers with Cisco Unified Communications Manager as it would normally.

Add Problem Report Tool Server to Expressway HTTP Allow List

Procedure

Step 1 On Expressway, go to **Configuration** > **Unified Communications** > **Configuration**.

Step 2 Click **HTTP server allow list**.

Step 3 Configure the hostname or IP address of the Problem Report Tool HTTP server.

Set the Allowed Authorization Request Rate

The rate of Mobile and Remote Access authorizations for a device is controlled by default. The default setting is 3 authorizations in 300 seconds. You may want to increase that rate if your Expressway server is issuing HTTP 429 “Too Many Requests” errors.

Procedure

Step 1 On Expressway, go to **Configuration** > **Unified Communications** > **Configuration** > **Advanced**.

Step 2 Set the **Authorization Rate Control**.

Enable Alternate TFTP Server

Procedure

Step 1 In the Settings application, tap **More**.

Step 2 Tap **TFTP Server Settings**.

Step 3 Check **Use Alternate TFTP Server**.

Set TFTP Server 1

Procedure

Step 1 In the Settings application, tap **More**.

Step 2 Tap **TFTP Server Settings**.

Step 3 Check **Use Alternate TFTP Server**.

Step 4 Tap **TFTP server 1**.

Step 5 Enter the TFTP server address and tap **OK**.

Set TFTP Server 2

Procedure

Step 1 In the Settings application, tap **More**.
Step 2 Tap **TFTP Server Settings**.
Step 3 Check **Use Alternate TFTP Server**.
Step 4 Tap **TFTP server 2**.
Step 5 Enter the TFTP server address and tap **OK**.

AnyConnect VPN

AnyConnect is a VPN client that provides remote users with secure VPN connections to the Cisco 5500 Series ASA running ASA Version 8.0, and later (with AnyConnect Mobile License) or Adaptive Security Device Manager (ASDM) 6.0 and later.

For more information about ASA, see http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

Add VPN Connection Profile

Procedure

Step 1 In the Settings application, tap **More**.
Step 2 Tap **VPN**.
Step 3 Tap **Add VPN profile**.
Step 4 Enter a description and the server address.
Step 5 Tap **Save**.

Connect to VPN

Procedure

Step 1 In the Settings application, tap **More**.
Step 2 Tap **VPN**.
Step 3 Tap and hold a VPN connection.
Step 4 If necessary, do either of the following in response to the appropriate prompts:

- Enter the credentials. If prompted to do so, also enter the secondary credentials to support double authentication.
- Tap **Get Certificate**, then enter the certificate enrollment credentials that your system administrator supplies. AnyConnect saves the certificate and reconnects to the VPN secure gateway to use the certificate for authentication.

Step 5 Tap **Connect**.

Optimize Video Call Experience Over VPN

Adjust video bandwidth settings to optimize the video call experience over VPN. A bandwidth of 1.5 Mbps is required for 720p video resolution. Lower bandwidth settings result in lower video resolution.

Note Throughput varies over time, due to factors like other traffic being shared on the network, or even time of day. These variations can affect the video experience.

Procedure

Step 1 Disconnect from VPN.

Step 2 Run a speed test for the device, and make a note of the upload speed in the test results.
Speed test applications, such as Internet Speed Test by Speed A.I. are available from Google Play.

Step 3 Reconnect to VPN.

Step 4 In the Call application, tap .

Step 5 Tap **Settings**.

Step 6 Tap **Video bandwidth**.

Step 7 Select a video bandwidth that is lower than the upload speed in the speed test results.

Configure VPN in Cisco Unified Communications Manager

The VPN Settings menu allows you to use the Secure Sockets Layer (SSL) to enable the VPN Client connection. Use the VPN connection when the device is located outside a trusted network or when network traffic between the device and Cisco Unified Communications Manager must cross untrusted networks.

Follow these steps from to configure VPN profiles. For more information, see the *Cisco Unified Communications Manager Security Guide* and the *Cisco Unified Communications Operating System Administration Guide*.

Procedure

Step 1 Set up VPN concentrators for each VPN gateway.

Step 2 Upload VPN certificates to a new Phone-VPN-Trust.

Step 3 Configure VPN gateways.

a) Choose **Advanced Features** > **VPN** > **VPN Gateway**.

b) Enter Gateway Name, Description, and URL.

Note You can assign up to ten certificates to a VPN Gateway. Assign at least one certificate to each gateway. Only certificates that are associated with the VPN role display in the available VPN certificates list.

The VPN Gateway URL is for the main concentrator in the gateway.

Step 4 Configure VPN Group. Choose **Advanced Features** > **VPN** > **VPN Group**.

Note You can add up to three VPN gateways to a VPN group. The total number of certificates in the VPN group cannot exceed ten.

Step 5 Configure VPN Profile. Choose **Advanced Features** > **VPN** > **VPN Profile**.

Note If **Enable Auto-Detect Network Connection** is enabled, the VPN client runs only if it detects that it is out of the corporate network.

If **Host ID Check** is enabled, the VPN Gateway certificate Common Name must match the URL to which the VPN client is connected.

If **Enable Password Persistence** is enabled, the user password is cached. If Store VPN Password on Device is also enabled, the user password is saved on the device until a sign-in failure occurs.

Step 6 Configure VPN Feature. Choose **Advanced Features** > **VPN** > **VPN Feature Configuration**.

Step 7 Assign a Common Phone Profile. Choose **Device** > **Device Settings** > **Common Phone Profile**.

VPN Configuration Settings

The following table describes the VPN configuration options for devices on Cisco Unified Communications Manager.

Table 14: VPN Configuration Options

Option	Description	To Change
Administrator Provisioned VPN Gateway	VPN enabled with VPN Group Configuration.	Display Only - Cannot change.

Option	Description	To Change
User Defined VPN Profiles	Shows whether option is enabled or disabled.	In the individual device configuration window or **Common Phone Profile** window (Product Specific Configuration layout area), set Allow User Defined Profiles to On or Off. **Note** Available for multilevel configurations. Administrator may change at device, common, or enterprise levels. If the feature is disabled on Cisco Unified Communications Manager, user-defined VPN profiles are removed from the list on the device and **Add New VPN Connection** is disabled.
Always Require VPN	Shows whether option is enabled or disabled.	Choose **Device** > **Device Settings** > **Common Phone Profile**. Choose the desired profile. Set Always Require VPN to On or Off. **Note** Always Require VPN setting overwrites enable and autoNetworkDetect values to True.
Store VPN Password on Device	Shows whether option is enabled or disabled.	Choose **Device** > **Device Settings** > **Common Phone Profile** or **Device** > **Phone** > **Phone Configuration**. Set Store VPN Password on Device to On or Off. **Note** Store VPN Password on Device only works if password persistence is enabled for the configured VPN profile, and if the client authentication method is “User and Password” or “Password only”.

Note Network configuration changes can potentially affect an active VPN connection.

If VPN is enabled, no proxy is configured or used for VPN.

VPN Authentication

Cisco DX Series devices support the following VPN authentication methods:

- Username and password
- Certificate only
- Password only

Note For password-only authentication, the device ID is prefilled as the username; Cisco Adaptive Security Appliance (ASA) configures the username.

The authentication that is specified on Cisco Unified Communications Manager must match authentication that is set on the ASA. If the authentication does not match that on the ASA, the user VPN is still allowed, but password persistence and autoconnect features are not applicable.

Startup Process

Upon connection to the network, Cisco DX Series devices go through a standard startup process. Depending on your specific network configuration, only some of these steps may occur on your devices.

1. Obtain power from the switch. If a device is not using external power, the switch provides inline power through the Ethernet cable that is attached to the device. The **Starting up...** screen appears for about 30 seconds.

   The device attempts to detect an Ethernet connection. If an Ethernet connection is detected but no IP address is assigned, the user is prompted to contact the administrator for assistance. If an Ethernet connection is not found, the device attempts to establish a wireless network connection.
2. (In a wireless LAN only) Scan for an access point. The device scans the RF coverage area. The device searches the network profiles and scans for access points that contain a matching Service Set Identifier (SSID) and authentication type. The device associates with the access point that matches the network profile configuration.
3. (In a wireless LAN only) Authenticate with the access point. The device begins the authentication process.
4. Load the stored device image. The device has nonvolatile flash memory in which the device stores firmware images and user-defined preferences. At startup, the device runs a bootstrap loader that loads a firmware image that is stored in flash memory. Using this image, the device initializes the software and hardware.
5. Configure the VLAN. If the device is connected to a Cisco Catalyst switch, the switch next informs the device of the voice VLAN that is defined on the switch. The device needs the VLAN membership information before it can proceed with the Dynamic Host Configuration Protocol (DHCP) request for an IP address.
6. Obtain an IP address. If the device is using DHCP to obtain an IP address, the device queries the DHCP server to obtain one. If you are not using DHCP in your network, you must assign static IP addresses to each device locally.

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

   If the TFTP server is not found, the user is prompted to sign in to Expressway.

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

8 (A device connected to Expressway skips this step)

   Request the CTL file. The TFTP server stores the CTL file. This file contains the certificates that are necessary to establish a secure connection between the device and Cisco Unified Communications Manager.

9 (A device connected to Expressway skips this step)

   Request the ITL file. The device requests the ITL file after it requests the CTL file. The ITL file contains the certificates of the entities that the device can trust. The certificates are used to authenticate a secure connection with the servers or to authenticate a digital signature that is signed by the servers. Cisco Unified Communications Manager 8.5 and later supports the ITL file.

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

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

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

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

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

12 If the device is booting for the first time, display the **Welcome** screen and run the Setup Assistant.

Set TFTP Server Manually During Startup

Procedure

Step 1 While the screen shows `Starting up...`, tap the upper left corner of the screen three times..

Step 2 An extra period is added to the end of `Starting up...` to indicate that the key sequence was detected.

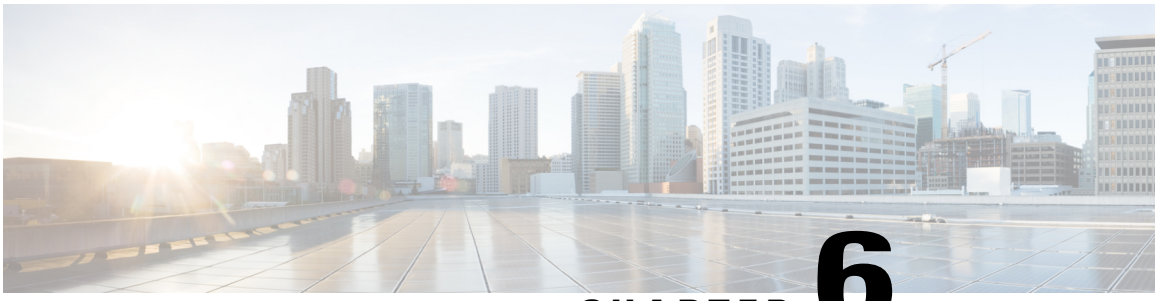
Step 3 The TFTP configuration screen appears. Enter the TFTP server address and tap **Confirm**.

Startup Verification

After the device has power connected to it, the device begins the startup diagnostic process by cycling through the following steps.

1. During the various stages of bootup as the device checks the hardware (Cisco DX650 only: the handset light and Mute button flash red and the Headset button and Speaker button flash green), the Lock/Power button is lit (white).
2. The Phone icon appears on the status bar.

If the device completes these stages successfully, it has started up properly, and the Lock/Power button stays lit.



CHAPTER 6

Contacts

- Contacts and Directories by Operating Mode, page 63
- Local Contacts, page 64
- Corporate Directory, page 64
- Contacts Search, page 65
- Application Dial Rules, page 65

Contacts and Directories by Operating Mode

Contact Source	Public Mode	Simple Mode	Enhanced Mode
Created on device	Yes	Yes	Yes
Imported from Bluetooth	Yes	Yes	Yes
Cisco User Data Services (UDS)	Yes	Yes	Yes
Jabber	No	No	Yes
Exchange Global Address List	No	No	Yes
Google	No	No	Yes
Third-party apps	No	No	Yes

Local Contacts

Local contacts are the contacts that a user creates on their DX device. Local contacts can also include contacts imported from a mobile phone via Bluetooth.

In Enhanced Mode, local contacts can also include contacts synced from Jabber, an Exchange account, a Google account, or third party applications.

Local contacts with a phone number are available on the Contacts tab in the Call application. All local contacts are available in the People application.

Corporate Directory

The Corporate Directory allows a user to look up contact information for coworkers. To support this feature, you must configure a corporate directory.

Cisco Unified Communications Manager uses a Lightweight Directory Access Protocol (LDAP) directory to store information about users of Cisco Unified Communications Manager, and to sync to Active Directory (AD).

Cisco DX Series devices use Cisco User Data Services (UDS) to query Cisco Unified Communications Manager for corporate directory information.

Cisco DX Series devices do not support traditional XML directories, including custom directories.

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

Set Company Photo Directory

Set this parameter to show directory photos when a user searches the corporate directory using UDS, and for directory search results that the user adds as a local contact.

Procedure

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

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

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

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

Step 2 Set **Company Photo Directory** to http://<servername>/<path>/%%uid%%.<image file extension>.

Step 3 Check **Override Common Settings**.

Contacts Search

Cisco DX Series users can search their locally stored contacts, Recents and corporate directory (UDS). Users operating DX Series devices in Enhanced Mode can also search Jabber contacts and online directories such as Exchange.

Users can search by:

- First name
- Last name
- Phone number
- Username

Users can search their corporate directory on the Directory tab. Corporate directory searches show a maximum of 25 results.

Search results will show a photo (if available), first and last name, and a URI or phone number. If the search result includes both a URI and a phone number, the URI is shown.

Optimize Search Results

By default, the user can search for local contacts on the Calls tab, but not directories. Follow this procedure to show corporate directory results while searching on the Calls tab. Directory results will show up below local contacts in the search results, and will be sorted by directory type.

Procedure

Step 1 Tap .

Step 2 Tap **Settings**.

Step 3 Check **Directory results**.

Application Dial Rules

Application Dial Rules are used to convert numbers for shared mobile contacts to network dialable numbers. Application Dial Rules do not apply when the user is dialing a number manually, or if the number is edited before the user places the call.

Application Dial Rules are set in Cisco Unified Communications Manager. For more information, see the "Dial Rules Overview" chapter of the *Cisco Unified Communications Manager System Guide*.

Configure Application Dial Rules

Procedure

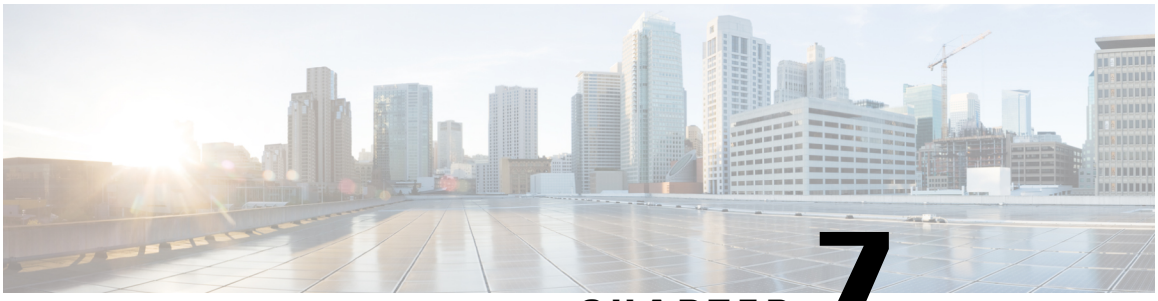
Step 1 In Cisco Unified Communications Manager Administration, go to **Call Routing** > **Dial Rules** > **Application Dial Rules**.

Step 2 Choose **Add New** to create a new application dial rule, or choose an existing application dial rule to edit it.

Step 3 Fill in the following fields:

- **Name** This field comprises a unique name for the dial rule that can contain up to 20 alphanumeric characters and any combination of spaces, periods (.), hyphens (-), and underscore characters (_).
- **Description** This field comprises a brief description that you enter for the dial rule.
- **Number Begins With** This field comprises the initial digits of the directory numbers to which you want to apply this application dial rule.
- **Number of Digits** This required field comprises the initial digits of the directory numbers to which you want to apply this application dial rule.
- **Total Digits to be Removed** This required field comprises the number of digits that you want Cisco Unified Communications Manager to remove from directory numbers that apply to this dial rule.
- **Prefix With Pattern** This required field comprises the pattern to prepend to directory numbers that apply to this application dial rule.
- **Application Dial Rule Priority** This field displays when you enter the Prefix With Pattern information. The field allows you to set the priority order of the application dial rules.

Step 4 Restart Cisco Unified Communications Manager.



CHAPTER 7

Self Care Portal Management

- Self Care Portal Overview, page 67
- Set Up Access to Self Care Portal, page 68
- Customize Self Care Portal Display, page 68

Self Care Portal Overview

From the Cisco Unified Communications Self Care Portal, users can customize and control phone features and settings. For information about the Self Care Portal, see the *Cisco Unified Communications Self Care Portal User Guide* located at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-user-guide-list.html.

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

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:

- *Cisco Unified Communications Manager Administration Guide*, “Access Control Group Setup” chapter
- *Cisco Unified Communications Manager Administration Guide*, “End User Setup” chapter
- *Cisco Unified Communications Manager Administrator Guide*, “Role Setup” chapter

Set Up Access to Self Care Portal

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

Procedure

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

Customize Self Care Portal Display

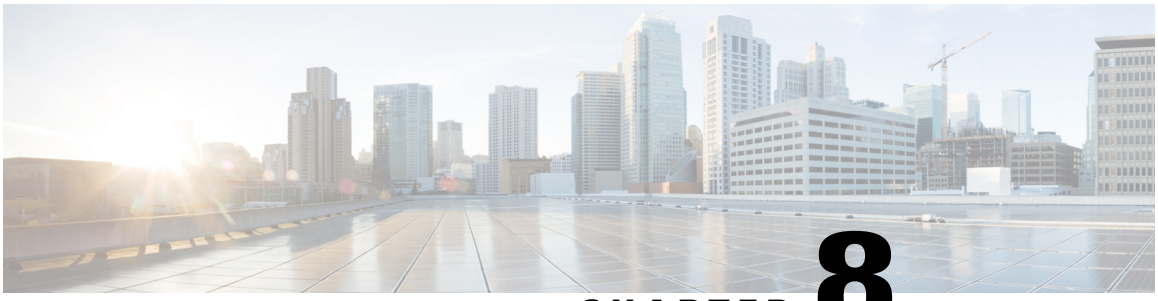
Most options display on the Self Care Portal. However, you must set the following options by using Enterprise Parameters Configuration settings in Cisco Unified Communications Manager Administration:

- 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**.



CHAPTER 8

Accessories

- Bluetooth Accessories, page 69
- Cable Lock, page 71
- External Cameras, page 71
- External Speakers and Microphone, page 72
- Headsets, page 72
- Video Displays, page 76
- Cisco DX650 Wall-Mount Kit, page 76

Bluetooth Accessories

Users can pair Bluetooth accessories, such as headsets, keyboards, and mobile phones, to their DX Series devices.

Users can pair multiple Bluetooth devices at one time, however they may only pair one Bluetooth audio device at a time.

Enabling Bluetooth may degrade a wireless network connection. For improved wireless network performance, users should disable Bluetooth when it is not in use, or use the 5 GHz band for their wireless network connection.

Bluetooth Device Profiles

The Device Profile Settings screen shows the profiles that are available for a paired device. If you disable a profile, the profile is unchecked and the user cannot enable it.

Handsfree Profile

Cisco DX Series devices support various Handsfree Profile features that enable you to use accessories (such as Bluetooth wireless headsets and Bluetooth-capable mobile phones) to perform certain tasks without the need to handle the device. For example, rather than tap Redial on the device, users can follow instructions from the headset manufacturer to redial a number from their Bluetooth wireless headset.

These hands-free features apply to Bluetooth accessories:

- Handle Bluetooth HFP connected/disconnected status.
- Dial a phone number on the Audio Gateway (AG) to make a call.
- Indicate when a call is connected or disconnected.
- Notify an application when a call is incoming (inband ringtone).
- Enable or disable inband ringing.
- Report phone status (such as caller ID, signal strength, and battery level, from the AG).
- Answer or reject calls.
- Receive call-waiting notification with caller ID.
- Put a call on hold and switch to a waiting call.
- Switch between calls on hold and active calls on the AG and in the Call application.
- Switch audio to the mobile phone and return audio back to the Hands-Free Unit.
- Retrieve the mobile phone call list.

Hands-free devices may differ as to how features are activated. Device manufacturers may also use different terms to refer to the same feature. For more information, see the manufacturer documentation.

Phone Book Access Profile

Bluetooth Phone Book Access Profile (PBAP) allows the user to share contacts and call history from a paired mobile phone to a Cisco DX Series device. The user can choose to download contacts and call history manually or automatically when they pair their mobile phone, and can choose to save the contacts on their device.

Enable Device Profiles

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Phone**, locate the device you want to modify, and go to the **Phone Configuration** window for that device.

Step 2 In the **Phone Configuration** window, choose **Enable** for the Bluetooth setting.

Step 3 Enable a device profile.

Step 4 Save your changes.

Pair Bluetooth Accessory

Procedure

Step 1 In the Settings application of the device, toggle **Bluetooth** on.

Step 2 Tap a device to pair from the available devices list.

Step 3 Verify the passkey and tap **Pair**.

Disable Bluetooth

Procedure

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

Step 2 In the **Find and List Phones** window, enter the search criteria for the device that you want to modify, and then click **Find**.

Step 3 In the Product Specific Configuration Layout area of the **Phone Configuration** window, choose **Disabled** from the Bluetooth drop-down list box.

Cable Lock

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

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

External Cameras

Cisco DX650 supports the add-on Logitech C920-C Webcam or Logitech C930e as an external camera.

The external camera connects to the device and allows the user to make a point-to-point video calls. For the external camera to work, video calling and USB devices must be enabled.

Note If the Cisco DX650 is powered by Power over Ethernet, the external camera requires 802.3at. If the phone is not powered by Power over Ethernet, the external camera requires an external power supply.

External Camera Settings

After you attach the external camera to the device, the user can control the settings of the external camera. Unlike the internal camera, the brightness setting for the external camera cannot be adjusted.

Perform External Camera Postinstallation Checks

Procedure

Step 1 Wait until the `External Camera Connected` message appears.

Step 2 In the Call application, tap .

Step 3 Tap **Self view**.

Step 4 Move the device and external camera to a position where no bright lights are in the field of view.

Step 5 Move the device and external camera so that the user is illuminated from the front.

External Speakers and Microphone

External speakers and microphones are plug-and-play accessories. You can use the line in/out jack to connect an external PC-type microphone and powered speakers (with amplifier) on the device. Connection to an external microphone disables the internal microphone, and connection to an external speaker disables the internal speaker.

Note Use of poor-quality external audio devices, use of loudspeakers at very loud volumes, or placement of the microphone very close to the loudspeaker may result in undesirable echo for other parties on your speakerphone calls.

Headsets

Although Cisco performs internal testing of third-party headsets, Cisco does not certify nor support products from headset or handset vendors.

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

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

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

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

Cisco recommends that customers test headsets in the intended environment to determine performance before purchase and deployment on a large scale.

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

Bluetooth Wireless Headsets

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

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

Wideband for Bluetooth headsets is not supported. Voice quality may be reduced when using Bluetooth headsets.

The best performance is in the 3- to 6-foot range (1 to 2 meters). You can pair five or more headsets, but only the last headset that was connected is used as the default. When headsets are more than 30 feet (10 meters) away from the device, Bluetooth drops the connection after a 15- to 20-second timeout. If the paired headset comes back into device range and the device is not connected to another Bluetooth headset, the in-range Bluetooth headset automatically reconnects. For certain devices that operate in power-save modes, the user can tap the operational button to initiate the reconnection and *wake up* the headset.

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

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

For more information about Bluetooth headsets, see the user guide that is provided with the headset.

Add Bluetooth Wireless Headset

Procedure

Step 1 Place the headset into discovery/pairing mode.

Note The procedure to place a headset into discovery/pairing mode is specific to the headset. See the headset manufacturer instructions for the pairing procedure.

The headset must be in discovery/pairing mode to successfully pair and connect to the device.

Step 2 Toggle on Bluetooth on the device, if you have not already done so.
To verify whether Bluetooth is on, look for the Bluetooth icon on the status bar.

Step 3 Select **Scan for devices**.
After the Bluetooth device is located, its name appears in the window.

The device automatically uses PIN `0000` to pair with the headset. If the headset uses a different PIN, enter the correct PIN as found in the user guide that came with the headset.

Note If pairing is unsuccessful, the device prompts you to enter the correct PIN.

After the device has the correct PIN, the device tries to connect to the accessory. If the device cannot connect, it displays an error alert to let the user know the reason for the failure. A timeout of 10 seconds occurs for the device to try to connect the accessory. If the timer expires without a successful connection, an error alert is shown.

After an accessory has been paired, its Bluetooth connection is maintained as long as both the Cisco DX Series device and the headset are enabled and within range of each other. The connection typically reestablishes itself automatically if either of the devices powers down and then powers up. However, some headsets require user action to reestablish the connection.

When a headset is out of range of the device, Bluetooth drops the connection after a 15- to 20-second timeout. If the paired headset comes back into range of the device (and the device is not connected to another Bluetooth headset), the in-range Bluetooth headset automatically reconnects. The user may have to tap the headset operational button to wake up the headset and begin the reconnect process.

If a user is using a Bluetooth headset on an active call and the headset is set to off, is out of range, or is disconnected for any reason, an alert prompts the user to either continue the call on the speaker/headset or disconnect the call. If the user takes no action within 30 seconds, the call ends.

Remove Bluetooth Headset

Procedure

Step 1 In the Settings application, select **Bluetooth**.

Step 2 Tap the **Settings** icon next to the device name.

Step 3 Tap **Unpair**.

USB Headsets

Wired and wireless USB headsets are supported. You can connect a USB headset (or the base station for a wireless headset) to any USB port.

Enable USB Headset

These parameters can be enabled in either the **Phone Configuration** window (**Device** > **Phone**), the **Enterprise Phone Configuration** window (**System** > **Enterprise Phone Configuration**), or the **Common Phone Profile** window (**Device** > **Device Settings** > **Common Phone Profile**).

Procedure

Step 1 Enable the applicable USB port in the Product Specific Configuration layout portion of the window.

Step 2 Choose **Audio Class** for the Enable/Disable USB Classes parameter and check **Override Common Settings**..

Disable USB Headset

Procedure

Disable the USB port (or disable the Audio Class parameter) that you enabled in Cisco Unified Communications Manager Administration.

Wired Headsets

Cisco DX70 and Cisco DX650 support 3.5 mm single-plug headsets. The user can place and answer calls with the headset.

Connect to Wired Headset

Procedure

Plug the headset into the Headset port.

Disable Wired Headset

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

Procedure

Step 1 To disable the headset from Cisco Unified Communications Manager Administration, choose **Device** > **Phone** and locate the device that you want to modify.

Step 2 In the **Phone Configuration** window (Product Specific Configuration layout area), check the **Disable Speakerphone and Headset** check box.

Video Displays

Cisco DX650 supports external display devices through the HDMI port. Connect a monitor to the device by inserting one end of an HDMI cable into the HDMI port and the other end into a monitor HDMI port.

Cisco DX650 Wall-Mount Kit

To mount the Cisco DX650 on the wall, use the special brackets that are available in a Cisco DX650 wall-mount kit. Wall-mount kits must be ordered separately from the device.

Before You Begin

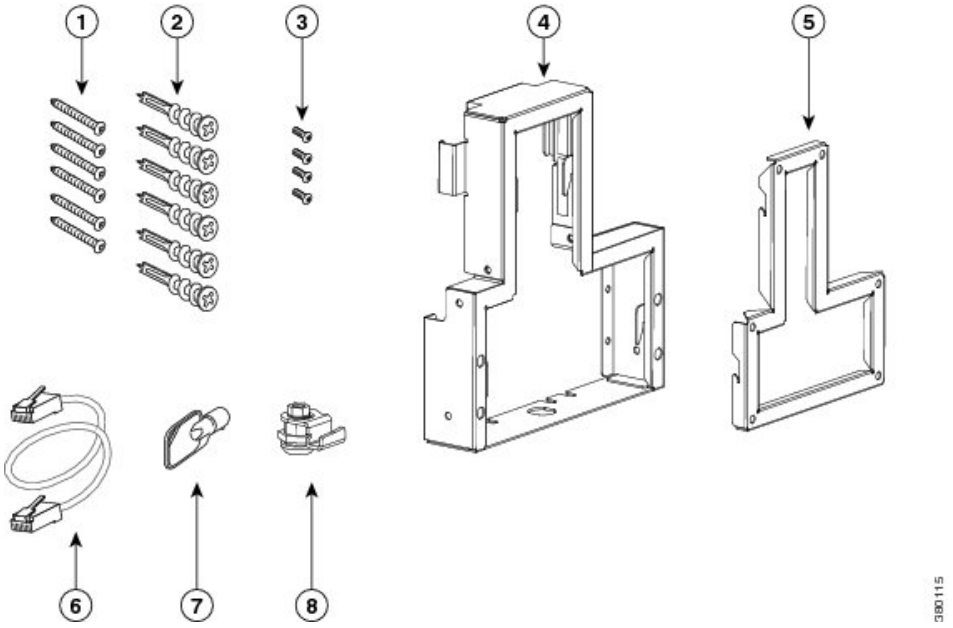
You need these tools to install the bracket:

- No. 1 and No. 2 Phillips screwdrivers
- Level

Wall-Mount Components

Note The hardware that is included in this wall-mount kit is for drywall installation. For installation onto other surfaces, such as brick or concrete, you must provide your own hardware.

Figure 1: Wall-Mount Kit for Single-Phone Assembly



1	Six 8-18 x 1.25 inch Phillips-head screws	5	One wall bracket
2	Six anchors	6	One 6-inch Ethernet cable
3	Four 3 x 6mm machine screws	7	One lock-down key
4	One phone bracket	8	One lock

Install Wall-Mount

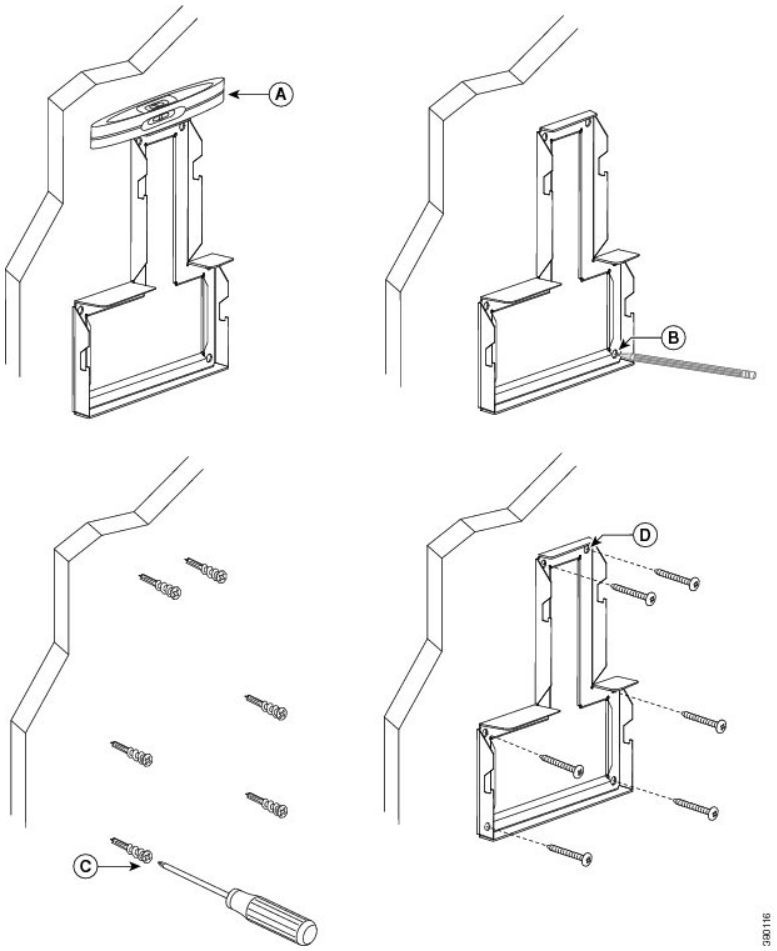
Procedure

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

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

b) Carefully center the anchor over the pencil mark and use a no. 2 Phillips screwdriver to press the anchor into the wall.
c) Screw the anchor clockwise into the wall until the anchor is seated flush.
d) Use the included screws and a no. 2 Phillips screwdriver to attach the bracket to the wall.

Figure 2: Attach Wall Bracket

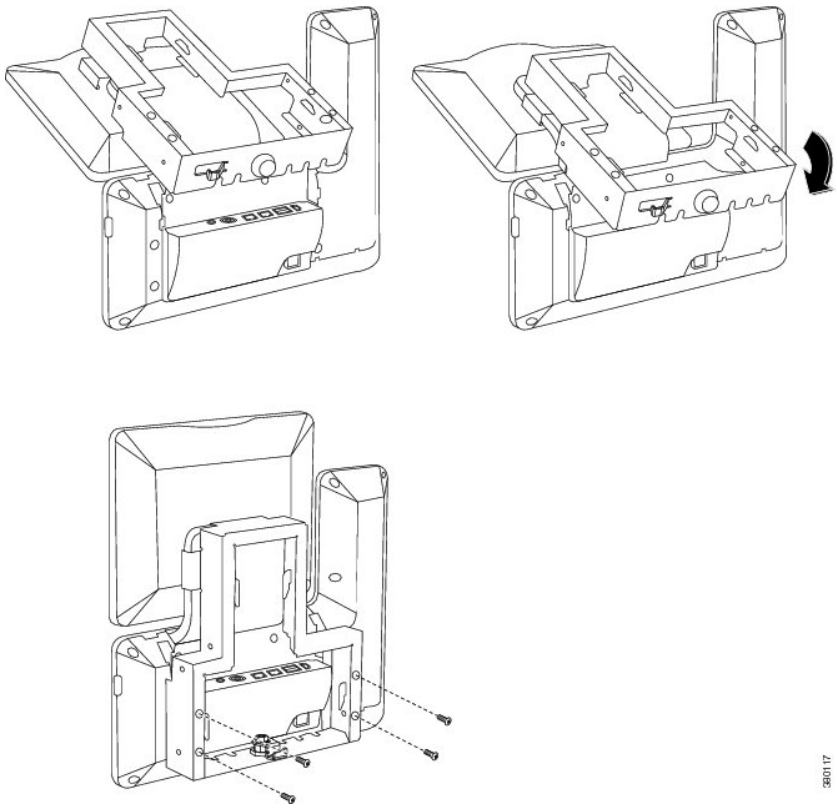


Step 2 Attach the phone bracket to the device.

a) Detach any attached cords from the base of the device.
b) Slide the phone bracket onto the phone. Ensure that the device ports are accessible through the holes in the bracket.
c) Use the machine screws to secure the phone bracket to the device.

d) Reattach the cords and seat them in the clips that are incorporated into the device body.

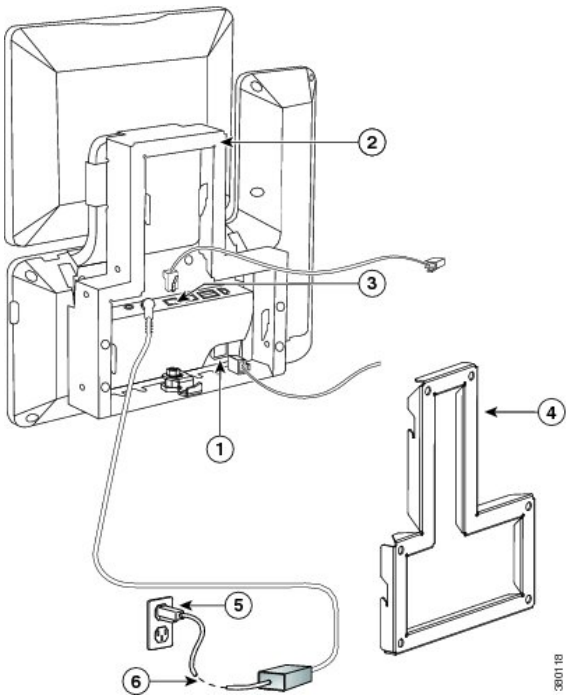
Figure 3: Attach Phone Bracket



Step 3 Attach the Ethernet cable to the 10/100/1000 SW network port and wall jack.
If you are connecting a network device (such as a computer) to the device, attach the cable to the 10/100/1000 computer (PC access) port.

If you are using an external power supply, plug the power cord into the device.

Figure 4: Attach Cables

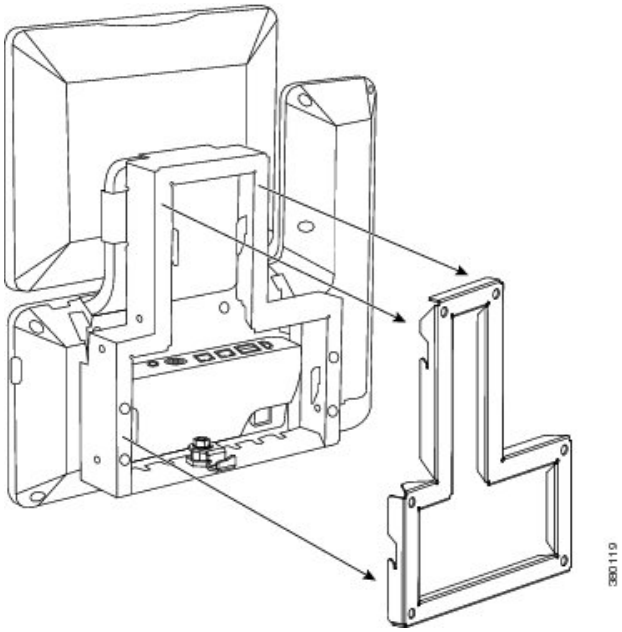


1	Handset port	4	Wall bracket
2	Phone bracket	5	AC adapter port
3	Network port	6	Power cable

Step 4 To attach the device to the wall bracket, insert the tabs on the top of the phone bracket into the slots on the wall bracket. Ensure that the power cord and any other cable that does not terminate in the wall behind the

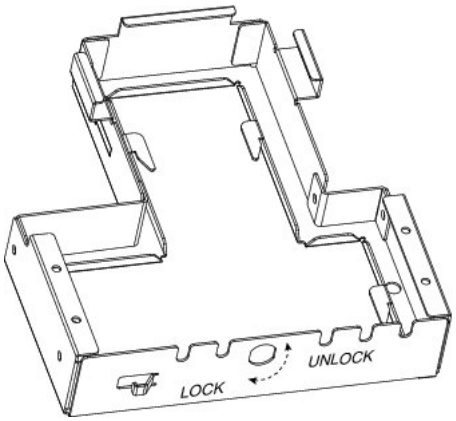
bracket are positioned in one of the cable-access openings in the bottom of the bracket. The phone and wall bracket openings together form circular openings with room for one cable per opening.

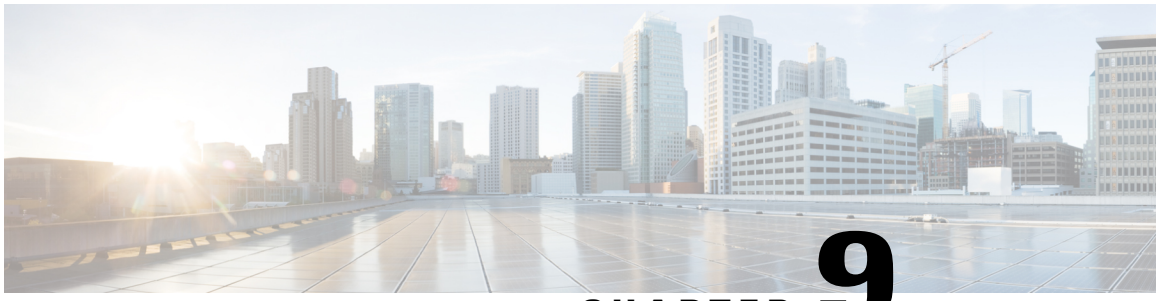
Figure 5: Attach Device to Wall Bracket



Step 5 Use the lock-down key to lock the device to the wall bracket.
You can store the lock-down key on the key hook at the bottom of the phone bracket.

Figure 6: Phone Bracket with Key Hook





CHAPTER 9

Security Features

- Device Security, page 83
- Screen Lock and Automatic Lock Setup, page 93

Device Security

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

Cisco Unified Communications Manager Release 8.5(1) and later includes Security by Default, which provides the following security features for devices without the need to run the CTL client:

- Signing of the configuration files
- Configuration file encryption
- HTTPS with Tomcat and other web services

Note Secure signaling and media features require a CTL file.

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

Alternatively, you can initiate the installation of an LSC from the Settings application on the device. This Settings application also lets you update or remove an LSC.

Overview of Security Features

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

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

Cisco DX Series devices use the device security profile, which defines whether the device is nonsecure or secure. For information about applying the security profile to the device, see the *Cisco Unified Communications Manager Security Guide*.

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

The following table provides an overview of the security features that the device supports.

Table 15: Overview of Security Features

Feature	Description
Image authentication	Signed binary files (with the extension .sbn) and encrypted binary files (with the extension .sebn) prevent tampering with the firmware image before the image is loaded on a device. Tampering with the image causes a device to fail the authentication process and reject the new image.
Customer-site certificate installation	Each device requires a unique certificate for device authentication. Devices include a manufacturing installed certificate (MIC), but for additional security, you can specify in Cisco Unified Communications Manager Administration that a certificate be installed through use of the Certificate Authority Proxy Function (CAPF). Alternatively, you can install a Locally Significant Certificate (LSC) from the Enterprise security menu on the device.
Device authentication	Occurs between the Cisco Unified Communications Manager server and the device when each entity accepts the certificate of the other entity. Determines whether a secure connection between the device and a Cisco Unified Communications Manager should occur; if necessary, creates a secure signaling path between the entities through TLS protocol. Cisco Unified Communications Manager does not register devices unless it can authenticate them.
File authentication	Validates digitally signed files that the device downloads. The device validates the signature to make sure that file tampering did not occur after file creation. Files that fail authentication are not written to flash memory on the device. The device rejects such files without further processing.
File encryption	Encryption prevents disclosure of sensitive information while the file is in transit to the device. In addition, the device validates the signature to make sure that file tampering did not occur after file creation. Files that fail authentication are not written to flash memory on the device. The device rejects such files without further processing.
Signaling authentication	Uses the TLS protocol to validate that no tampering to signaling packets has occurred during transmission.
Manufacturing installed certificate	Each device contains a unique manufacturing installed certificate (MIC), which is used for device authentication. The MIC provides permanent unique proof of identity for the device and allows Cisco Unified Communications Manager to authenticate the device.

Feature	Description
Media encryption	Uses SRTP to ensure that media streams between supported devices prove secure and that only the intended device receives and reads the data. Includes creation of a media master key pair for the devices, delivery of the keys to the devices, and securing the delivery of the keys while the keys are in transport.
CAPF (Certificate Authority Proxy Function)	Implements parts of the certificate generation procedure that are too processing-intensive for the device, and interacts with the device for key generation and certificate installation. The CAPF can be configured to request certificates from customer-specified certificate authorities on behalf of the device, or it can be configured to generate certificates locally.
Security profile	Defines whether the device is nonsecure, authenticated, encrypted, or protected. Other entries in this table describe security features. For more information about these features, see the *Cisco Unified Communications Manager Security Guide*.
Encrypted configuration files	Lets you ensure the privacy of device configuration files.
Optional web server disabling for a phone	For security purposes, you can prevent access to the web pages for a device (which display a variety of operational statistics for the device).
Phone hardening	Additional security options, which you control from Cisco Unified Communications Manager Administration: • Disable PC port • Disable Gratuitous ARP (GARP) • Disable PC Voice VLAN access • Provide restricted access to the web applications • Disable Bluetooth Accessory Port • Disable access to web pages for a device • Require a screen lock • Control access to Google Play™ • Control access to installation of applications from unknown sources
802.1X Authentication	The device can use 802.1X authentication to request and gain access to the network.
Secure SIP Failover for SRST	After you configure a Survivable Remote Site Telephony (SRST) reference for security and then reset the dependent devices in Cisco Unified Communications Manager Administration, the TFTP server adds the SRST certificate to the device cnf.xml file and sends the file to the device. A secure device then uses a TLS connection to interact with the SRST-enabled router.
Signaling encryption	Ensures that all SIP signaling messages that are sent between the device and the Cisco Unified Communications Manager server are encrypted.

Feature	Description
AES 256 Encryption	When connected to Cisco Unified Communications Manager Release 10.5(2) and later, DX Series devices support AES 256 encryption support for TLS and SIP for signaling and media encryption. This enables the devices to initiate and support TLS 1.2 connections using AES-256 based ciphers that conform to SHA-2 (Secure Hash Algorithm) standards and are Federal Information Processing Standards (FIPS) compliant.

Security Profiles

Cisco DX Series devices use a security profile, which defines whether the device is nonsecure, authenticated, or encrypted. For information about configuration of the security profile and application of the profile to the device, see the *Cisco Unified Communications Manager Security Guide*.

To view the security mode that is set for the device, view the Security menu in the Settings application.

SE Android

The Security Enhancements for Android™ (SE Android) feature enhances device security. SE Android protects against malicious applications through prevention of attempts to execute unauthorized or dangerous code on the device. SE Android does the following:

- Can prevent privilege escalation by processes
- Can prevent misuse and limit damage if privileged process, such as root, is compromised
- Provides centralized, enforced, analyzable policy
- Protects from undiscovered vulnerabilities

The device contains a policy that specifies the data that an application, process, or user can access. SE Android supports two modes:

- Permissive
- Enforcing

Anything that violates the policy is logged. If the mode is enforcing, the action is denied. No user nor administrator control exists over the policy or the mode.

Upgrades and SE Android

Upon upgrade to Release 10.2(2), Cisco DX650 remains in permissive mode because it must work with existing field units, which require a factory reset before enforcing mode can be enabled. In permissive mode, SE Android has no impact on the endpoint operation.

After a Cisco DX650 has been factory reset, the mode switches automatically to enforcing mode. This action activates SE Android protection and starts denial of actions that violate the policy.

Enforcing mode remains in effect unless the device is downgraded to a firmware release below 10.2(2). Upon upgrade to Release 10.2(2) or later, the device returns to permissive mode until factory reset is performed.

Cisco DX70 and Cisco DX80 devices are always in enforcing mode from the factory. Cisco DX70 and Cisco DX80 devices cannot be placed in permissive mode.

SE Android Troubleshooting

Policy is tuned to the expectation of what an application should be allowed to do. However, policy may prevent an operation that should be allowed. Symptoms of policy errors may include:

- Third-party or other app shows error on launch or while executing.
- App or feature works on endpoint that is in permissive mode, such as Cisco DX650, but not on a similarly configured device in enforcing mode.
- SE Android is an always-on feature and is not under administrator control. Field problems should be diagnosed and reported as defects.

Diagnose SE Android Policy Issues

Procedure

Step 1 Determine the SE Android mode:

a) From the Settings application, tap **About device** > **SELinux status**.

b) From Debugsh, enter command **show selinux status**.

If the mode is permissive, the problem is not SE Android related.

Step 2 If mode is enforcing, retest on a device that is in permissive mode.
If the problem is not reproducible in permissive mode, the problem is most likely SE Android related.

Step 3 If problem is SE Android related or cannot be determined, collect logs and report.

ADB Shell Limitations

When the endpoint is in enforcing mode, the Android Debug Bridge (adb) shell is limited. Commands such as **ls** and **ps** may not show full results.

Use debugsh commands for full results. For example, use debugsh **show process** instead of **ps** from the shell.

Enforcing mode also prevents you from freely browsing the file system, as many directories are off limits in enforcing mode.

SE Android Log Collection

To report an issue, collect this information:

- Brief description of the issue, including time of occurrence
- Screenshot of the problem if possible
- Output of debugsh **show selinux all** command
- Output of Problem Reporting Tool (PRT)

Set Up Locally Significant Certificate

Before You Begin

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

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

See the *Cisco Unified Communications Manager Security Guide* for more information.

Procedure

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

Step 2 In the Settings application, choose **Security** > **Enterprise security settings**.

Step 3 Tap **LSC**.
The device prompts for an authentication string.

Step 4 Enter the authentication string and tap **Submit**.
The device begins to install, update, or remove the LSC, depending on how the CAPF was configured. During the procedure, a series of messages appear so you can monitor progress.

Note The LSC installation, update, or removal process can take a long time to complete. You can stop the process at any time by tapping **Cancel**.

After the installation procedure is completed successfully, the device indicates `Installed`. If the device indicates `Not Installed`, the authorization string may be incorrect or the device may not enabled for upgrade. If the CAPF operation deletes the LSC, the device indicates `Not Installed` to indicate that the operation was successful. See error messages that are generated on the CAPF server and take appropriate actions.

Note The device restarts after LSC is installed, upgraded, or deleted.

SHA-256 Manufacturing Installed Certificate

Cisco DX70 and Cisco DX80 use a manufacturing installed certificate (MIC) with the signature algorithm of SHA-256 with an RSA 2048 key. The signature algorithm requires Cisco Unified Communications Manager, Cisco Secure Access Control Server (ACS), and Secure SRST support.

The SHA-256 MIC feature has the following support requirements:

- Cisco Unified Communications Manager Release 9.1(2) and later
- ACS Release 5.2 and later.

Note ACS 5.2 and later do not support EAP-FAST with EAP-TLS inner method. Use EAP-TLS or migrate to ISE for EAP-FAST with EAP-TLS inner method.

- IOS 12.4(15)T1 and later
- Cisco Identity Service Engine release is 1.1 and later. The EAP-FAST with EAP-TLS inner method is supported starting from ISE release 1.2 and later.

The Cisco certificate authority issuing the MIC for this series of phones can be obtained from the following links if separate applications are used and these applications need to authenticate MIC from the phone:

- http://www.cisco.com/security/pki/certs/cmca2.cer
- http://www.cisco.com/security/pki/certs/crcam2.cer

These Cisco certificate authorities must be imported into applications in order for the applications to authenticate MIC for Cisco DX Series devices.

Secure Phone Calls

To implement security for Cisco DX Series devices, enable the Protected Device parameter from the **Phone Configuration** window in Cisco Unified Communications Manager Administration. When security is implemented, the presence of the Secure Call icon in the Call application indicates secure phone calls.

In a secure call, all call signaling and media streams are encrypted. A secure call offers a high level of security and provides integrity and privacy to the call. When a call in progress is being encrypted, the Security Mode status on **Enterprise security** in the Settings application indicates Encrypted.

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

In a secure call, a 2-second tone notifies the users when a call is encrypted and both devices are configured as protected devices, and if secure tone features are enabled on Cisco Unified Communications Manager. The tone plays for both parties when the call is answered. The tone does not play unless both devices are protected and the call occurs over encrypted media. If the system determines that the call is not encrypted, the device plays a nonsecure indication tone (6 beeps) to alert the user that the call is not protected. For a detailed description of the Secure Indication Tone feature and the configuration requirements, see the *Cisco Unified Communications Manager Security Guide*.

Note Audio and video can be transmitted as secure, but presentations are transmitted as nonsecure. The **Encrypted** lock icon is displayed for calls with a presentation by default. You can configure **Secure Call Icon Display Policy Required** to another option in Cisco Unified Communications Manager at **System** > **Service Parameter**. The default setting is **All media except BFCP and iX transports must be encrypted**.

Secure Phone Call Identification

A secure call is established when a Cisco DX Series device and a device on the other end are configured for secure calling. Both devices can be in the same Cisco IP network, or on a network outside the IP network. A secure conference call is established through this process:

1. A user initiates the call from a secured device (Encrypted security mode).
2. The device indicates the Encrypted status on Enterprise security in the Settings application. This status indicates that the device is configured for secure calls, but does not mean that the other connected phone is also secured.
3. A security tone plays if the call connects to another secured device, which indicates that both ends of the conversation are encrypted and secured. Otherwise, nonsecure tone plays.

Note Secure tone plays only when it is enabled on Cisco Unified Communications Manager. If secure tone is disabled, no secure tone plays even the call is secure. For more information, see the "Secure and Nonsecure Indication Tone Setup" chapter of the *Cisco Unified Communications Manager Security Guide*.

Secure Conference Call Identification

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

1. A user initiates the conference from a secure device.
2. Cisco Unified Communications Manager assigns a secure conference bridge to the call.
3. As participants are added, Cisco Unified Communications Manager verifies the security mode of each device and maintains the secure level for the conference.
4. The device indicates the security level of the conference call.

Various interactions, restrictions, and limitations affect the security level of the conference call, as determined by the security mode of the participant devices and the availability of secure conference bridges. Cisco DX Series devices support secure audio and video conference calls.

Audio and video can be transmitted as secure, but presentations are transmitted as nonsecure. The **Encrypted** lock icon is displayed for conference calls with a presentation by default. You can configure **Secure Call Icon Display Policy Required** to another option in Cisco Unified Communications Manager at **System** > **Service Parameter**. The default setting is **All media except BFCP and iX transports must be encrypted**.

Call Security Interactions and Restrictions

Cisco Unified Communications Manager checks the device security status when conferences are established and changes the security indication for the conference or blocks the completion of the call to maintain integrity and security in the system. The following table provides information about changes to call security levels with the Barge feature.

Table 16: Call Security Interactions with the Barge Feature

Initiator Phone Security Level	Feature Used	Call Security Level	Results of Action
Nonsecure	Barge	Encrypted call	The call is barged and identified as nonsecure call
Secure	Barge	Encrypted call	The call is barged and identified as secure call

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

Table 17: Security Restrictions with Conference Calls

Initiator Phone Security Level	Feature Used	Security Level of Participants	Results of Action
Nonsecure	Conference	Secure	Nonsecure conference bridge Nonsecure conference
Secure	Conference	At least one member is nonsecure.	Secure conference bridge Nonsecure conference
Secure	Conference	Secure	Secure conference bridge Secure encrypted level conference
Nonsecure	Meet Me	Minimum security level is encrypted.	Initiator receives message `Does not meet Security Level, call rejected`.
Secure	Meet Me	Minimum security level is nonsecure.	Secure conference bridge Conference accepts all calls.

When secure video is in use over VPN and Cisco Virtualization Experience Client (VXC) VPN, the maximum supported bandwidth is 320 kpbs.

When the device calls Cisco TelePresence, the maximum bandwidth is 320 kbps.

Check Device Security Information Remotely

Procedure

Step 1 To check device security information remotely, the device must be, or previously have been, registered to the Cisco Unified Communications Manager server, and Web Access must be enabled on the device configuration page.

Step 2 In a web browser, go to http://<device ip>/SecurityInformation to view device security information, or http://<device ip>/SecurityInformationX to view device security information in an XML format.

Encryption for Barge

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

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

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

802.1X Authentication Support

Cisco DX Series devices 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 DX Series devices provide an EAPOL pass-through mechanism. This mechanism allows a workstation that is attached to the device to pass EAPOL messages to the 802.1X authenticator at the LAN switch. The pass-through mechanism ensures that the device does not act as the LAN switch to authenticate a data endpoint before the device accesses the network.

Cisco DX Series devices also provide a proxy EAPOL Logoff mechanism. In the event that the locally attached PC disconnects from the device, the LAN switch does not see the physical link fail, because the link between the LAN switch and the device is maintained. To maintain network integrity, the device 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.

Cisco DX Series devices also contain an 802.1X supplicant. This supplicant allows network administrators to control the connectivity of devices to the LAN switch ports. The current release of the device 802.1X supplicant uses the EAP-FAST and EAP-TLS options for network authentication.

Required Network Components

Support for 802.1X authentication on Cisco DX Series devices requires several components. These include:

- The device itself, which acts as the 802.1X supplicant, which initiates the request to access the network.

- Cisco Secure Access Control Server (ACS) (or other third-party authentication server). The authentication server must be configured with a shared secret that authenticates the device.
- 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 device and the authentication server. After the exchange completes, the switch grants or denies the device access to the network.

Best Practices

The following list describes requirements and recommendations for 802.1X configuration.

- Enable 802.1X Authentication: If you want to use the 802.1X standard to authenticate Cisco DX Series devices, be sure that you properly configure the other components before you enable authentication on the device.
- Configure PC Port: The 802.1X standard does not take into account the use of 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 device.
    - 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, the devices 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/c/en/us/support/switches/catalyst-6500-series-switches/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 device 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 assignment of the port to the native VLAN.

Screen Lock and Automatic Lock Setup

The Screen Lock Timeout value controls the normal device idle timeout when the screen turns off and the screen lock is activated. The variable is configurable within a range of 1 to 60 minutes.

The Automatic Lock controls how long the display will stay on before it dims or goes off. If the device is in the Always On mode, the device will dim. If the device is in the Nightlight mode, it will turn off completely. The Automatic Lock value can be configured to a maximum value of 10 minutes. To configure the Automatic Lock value, go to **Settings** > **Security** > **Automatically lock**.

The following table shows the relationship of the Screen Lock Timeout value and Automatic Lock value.

Table 18: Screen Lock Timeout and Automatic Lock Value Relationship

Condition	Outcome
Screen Lock Timeout value is lower than Automatic Lock value	When the Screen Lock Timeout value is reached, screen stays at full brightness; locked screen displays.
Automatic Lock value is lower than Screen Lock Timeout value	When the Automatic Lock value is reached, two outcomes are possible: • If the device is in Always On mode, the device dims when the Automatic Lock value is reached. When the Screen Lock Timeout value is reached, the device locks and remains dimmed. • If the device is in Nightlight mode, the device locks and turns off when the Automatic Lock value is reached. When the Screen Lock Timeout value is reached, no additional changes occur.
Screen Lock Timeout value the same as the Automatic Lock value	When the value is reached, screen stays at full brightness; locked screen displays.

Set Up Screen Unlock/Password Reset

This feature allows the user to reset the PIN/password that is used to unlock the screen. The user can reset the PIN/password through use of Cisco Unified Communications Manager or configured Google™ account credentials. Use the following procedure to reset the PIN/password with Cisco Unified Communications Manager.

Procedure

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

Step 2 Click **Add New**.

Step 3 Enter required user information.

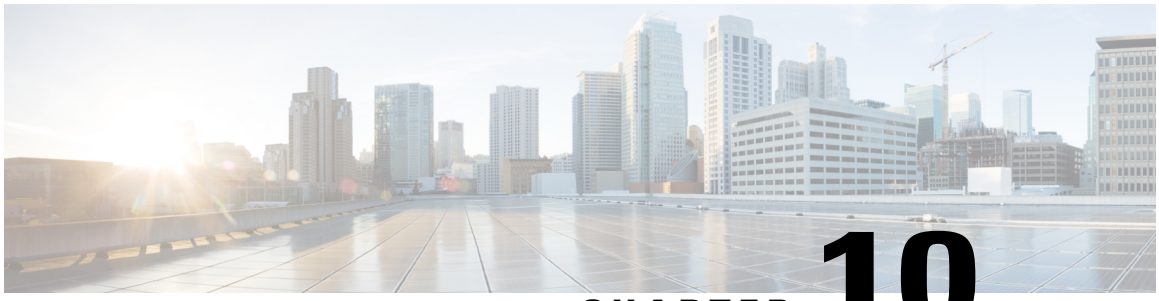
Step 4 In the **Device Information** window, choose the device with which you want to associate the user.

Step 5 Click **Save**.

Step 6 In the **Permissions Information** window, assign the user Cisco Unified Communications Manager Administration permissions.

Step 7 In the **Permissions Information** window, choose **Standard CCM End Users**.

Step 8 Click **Save** and **Apply Config**. After the device reregisters, the user is configured to the device.



CHAPTER 10

Features and Services

- Available Telephony Features, page 95
- Feature Buttons, page 105
- Set Up Feature Control Policies, page 107
- Phone Button Templates, page 108
- Configure Product-Specific Options, page 109
- Video Transmit Resolution Setup, page 120
- Instant Messaging and Presence Setup, page 121
- Application Setup, page 122
- Push Android APK Files Through Cisco Unified Communications Manager, page 123

Available Telephony Features

Cisco DX Series devices provide an integrated suite of collaborative applications, including Cisco WebEx, Cisco Unified Presence, instant messaging, email, visual voicemail, and Cisco Unified Communications Manager voice and video telephony features. These devices also support applications from Google Play.

After you install Cisco DX Series devices in your network, configure their network settings, and add them to Cisco Unified Communications Manager, you must use Cisco Unified Communications Manager Administration to configure telephony features and set up services.

Note Cisco Unified Communications Manager also provides several service parameters that you can use to configure various telephony functions. For more information about accessing and configuring service parameters, see the *Cisco Unified Communications Manager Administration Guide*. For more information about the functions of a service, click on the name of the parameter or the question mark help button in the **Service Parameter Configuration** window.

Agent Greeting

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

For more information, see:

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

Enable Agent Greeting

Procedure

Step 1 Select **Device** > **Phone**.

Step 2 Locate the device that you want to configure.

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

Step 4 Choose **Save**.

Step 5 Check the setting of the bridge:

a) Choose **System** > **Service Parameters**.

b) Select the appropriate Server and Service.

c) Scroll to the Clusterwide Parameters (Device - Phone) pane and set **Builtin Bridge Enable** to On.

d) Choose **Save**.

All Calls

Allows a user to view a list of active and held calls; this list is sorted in chronological order (oldest first). The user can also view a list of incoming and completed calls; this list is sorted newest to oldest.

All Calls on Primary Line

Allows the primary line to assume the All Calls functionality. All incoming calls display in the primary line call list and can be answered on the primary line.

AutoAnswer

Connects incoming calls automatically after a ring or two. AutoAnswer works with either the speakerphone or the headset. If AutoAnswer for headset is enabled for a device, but no headset is connected to the device, the device will not automatically answer any calls.

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

Auto Dial

Allows the user to choose from matching numbers in the Recent Call History, which includes placed, received, and missed calls. To place the call, the user can choose a number from any of these call lists or continue to enter digits manually.

Barge

Allows a user to join a nonprivate call on a shared phone line. Barge adds a user to a call and converts the call into a conference. The user and other parties can then access conference features.

Note Users can still use Barge if the Built In Bridge Enable service parameter is set to Off. To prevent a user from using the Barge feature on a device, you must disable Barge in the Feature Control Policy for the device.

For more information, see:

- *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Setup" chapter
- *Cisco Unified Communications Manager System Guide*, "Cisco Unified IP Phones" chapter
- *Features and Services Guide for Cisco Unified Communications Manager*, "Barge and Privacy" chapter
- *Cisco Unified Communications Manager Administration Guide*, "Feature Control Policy Setup" chapter

Busy Lamp Field

Allows a user to monitor the call state of a directory number that is associated with a speed-dial button, call log, or directory listing on the device.

For more information, go to the "IM and Presence Service" chapter in the *Features and Services Guide for Cisco Unified Communications Manager*.

Call Forward

Allows users to redirect incoming calls to another number. Call forward options include Call Forward All, Call Forward Busy, Call Forward No Answer, and Call Forward No Coverage.

Additional options include:

- Allow calls that are placed from the target number to ring through rather than be forwarded.
- Prevent a call-forward loop from exceeding the maximum number of links in a call-forwarding chain.

Call forward options can be assigned on a per-line basis.

For more information, see:

- *Cisco Unified Communications Manager Administration Guide*, “Directory Number Setup” chapter.
- *Cisco Unified Communications Manager System Guide*, “Cisco Unified IP Phones” chapter.

Calling Line Identification

Allows a user to enable the full, external number to be used for calling line identification.

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

Calling Line Identification Presentation

Allows a user to enable or restrict the originating caller number on a case-by-case basis.

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

Cisco Extension Mobility

Allows users to temporarily access their device configuration, such as line appearances, services, and speed dials, from a shared device through login to the Cisco Extension Mobility service on that device.

Cisco Extension Mobility can be useful if users work from a variety of locations within your company or if they share a workspace with coworkers.

Note This feature is not supported for DX Series devices that are deployed with Mobile and Remote Access through Expressway.

To log in to a device, the user enters extension mobility credentials that the administrator supplies. These credentials differ from the user Screen Lock PIN.

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

Extension Mobility Multi-User

The extension mobility multi-user feature uses the extension mobility login/logout process. When the user logs in, the Cisco Unified Communications Manager server authenticates the user credentials; the server uses the same messaging scheme as the extension mobility feature.

When user A logs in to a device for the first time, the device goes through a reboot cycle and creates a user partition for user A on the device. The device presents user A with the Setup Wizard. User A gets dedicated space for personal apps and data, and the Call application works as it does on any Cisco DX Series device. After initial login, user A configures any app-related settings. When user A logs out from this device, the user settings are saved for the next time that user A logs in to the device.

When user A logs out from the device, user B can log in to the device with user B credentials. User B has the same experience upon obtaining the user B partition: for the first login, the Setup Wizard prompts user B to set up personal apps and data, and user B also has a Call application that works as usual on a Cisco DX Series device.

Partitions are completely separate, so that any user can never see the data of any other user.

Extension mobility multi-user offers an enterprise multi-user approach: the system administrator decides which devices are configured for extension mobility multi-user, and provides credentials for those users that can log in to a particular device. With proper credentials, users can log in only to a particular device and configure their own accounts, which includes removal of their own accounts. Users cannot modify the accounts of other users on the same device.

An algorithm limits the number of users that can log in to a particular device. The maximum number of users on a device depends on the usage of each user. When the flash memory on the device drops below a certain quotient, the account of the least recently logged in user is deleted to create space for a new user to log in. Thus, a new user never fails to log in due to lack of space on the device.

Set Up Cisco Extension Mobility

Perform the procedures in the order shown in the following steps to configure Cisco Extension Mobility for DX Series devices.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Device Profile** and click **Add New**.

a) Enter the Device Type.
b) Enter the Device Profile Name, and click **Save**.
c) Enter the directory numbers and required information and click **Save**.

Step 2 Choose **User Management** > **End User** and select or create a user.

a) In Extension Mobility Available Profiles, choose the user device profile and click the down arrow; this places the service that you chose in the Controlled Profiles box.
b) Click **Save**.

Step 3 Choose **Device** > **Phone**.

a) Choose your device type.
b) Select a user ID.
c) In the Product Specific Configuration Layout area of the **Phone Configuration** window, in Extension Information, check **Enable Extension Mobility**.
d) In the Product Specific Configuration Layout area of the **Phone Configuration** window, choose the **Enabled** value for the Multi-User drop-down list box.

Cisco Mobility

Enables users to manage business calls by using a single phone number and pick up in-progress calls on the desktop phone and a remote device, such as on a mobile phone. Users can restrict the group of callers according to phone number and time of day.

Cisco Mobility for Cisco DX Series devices requires Cisco Unified Communications Manager Release 9.0(1) or later.

For more information, see the "Cisco Mobility" chapter in the *Features and Services Guide for Cisco Unified Communications Manager*

Conference

- Allows a user to talk simultaneously with multiple parties; to do so, the feature calls each participant individually.
- Allows any participant in a standard (ad hoc) conference to add or remove participants.
- Allows users to join two or more calls that are on one line to create a conference call and remain on the call.

The service parameter Advanced Adhoc Conference (disabled by default in Cisco Unified Communications Manager) allows you to enable these features.

For information about conferences, go to the "Conference Bridges" chapter in the *Cisco Unified Communications Manager System Guide*.

Secure Conference

Secure Conference allows secure devices to place conference calls through use of a secure conference bridge. As new participants are added, the Secure Call icon is displayed as long as all participants use secure devices.

For additional information, see:

- *Cisco Unified Communications Manager System Guide*, "Conference Bridges" chapter
- *Cisco Unified Communications Manager Administration Guide*, "Conference Bridge Setup" chapter
- *Cisco Unified Communications Manager Security Guide*

Divert

After Enhanced Immediate Divert is enabled, the feature allows users to divert incoming calls directly to their voice messaging system.

For more information about diverting calls to voicemail, see the "Immediate Divert" chapter in the *Features and Services Guide for Cisco Unified Communications Manager*.

For more information about Enhanced Immediate Divert, see the "Cisco Unified IP Phones" chapter in the *Cisco Unified Communications Manager System Guide*.

Do Not Disturb

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

Note DND does not affect 911 calls.

The following DND-related parameters are configurable in Cisco Unified Communications Manager Administration:

- Do Not Disturb - This check box allows you to enable DND on a per-device basis. In Cisco Unified Communications Manager Administration, choose **Device** > **Phone** > **Phone Configuration**.
- DND Incoming Call Alert - Choose the type of alert to play, if any, on a device for incoming calls when DND is active. This parameter is located in both the **Common Phone Profile** window and the **Phone Configuration** window. (The **Phone Configuration** window value takes precedence.)

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

Gateway Recording

This feature directs the Media Gateway to send the call to the recording server and thus improve call monitoring.

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

Hold Status

Enables devices with a shared line to distinguish between the local and remote lines that placed a call on hold.

Hold and Resume

Allows the user to move a connected call from an active state to a held state.

Music on Hold

Plays music while callers are on hold.

For more information, see the "Music On Hold" chapter in the *Features and Services Guide for Cisco Unified Communications Manager*.

Ignore

Allows a user to ignore an incoming call from the notification window.

Message Waiting Indicator

A light on the handset indicates that a user has one or more new voice messages.

For more information, see:

- *Cisco Unified Communications Manager Administration Guide*, "Message Waiting Setup" chapter
- *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Unified Communications Manager" chapter

Mute

Mutes the audio input for all input devices, including device speakers, handset, and headsets.

Plus Dialing

Allows the user to dial E.164 numbers prefixed with a + sign.

To dial the + sign, the user needs to press and hold the * key for at least 1 second. This applies only to dialing the first digit for an on-hook or off-hook call.

Protected Calling

Provides a secure (encrypted) connection between two devices. A security tone is played at the beginning of the call to indicate that both devices are protected. Some features, such as conference calling, shared lines, and Join Across Lines are not available when protected calling is configured. Protected calls are not authenticated.

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

Ringtone Setting

Identifies ring type used for a line when the device has another active call.

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

Ringtone

Users can customize how their device indicates an incoming call and a new voice message.

Secure and Nonsecure Indication Tone

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

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

Only protected devices hear these secure or nonsecure indication tones. (Nonprotected devices never hear tones.) If the overall call status changes during the call, the indication tone changes accordingly. At that time, the protected device plays the appropriate tone.

A protected device plays or does not play a tone under these circumstances:

- After the option to play the tone is enabled, Play Secure Indication Tone option is enabled (True):
  - When end-to-end secure media is established and the call status is secure, the device plays the secure indication tone (three long beeps with pauses).
  - After end-to-end nonsecure media is established and the call status is nonsecure, the device plays the nonsecure indication tone (six short beeps with brief pauses).
- If the Play Secure Indication Tone option is disabled, no tone plays.

Serviceability

Allows administrators to gather debug information quickly and easily from devices.

This feature uses SSH to access each phone remotely. SSH must be enabled on each phone for this feature to function.

Shared Line

Allows a user to have multiple devices that share the same directory number or allows a user to share a directory number with a coworker.

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

Speed Dial

Allows a user to configure speed dial to a specific destination directory number.

Transfer

Allows users to redirect connected calls from their device to another number.

The user can connect two calls to each other. The user can remain on the line or transfer the call without staying on line.

Uniform Resource Identifier Dialing

The Uniform Resource Identifier (URI) Dialing feature allows the user to place calls by using an alphanumeric URI address as a directory number, for example, bob@cisco.com. The user must enter the URI address to select the contact.

The screen displays the call information for the URI call. The call logs record the URI call information in the Call History and the Details page.

For more information, see *Features and Services Guide for Cisco Unified Communications Manager*.

Video Toggle

Users can toggle video off or on during video calls.

Voice Messaging System

Enables callers to leave messages if calls are unanswered.

For more information, see:

- *Features and Services Guide for Cisco Unified Communications Manager*
- *Cisco Unified Communications Manager System Guide*, "Voice Mail Connectivity to Cisco Unified Communications Manager" chapter

Set Up Visual Voicemail

Visual Voicemail is configured for all devices or to an individual user or group of users from Cisco Unified Communications Manager Administration. Use the following procedure to configure Visual Voicemail for all devices.

Procedure

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

Step 2 Choose **Find** and choose **Standard Common Phone Profile**.

Step 3 In the **Product Specific Configuration Layout** window, enter the following information in the **Voicemail Server (Primary)** field:

- If you are configuring for Cisco Unified IP Phone standalone configuration, enter the fully qualified domain name of the Cisco Unified IP Phone system.
- If you are configuring for Cisco Unified IP Phone failover configuration, enter the DNS alias of the Cisco Unified IP Phone system.

Step 4 Save changes and click **Apply Config**.
For more information about configuration and synchronization of Visual Voicemail, see the "Voice-Mail Profile Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide*.

Set Up Visual Voicemail for Specific User or Group

Use the following procedure to configure Visual Voicemail for a specific user or group of users.

Procedure

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

Step 2 Choose the device that associates with the user you are searching for.

Step 3 In the **Product Specific Configuration Layout** window, enter the following information in the **Voicemail Server (Primary)** field:

- If you are configuring for Cisco Unified IP Phone standalone configuration, enter the fully qualified domain name of the Cisco Unified IP Phone system.
- If you are configuring for Cisco Unified IP Phone failover configuration, enter the DNS alias of the Cisco Unified IP Phone system.

Step 4 Save changes and click **Apply Config**.

Step 5 Choose **Reset** and **Restart** to deliver the new settings to the device.

Step 6 To allow secure messages on the device, from Cisco Unified Communications Manager Administration, choose **System Settings** > **Advanced API Configuration** and enable both **Allow Access to Secure Message Recordings through CUMI** and **Allow Message Attachments through CUMI**.

Step 7 To configure Cisco Unified Communications Manager so that directory photos are configured in Visual Voice Mail, choose **Device** > **Device Settings** > **Common Phone Profile**, choose a Common Phone Profile, and enter the URL for your organization's photo directory in the **Company Photo Directory** field.
For more information about configuration and synchronization of Visual Voicemail, see the "Voice-Mail Profile Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide*.

Feature Buttons

The following table provides information about features that are available on the call control bar, and features that you need to configure as programmable feature buttons. An "X" in the table indicates that the feature is

supported for the corresponding button type. Of the two button types, only programmable feature buttons require configuration in Cisco Unified Communications Manager administration.

Table 19: Features and Corresponding Buttons

Feature Name	Call Control Bar Button	Programmable Feature Button
Call Back		X
Call Forward	X	
Call Forward All		X
Call Park	X	
Call Pickup		X
Cisco Mobility		X
Conference (Add)	X	
Divert		X
Do Not Disturb		X
End Call	X	
Group Pickup		X
Hold	X	
Hunt Group		X
Intercom		X
Malicious Call Identification (MCID)		X
Meet Me		X
Privacy		X
Redial		X
Share (DX70 & DX80 only)	X	
Speed Dial		X
Stop Video		X
Transfer	X	

Set Up Feature Control Policies

You can limit the appearance of some telephony features on Cisco DX Series devices by enabling or disabling these features in the feature control policy configuration. If you disable a feature in the feature control policy configuration, you restrict user access to the feature.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Feature Control Policy**.
The **Find and List Feature Control Policy** window appears.

Step 2 Click **Add New** to define a set of policies.

Step 3 Enter the following settings:

- Name - Enter a name for a new Feature Control Policy.
- Description - Enter a description.
- Feature Control Section - Check the check box for the features for which you want to change the default setting.

Step 4 Click **Save**.

Step 5 Apply the policy to Cisco DX Series devices by including it in the following settings:

- Enterprise Parameters Configuration - Applies to all Cisco DX Series devices in the system.
- Common Phone Profile Configuration - Applies to all Cisco DX Series devices in a group.
- Phone Configuration - Applies to an individual Cisco DX Series device.

Feature Control Policy Default Values

The following table shows the list of features that you can configure, and the default value.

Table 20: Feature Control Policy Default Values

Feature	Default value
Barge	Enabled
Call Back	Enabled
Call PickUp	Disabled
Conference List	Enabled

Feature	Default value
Divert (Alerting)	Disabled
Divert (Connected)	Disabled
Forward All	Enabled
Group Call PickUp	Disabled
Meet Me	Disabled
Mobility	Disabled
Other Call PickUp	Disabled
Park	Disabled
Redial	Enabled
Report Caller	Disabled
Report Quality	Disabled
Speed Dial	Enabled

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

Phone Button Templates

Phone button templates let you assign speed dials and call-handling features to programmable buttons.

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

Modify Phone Button Templates

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

Procedure

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

Step 2 Click **Find**.

Step 3 Choose the device model.

Step 4 Choose **Copy**, enter a name for the new template, and choose **Save**.

The **Phone Button Template Configuration** window opens.

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

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

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

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

Step 9 Click **Save** to store the change and then click **Reset** to implement the change.
The user can now access the Self Care Portal and associate the service with a button on the device.

Configure Product-Specific Options

Cisco Unified Communications Manager Administration allows you to set some product-specific configuration parameters for devices in any of the following windows:

- **Enterprise Phone Configuration** window (**System** > **Enterprise Phone Configuration**)
- **Common Phone Profile window** (**Device** > **Device Settings** > **Common Phone Profile**), in the Product Specific Configuration Layout portion of window
- **Device Phone Configuration** window (**Device** > **Phone** > **Add New** > **Cisco DX650, Cisco DX70, or Cisco DX80**), in the Product Specific Configuration Layout area of window

The following table shows the product-specific configuration options.

Table 21: Cisco DX Series Product-Specific Configuration Options

Feature	Description
Disable Speakerphone	Disables only the speakerphone functionality. Disabling speakerphone functionality does not affect the headset. You can use lines and speed dials with headset/handset. Default: False
Disable Speakerphone and Headset	Disables all speakerphone functions and the headset microphone. Default: False
Disable USB	Disables the USB ports on the device. Default: False
SDIO	Indicates whether the SDIO device on the device is enabled or disabled. Default: Disabled
Bluetooth	Indicates whether the Bluetooth service on the device is enabled or disabled. Default: Enabled

Feature	Description
Allow Bluetooth Contacts Import	Allows the user to import and sync contacts and call history from their Bluetooth device. Default: Enabled
Allow Bluetooth Mobile Handsfree Mode	Allows the user to use their mobile phone line on the desk phone. Default: Enabled
Days Display Not Active	Allows the user to specify the days that the backlight is to remain off by default. Default: Typically Saturday and Sunday for U.S. corporate customers. **Note** The list contains all of the days of the week. To turn off backlight on Saturday and Sunday, hold down Control and choose Saturday and Sunday.
Display On Time	Indicates the time of day the display is to automatically turn itself on for days that are listed in the off schedule. Default: 07:30 Maximum length: 5 **Note** Enter value in a 24-hour format, where 00:00 is the beginning of the day and 23:59 is the end of the day.
Display On Duration	Indicates the amount of time the display is to be active when it is turned on by the programmed schedule. Default: 10:30 Maximum length: 5 **Note** Maximum value is 24 hours. This value is in hours and minutes format. For example, “01:30” activates the display for 1 hour and 30 minutes.
Display On When Incoming Call	When the device is in screen saver mode, this setting turns the display on when a call is ringing. Default: Enabled

Feature	Description
Enable Power Save Plus	To enable the Power Save Plus feature, select the day(s) that you want the device to power off on schedule. You can select multiple days by pressing and holding the Control key while clicking on the days that you want Power Save Plus to operate. In Power Save Plus mode, enough power is maintained to illuminate one key. All other functions of the device are turned off. Power Save Plus mode turns off the device for the time period specified in the Phone On Time and Phone Off Time fields. This time period is usually outside of your organization's regular operating hours. The illuminated key allows a user to press it to restore full power to the device. After pressing the illuminated key, the phone power-cycles and reregisters with Unified CM before it becomes fully operational. When you select day(s) in this field, the following notice displays to indicate e911 concerns. By enabling Power Save Plus, you are agreeing to the terms specified in this Notice. While Power Save Plus Mode is in effect, endpoints configured for the mode are disabled for emergency calling and from receiving inbound calls. By selecting this mode, you agree to the following: **1** You are taking full responsibility for providing alternate methods for emergency calling and receiving calls while the mode is in effect. **2** Cisco has no liability in connection with your selection of the mode and all liability in connection with enabling the mode is your responsibility. **3** You will fully inform users of the effects of the mode on calls, calling and otherwise. Default: No days selected
Phone On Time	This field determines the time that the device turns on automatically on the days that are selected in the Enable Power Save Plus list box. Enter the time in 24 hour format, where 00:00 represents midnight. For example, to automatically turn the phone on at 7:00 a.m., (0700), enter 07:00. To turn the phone on at 2:00 p.m. (1400), enter 14:00.If this field is blank, the device automatically turns on at 00:00. Default: 0:00 Maximum length: 5
Phone Off Time	This field determines the time of day that the device will turn itself off on the days that are selected in the Enable Power Save Plus list box. Enter the time in the following format hours:minutes. If this field is blank, the device automatically turns off at midnight (00:00). **Note** If Phone On Time is blank (or 00:00) and Phone Off Time is blank (or 24:00), the device will remain on continuously, effectively disabling the Power Save Plus feature unless you allow EnergyWise to send overrides. Default: 24:00 Maximum length: 5

Feature	Description
Phone Off Idle Timeout	This field represents the number of minutes that the device must be idle before the device will request the power sourcing equipment (PSE) to power down the device. The value in this field takes effect: • When the device was in Power Save Plus mode as scheduled and was taken out of Power Save Plus mode because the user pressed a key • When the device is repowered by the attached switch • When the Phone Off Time is met but the device is in use. The unit is minutes. The default is 60. The range is 20 to 1440.
Enable Audible Alert	This checkbox, when enabled, instructs the device to play an audible alert ten minutes prior to the time specified in the field, Phone Off Time. The default is disabled. This checkbox only applies if the Enable Power Save Plus list box has one or more days selected.
EnergyWise Domain	This field defines the EnergyWise domain in which the phondevice is participating. An EnergyWise domain is required by the Power Save Plus feature. If you have chosen days in the Enable Power Save Plus list box, you must also provide an EnergyWise domain. The default is blank. Maximum length: 127
EnergyWise Endpoint Security Secret	This field defines the password (shared secret) used to communicate within the EnergyWise domain. An EnergyWise domain and secret is required by the Power Save Plus feature. If you have chosen days in the Enable Power Save Plus list box, you must also provide an EnergyWise domain and secret. The default is blank. Maximum length: 127
Allow EnergyWise Overrides	This checkbox determines whether you will allow the EnergyWise domain controller policy to send power level updates to the phones. A few conditions apply; first, one or more days must be selected in the Enable Power Save Plus field. If the Enable Power Save Plus list box does not have any days selected, the device will ignore the EnergyWise directive to turn off the device. Second, the settings in Unified CM Administration will take effect on schedule even if EnergyWise sends an override. For example, assume the Display Off Time is set to 22:00 (10 p.m.), the value in the Display On Time field is 06:00 (6 a.m.), and the Enable Power Save Plus has one or more days selected. If EnergyWise directs the device to turn off at 20:00 (8 p.m.), that directive will remain in effect (assuming no user intervention occurs) until the configured Phone On Time at 6 a.m. At 6 a.m., the device will turn on and resume receiving its power level changes from the settings in Unified CM Administration. To change the power level on the device again, EnergyWise must reissue a new power level change command. Also, any user interaction will take effect so if a user presses a key after EnergyWise has directed the device to power off, the device will power on as a result of the user action. The default is unchecked.

Feature	Description
Recording Tone	This can be used to configure whether the recording tone is enabled or disabled on the device. Default: Disabled
Recording Tone Local Volume	This can be used to configure the loudness setting of the recording tone that the local party hears. This loudness setting applies regardless of the actual device used for hearing (handset, speakerphone, headset). The loudness setting should be in the range of 0% to 100%, with 0% being no tone and 100% being at the same level as the current volume setting. The default value is 100%.
Recording Tone Remote Volume	This can be used to configure the loudness setting of the recording tone that the remote party hears. The loudness setting should be in the range of 0% to 100%, with 0% being less than -66dBM and 100% being -4dBM. The default value is -10dBM or 50%.
Recording Tone Duration	Indicates the length of time in milliseconds for which the recording tone is inserted in the audio stream. The default for this parameter is set to the value in the Network locale file for this field. The valid range for this parameter is a value between 1 and 3000 milliseconds.
Advertise G.722 and iSAC Codecs	Indicates whether the Call application advertises the wideband codecs to the Cisco Unified Communications Manager. Codec negotiation involves two steps: 1 The Call application must advertise the supported codecs to Cisco Unified Communications Manager. 2 When Cisco Unified Communications Manager gets the list of supported codecs from all devices that are involved in the call attempt, it chooses a commonly supported codec based on various factors, including the region pair setting. Use System Default Valid values: • System Default - Call application defers to the setting that is specified in the enterprise parameter, Advertise G.722 and iSAC Codecs. • Disabled - Call application does not advertise the wideband codecs to Cisco Unified Communications Manager. • Enabled - Call application advertises the wideband codecs to Cisco Unified Communications Manager.
Video Calling	When enabled, indicates that the device will participate in video calls. Default: Enabled

Feature	Description
Device UI Profile	Changes the device user interface characteristics to optimize for specific user personas such as basic video callers (Simple mode) or general collaboration users (Enhanced). Default: Simple
Wifi	Indicates whether the Wi-Fi on the device is enabled or disabled. **Note** For the Enterprise and Common settings, the Wifi parameter is set at the default value (Enabled) and the **Override Common Settings** check box is checked. **Note** For the Device setting, the Wifi parameter is left at the default value (Enabled) but without the **Override Common Settings** check box checked. **Tip** Cisco recommends that you create a new common phone profile for devices with Wifi parameter set to Enabled if the deployment environment default setting at the enterprise and common level is Disabled, unless it is company policy to set the Wifi default to Disabled for all devices. Default: Enabled
PC Port	Indicates whether the PC port is enabled or disabled. Default: Enabled
Span to PC Port	Indicates whether the device will forward packets that are transmitted and received on the PC port. **Note** Choose **Enabled** if an application is running on the PC port that requires monitoring of the device traffic, such as monitoring and recording applications or network packet-capture tools that are used for diagnostic purposes. To use this feature, PC Voice VLAN access must be enabled. Default: Disabled
PC Voice VLAN Access	Indicates whether a device that is attached to the PC port is allowed access to the Voice VLAN. **Note** Disabling Voice VLAN Access prevents the attached PC from transmission and receipt of data on the Voice VLAN. It also prevents the PC from receiving data sent and received by the device. Default: Enabled
PC Port Remote Configuration	Allows remote configuration of the PC port speed and duplex of the device. Default: Disabled
Switch Port Remote Configuration	Allows remote configuration of the switch port speed and duplex of the device. This overrides any manual configuration on the device. Default: Disabled

Feature	Description
Detect Unified CM Connection Failure	This field determines the sensitivity that the phone has for detecting a connection failure to Cisco Unified Communications Manager (Unified CM), which is the first step before device failover to a backup Unified CM/SRST occurs. Valid values specify Normal (detection of a Unified CM connection failure occurs at the standard system rate) or Delayed (detection of a Unified CM connection failover occurs approximately four times slower than Normal). For faster recognition of a Unified CM connection failure, choose Normal. If you prefer failover to be delayed slightly to give the connection the opportunity to reestablish, choose Delayed. Note that the precise time difference between Normal and Delayed connection failure detection depends on many variables that are constantly changing. This only applies to the wired Ethernet connection. Default: Normal
Gratuitous ARP	Indicates whether the device will learn MAC addresses from Gratuitous ARP responses. **Note** Disabling the device ability to accept Gratuitous ARP prevents applications that use this mechanism for monitoring and recording of voice streams from working. Default: Disabled
Cisco Discovery Protocol (CDP): Switch Port	Allows administrator to enable or disable CDP on the switch port. **Warning** Disable CDP on the network port only if the device connects to a non-Cisco switch. For more details, see the *Cisco Unified Communications Manager Administration Guide*. Default: Enabled
Cisco Discovery Protocol (CDP): PC Port	Indicates whether CDP is supported on the PC port. Default: Enabled
Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port	Allows administrator to enable or disable Link Layer Discovery Protocol (LLDP-MED) on the switch port. Default: Enabled
Link Layer Discovery Protocol (LLDP): PC Port	Allows administrator to enable or disable Link Layer Discovery Protocol (LLDP) on the PC port. Default: Enabled
LLDP Asset ID	Allows administrator to set Asset ID for Link Layer Discovery Protocol. Maximum length: 32
LLDP Power Priority	Allows administrator to set Power Priority for Link Layer Discovery Protocol. Default: Unknown

Feature	Description
Power Negotiation	Allows administrator to enable or disable Power Negotiation. **Note** Enable the Power Negotiation feature when the device is connected to a switch that supports power negotiation. However, if a switch does not support power negotiation, disable the Power Negotiation feature before you power up accessories over PoE+. Default: Enabled
Automatic Port Synchronization	Enables the phone to synchronize the PC and SW ports to the same speed and to duplex. Only ports configured for auto negotiate change speeds. Default: Disabled
802.1x Authentication	Specifies the 802.1x Authentication feature status. Options: • Enabled - The device uses 802.1X authentication to request network access. • Disabled - Default setting in which the device uses CDP to acquire VLAN and network access. Default: User controlled
Always On VPN	Indicates whether the device always starts the VPN AnyConnect client and establishes a connection with the configured VPN profile from Cisco Unified Communications Manager. Default: False
Store VPN Password on Device	This parameter controls whether VPN password can be stored on the device. Its value is used only when Password Persistence is set to true. If disabled, the user's VPN password is stored in memory and is automatically re-submitted upon subsequent connects. However, when the device reboots, the user will have to re-enter their VPN password again. If enabled, the user's VPN password is stored on the device and will persist across reboots. Default: False
Allow User-Defined VPN Profiles	Controls whether the user can use the AnyConnect VPN client to create VPN profiles. If disabled, the user cannot create VPN profiles. Default: True
Require Screen Lock	Indicates whether screen lock is required on the device. Options: • User controlled. • PIN - A numeric password that is at least four digits long. • Password - An alphanumeric password, which consists of at least four alphanumeric characters, one of which must be a non-numeric character, and one must be a capital letter. Default: PIN

Feature	Description
Maximum Screen Lock Timeout	Indicates maximum idle time in seconds before the device automatically locks the screen. After the screen is locked, the user password is required to unlock it. Default: 600 Minimum: 15 Maximum: 1800
Enforce Screen Lock During Display-On Time	This parameter provides an unobtrusive lock policy that allows users to work freely with their device throughout the workday, without the device locking after the interval that is set in Cisco Unified Communications Manager. After work, the device locks as defined in the policy, to prevent unauthorized users from accessing it. The device always supports the user-controlled manual lock option (power button), for meetings or lunch breaks. The device remains locked until the user enters the PIN/password on next use. ON - Device locks during the workday or during display-on time (default setting). OFF - Device locks only during display-off time or after work hours, based on day/time settings listed above. Default: True **Note** Disabling this parameter overrides all third-party device administration policies that are installed on the device that relate to lock screen timeout.
Lock Device During Audio Call	When the device is in a charging state and an active voice call is in progress, an administrator can override the screen lock PIN enforcement timer to keep the screen active during an audio call. Screen lock timer takes effect after audio call is completed and timer is exceeded. Default: Disabled
Kerberos Server	Authentication server for web proxy Kerberos. Maximum length: 256
Kerberos Realm	Authentication realm for web proxy Kerberos. Maximum length: 256
Load Server	Indicates that the device will use an alternative server to obtain firmware loads and upgrades, rather than the defined TFTP server. Default: Hostname or the IP address of local server Maximum length: 256
Peer Firmware Sharing	Enables or disables Peer to Peer image distribution in order to allow a single device in a subnet to retrieve an image firmware file and then distribute it to its peers. Default: Enabled
Log Server	Specifies an IP address and port of a remote system to which log messages are sent. Default: IP address of remote system Maximum length: 32

Feature	Description
Log Profile	Run the pre-defined debug command remotely. Default: Preset
Web Access	Indicates whether the device accepts connections from a web browser or other HTTP client. Default: Disabled
SSH Access	This parameter indicates whether the device accepts SSH connections. Disabling the SSH server functionality of the device will block access to the device. Default: Disabled
Android Debug Bridge (ADB)	Enables or disables the ADB on the device. Can be set to Enabled, Disabled, or User Controlled. Default: Disabled
Multi-User	Indicates whether multi-user is enabled or disabled on the device. Default: Disabled
Allow Applications from Unknown Sources	Controls whether the user can install Android applications on the device from a URL or from Android application package files (APK) that are received through email, through instant message (IM), or from a Secure Digital (SD) card. Can be set to Enabled, Disabled, or User Controlled. Default: Disabled
Allow Applications from Google Play	Controls whether the user can install Android applications from Google Play. **Note** Some applications that are found in Google Play may have hardware requirements that are not available on Cisco DX Series devices, such as GPS or a rear-facing camera. Cisco cannot guarantee that an application that is downloaded from a third-party site will work. Default: False
Enable Cisco UCM App Client	Controls whether the Application Client runs on the device. When the Application Client is enabled, users can select the applications they want to install from Cisco Unified Communications Manager. Default: False
Background Image	This parameter specifies the default wallpaper file. Only the administrator disables end user access to phone wallpaper list, could this parameter take effect. Maximum length: 64

Feature	Description
Company Photo Directory	Specifies the URL that the device can query for a user and get the image that is associated with that user. Example: http://www.cisco.com/dir/photo/zoom/%%uid%%, where uid is employee user ID. Default: Photo directory URL Maximum length: 256
Voicemail Server (Primary)	Hostname or IP address of the primary visual voicemail server. Default: IP address of primary visual voicemail server Maximum length: 256
Voicemail Server (Backup)	Hostname or IP address of the backup visual voicemail server. Default: IP address of backup visual voicemail server Maximum length: 256
Presence and Chat Server (Primary)	Hostname or IP address of the primary presence server. Default: IP address of primary presence server Maximum length: 256
Presence and Chat Server Type	Specifies the type of secondary presence and IM server for the device to use. Can be set to Cisco Unified Presence or Cisco WebEx Connect. Default: Cisco WebEx Connect
Presence and Chat Single Sign-On (SSO) Domain	The enterprise domain that Cisco WebEx Connect Cloud uses to perform Single Sign-On (SSO) authentication against an enterprise. Default: Empty field Maximum length: 256
Multi-User URL	This parameter specifies the URL of the extension mobility server. Maximum length: 256
User Credentials Persistent for Expressway Sign In	This parameter controls whether Expressway credentials can be stored on the device. Default: Disabled
Customer support upload URL	This sets a server address to which the user can send problem report files from the 'Problem Reporting Tool' on the endpoint. Maximum length: 256

Note For additional configuration information, see the *Cisco DX Series Wireless LAN Deployment Guide*.

Override Common Settings Check Box

After you set the parameters, check the Override Common Settings check box for each setting you wish to update. If you do not check this check box, the corresponding parameter setting does not take effect. If you set the parameters at the three configuration windows, the setting takes precedence in the following order:

1 **Phone Configuration** window

2 **Common Phone Profile** window

3 **Enterprise Phone Configuration** window

Video Transmit Resolution Setup

Cisco DX Series devices support video calling through a high-resolution multitouch color LCD and integrated camera. For the device to send and receive video, the video capability must be enabled in Cisco Unified Communications Manager.

Note When the Video Calls option is set to Off, the Auto Transmit Video setting is dimmed. All video settings under the Call settings menu are dimmed if Video Calling is disabled in the **Product Specific Configuration Layout** window.

Table 22: Video Transmit Resolutions and Capabilities

Video Type	Video Resolution	FPS	Video Bit Range Rate (bandwidth)	DX650 External Camera Support
240p	432 x 240	15	64-149 kbps	Yes, but the Logitech C930e uses a video resolution of 424 x 240.
240p	432 x 240	30	150-299 kbps	Yes, but the Logitech C930e uses a video resolution of 424 x 240.
360p	640 x 360	30	300-599 kbps	Yes

Video Type	Video Resolution	FPS	Video Bit Range Rate (bandwidth)	DX650 External Camera Support
480p	848 x 480	30	600-799 kbps	Yes, but the Logitech C920-C uses a video resolution of 864 x 480.
576p	1024 x 576	30	800-1299 kbps	Yes
600p	1024 x 600	30	800-3000 kbps	No
720p	1280 x 720	30	900-1999 kbps	Yes
1080p	1920 x 1080	30	2000-4000 kbps	Yes
CIF	352 x 288 (4:3)	30	64-299 kbps	Yes
VGA	640 x 480 (4:3)	30	400-1500 kbps	Yes

Note The external camera does not support some of these resolutions, such as 600p, and the minimum bit rate at which the external camera can operate is 64 kbps.

Note When a Cisco DX650 is in a call that is using the Logitech C920-C Webcam, and the remote device only supports Packetization mode 0, the maximum transmit resolution is 640x360. When Packetization mode 1 is used, the maximum transmit resolution is 1920x1080.

Note The optimal resolution over VGA for a Cisco DX Series device is w360p; for bandwidths ranging from 400 kbps to 999 kbps, the device will send w360p.

Instant Messaging and Presence Setup

Instant Messaging and Presence allows users to communicate at any time, any place, and with any device. Cisco DX Series devices support Jabber IM with either Cisco Unified Presence or WebEx back end server. For security reasons, all cloud-based IM and Presence traffic is routed through a proxy.

Instant Messaging and Presence is configured at the device, group, or enterprise levels in the **Product Specific Configuration** window for the device. Enter the hostname or IP address for the Presence and IM Server (Primary) and Presence and IM Server type.

Application Setup

Users can download applications to customize and extend the capabilities of the device. Applications are available from Google Play. Cisco Unified Communications Manager Administration provides access to applications through configuration of the following parameters (in the Product Specific Configuration Layout area of the individual device configuration window or **Common Phone Profile** window):

- Allow Applications from Unknown Sources: Controls the ability of user to install applications from sources other than Google Play.
- Allow Applications from Google Play: Controls the ability of user to install applications from Google Play.
- Enable Cisco UCM App Client: Controls the ability of administrator to push applications from Cisco Unified Communications Manager.

  UCM App is the client on the device that can be used to subscribe or unsubscribe Android applications that are created on Cisco Unified Communications Manager. This client provides the same functionality as subscribing or unsubscribing Android applications from Cisco Unified Communications Manager, but adds the convenience of doing so from the device.

Enable Cisco UCM App Client

Procedure

Step 1 In the Product Specific Configuration Layout portion of the **Device Configuration** window of a device, check the **Enable Cisco UCM App Client** check box.

Step 2 Click **Save.**

Step 3 Click **Apply Config**.
This action installs the UCM App client on the device.

After the UCM App client is installed on the device, the device user can subscribe or unsubscribe to applications that are created in Cisco Unified Communications Manager by logging in to the UCM App client.

Create End User to Log In to UCM App

The administrator must create an end user, associate the end user with the device, and assign the end user as device owner before the end user can log in to the UCM App.

Procedure

Step 1 Create an end user. (In Cisco Unified Communications Manager Administration, choose **User Management** > **End User** to create a new end user.)

Step 2 Associate the device with the end user, so that the device is displayed under Controlled Devices for the end user.

Step 3 Assign the Standard CCM End User permissions to the end user.

Step 4 In the **Device Configuration** window for the device, assign this end user in the **Owner User ID** field.

Subscribe User with UCM App

A device user uses the UCM app on the device to subscribe or unsubscribe applications that were created on Cisco Unified Communications Manager.

Procedure

Step 1 Use the end user credentials to log in to UCM App on the device.
Upon successful login, the UCM App displays all Android applications that have been created in Cisco Unified Communications Manager.

Step 2 To subscribe to an application, check the check box next to the application name.
This action triggers the download and installation of the application on the device.

Note Some applications present detailed information to the user. Upon checking the box or choosing the application, the user sees a second screen. To subscribe to these applications, check the box on the second screen and tap **Back**. This action triggers the installation.

Step 3 To unsubscribe from an application, uncheck the check box next to the application name.

Push Android APK Files Through Cisco Unified Communications Manager

To push Android APK files from Cisco Unified Communications Manager, first configure the application as a phone service and then subscribe a device to the service.

Procedure

Step 1 Extract the AndroidManifest file from the APK by using the following apktool:

http://code.google.com/p/android-apktool/

Step 2 Add the Android Service in Cisco Unified Communications Manager Administration.

Step 3 Subscribe the device to the Android Service.

Add Android Service in Cisco Unified Communications Manager Administration

Follow these steps to add an Android service in Cisco Unified Communications Manager Administration.

Before You Begin

Use this procedure after you extract an AndroidManifest file from an APK.

Procedure

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

Step 2 Click **Add New**.

Step 3 In the **Service Name** field, enter a name that matches the package name from the AndroidManifest file that you extracted from the APK.

Step 4 In the **Service Category** drop-down list box, choose **Android APK**.

Step 5 Other fields in this window are optional: you may enter information that you see in the AndroidManifest file.

Step 6 Check the **Enable** check box.

Step 7 Click **Save**.

Subscribe Device to Android Phone Service

Before You Begin

You must add an Android phone service in Cisco Unified Communications Manager Administration before you can subscribe a device to that phone service.

Procedure

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

Step 2 In the **Find and List Phone** window that is displayed, find the device to subscribe to the Android phone service.

Step 3 Click the Device Name entry for the device that you choose.

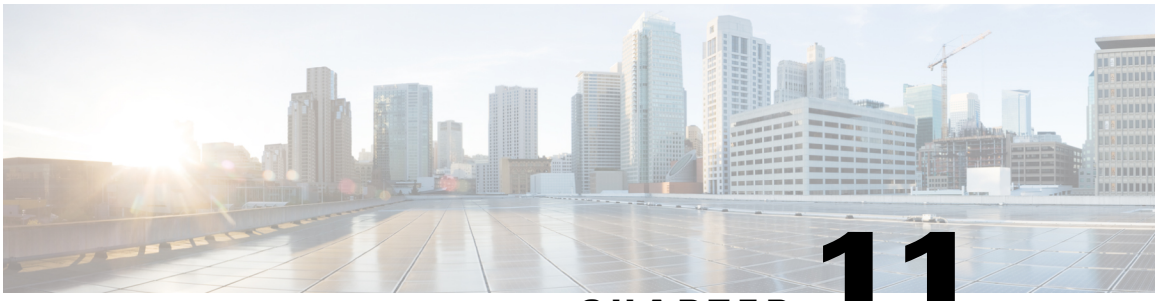
Step 4 In the **Phone Configuration** window for the device, choose **Subscribe/Unsubscribe Services** from the **Related Links** drop-down list box.

The Subscribed Cisco IP Phone Services for <device name> window opens.

Step 5 In the Subscribed Cisco IP Phone Services window for the device, use the **Select a service** drop-down list box to choose the service that you created.
This action triggers subscription of the device to the service that you specify.

Step 6 Click **Next**.

Step 7 Click **Subscribe**.



CHAPTER 11

Customization

- Wideband Codec Setup, page 127
- Operating Modes, page 128
- Default Wallpaper, page 129
- SSH Access, page 130
- Unified Communications Manager Endpoints Locale Installer, page 131
- International Call Logging Support, page 131

Wideband Codec Setup

By default, the G.722 codec is enabled for Cisco DX Series devices. If Cisco Unified Communications Manager is configured to use G.722 and if the far endpoint supports G.722, the call uses the G.722 codec instead of G.711 to connect.

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

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

- Advertise G.722 Codec field: From Cisco Unified Communications Manager Administration, choose **System** > **Enterprise Parameters**. The default value of this enterprise parameter is **True**, which means that all Cisco DX Series devices that register to this Cisco Unified Communications Manager advertise G.722 to Cisco Unified Communications Manager. If each endpoint in the attempted call supports G.722 in the capabilities set, Cisco Unified Communications Manager chooses that codec for the call whenever possible.
- A specific device advertises the G.722 codec: From Cisco Unified Communications Manager Administration, choose **Device** > **Phone**. The default value of this product-specific parameter is to use the value that the enterprise parameter specifies. If you want to override this on a per-device basis, choose

Enabled or **Disabled** in the Advertise G.722 Codec parameter in the Product Specific Configuration area of the **Phone Configuration** window.

Operating Modes

Cisco DX Series devices function in different modes:

- Public Mode
- Simple Mode
- Enhanced Mode

The default is Simple Mode.

The following table shows which features are available to the user in each mode.

Feature	Public Mode	Simple Mode	Enhanced Mode
Call application	Yes	Yes	Yes
Lock Screen	No	Yes	Yes
Network configuration	No	Yes	Yes
Home screen	No	Yes	Yes
Add or remove widgets and shortcuts	No	Yes	Yes
Visual Voicemail	No	Yes	Yes
Cisco User Data Service	Yes	Yes	Yes
Bluetooth	Yes	Yes	Yes
Set date and time	No	Yes	Yes
Recent applications list	No	Yes	Yes
External storage devices	No	No	Yes
Jabber IM	No	No	Yes
Android applications	No	No	Yes

Set Operating Mode

Before You Begin

We recommend that you disable Android Debug Bridge (ADB) for devices in Simple or Public Mode. Because the Email application is disabled in Simple or Public Mode, the user is unable to use the Problem Report Tool to email logs to the administrator. The logs must be collected from the serviceability web page.

Procedure

Step 1 Install the latest device packs on your Cisco Unified Communications Manager servers. See *Release Notes for Cisco DX Series* for more information on installing device packs.

Step 2 In the **Enterprise Phone Configuration** window, the **Common Phone Profile** window, or the **Phone Configuration** window, set **Device UI Profile** to the desired mode.

Step 3 Check **Override Common Settings**.
The device reboots when you switch from Enhanced Mode to Public Mode or Simple Mode. The device also reboots when you switch from Public Mode or Simple Mode to Enhanced Mode. The device does not reboot when you switch between Public Mode and Simple Mode.

Default Wallpaper

You can control whether you or the user can set the default wallpaper for a device from the Cisco Unified Communications Manager Administration page for the device. Each type of DX Series device requires a different size wallpaper image, which stretches across 5 home screens.

Assign Wallpaper Control

By default, the user is able to change the wallpaper on the device.

Procedure

Step 1 Go to **Device** > **Device Settings** > **Common Phone Profile**.

Step 2 To restrict wallpaper control to the administrator, uncheck **Enable End User Access to Phone Background Image Settings**.

Specify Default Wallpaper (DX70 and DX80)

We recommend an image resolution of 2985x1280 for Cisco DX70 and DX80 wallpaper. The devices crop the image to 2985x1080, meaning that the top and bottom 100px of a 2985x1280 image do not display on the device. The wallpaper is spread across five screens, and each screen is 1920px wide.

Procedure

Step 1 Upload the wallpaper image to the Desktops/2985x1080x24 folder on all nodes running the TFTP service.

Step 2 Restart the TFTP service on all nodes running TFTP.

Step 3 Go to the DX70 and DX80 Common Phone Profile in Cisco Unified Communications Manager administration and change the following:

a) Uncheck **Enable End User Access to Phone Background Image Setting**.
b) Enter the wallpaper image filename in **Background Image**.
c) Check **Override Common Settings**.

Step 4 Save and Apply the configuration to the common phone profile.

Step 5 Go to the phone device page and apply the configuration to the devices you want the wallpaper to be loaded on.
If you have a large network of endpoints apply the configuration to all devices, or restart the Cisco Unified Communications Manager server, so that all the endpoints get the image.

Specify Default Wallpaper (DX650)

We recommend an image resolution of 1600x1280 for Cisco DX650 wallpaper. The device crops the image to 1600x600 and the top and bottom 340px of a 1600x1280 image do not display on the device. The wallpaper is spread across five screens, and each screen is 1024px wide.

Procedure

Step 1 Upload the wallpaper image to the Desktops/1600x1280x24 folder on all nodes running the TFTP service.

Step 2 Restart the TFTP service on all nodes running TFTP.

Step 3 Go to the DX650 Common Phone Profile in Cisco Unified Communications Manager administration and change the following:
a) Uncheck **Enable End User Access to Phone Background Image Setting**.
b) Enter the wallpaper image filename in **Background Image**.
c) Check **Override Common Settings**.

Step 4 Save and Apply the configuration to the common phone profile.

Step 5 Go to the phone device page and apply the configuration to the devices you want the wallpaper to be loaded on.
If you have a large network of endpoints, apply the configuration to all devices, or restart the Cisco Unified Communications Manager server so that all the endpoints get the image.

SSH Access

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

SSH access requires you to enter two sets of credentials, in order:

1. The Secure Shell User and Secure Shell Password given in the Secure Shell Information section of Cisco Unified Communications Manager configuration
2. The debug userid and password

The **SSH Access** field is found in these windows:

- Common Phone Profile Configuration (**Device** > **Device Settings** > **Common Phone Profile**)
- Phone Configuration (**Device** > **Phone windows**)

Unified Communications Manager Endpoints Locale Installer

By default, devices are set up for the English (United States) locale. To use the devices 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 devices.

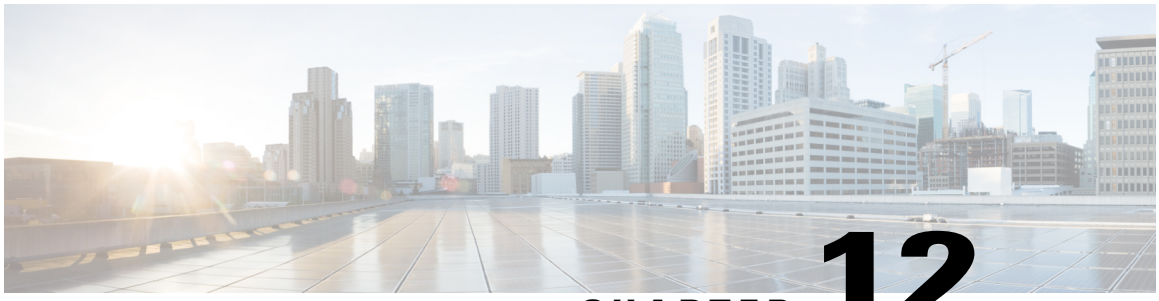
To access the Locale Installer required for a release, access http://software.cisco.com/download/navigator.html?mdfid=286037605&flowid=46245, navigate to your device model, and select the Unified Communications Manager Endpoints Locale Installer link.

For more information, see the "Locale Installer" section in the *Cisco Unified Communications Operating System Administration Guide*.

Note The latest Locale Installer may not be immediately available; continue to check the website for updates.

International Call Logging Support

If your phone system is configured for international call logging (calling party normalization), the call logs, redial, or call directory entries may display a "+" 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.



CHAPTER 12

Maintenance

- Reset Device, page 133
- Reset Options and Load Upgrades, page 135
- Remote Lock, page 135
- Remote Wipe, page 136
- Boot Alternate Image for Cisco DX70, page 136
- Boot Alternate Image for Cisco DX80, page 137
- Boot Alternate Image for Cisco DX650, page 137
- Data Migration, page 137
- Debugging Log Profiles, page 137
- User Support, page 138

Reset Device

A device reset provides a way to reset or restore various configuration and security settings or provides a way to recover the device if the device encounters an error.

The following procedure describes the types of resets that you can perform.

Note All three reset methods cause deletion of all user data and reset all settings from the device.

The following occurs on a device when you perform a reset:

- User configuration settings - Reset to default values.
- Network configuration settings - Reset to default values.
- Call histories - Get erased.
- Locale information - Reset to default values.

- Security settings - Reset to default values; this includes deletion of the CTL file and change of the 802.1x Device Authentication parameter to Disabled.

Note Do not power down the device until it completes the factory reset process.

Procedure

You can reset the device with any of these operations. Choose the operation that is appropriate for your situation.

- Method 1: Cisco Unified Communications Manager Administrator Web GUI
  1. From the Product Specific Configuration Layout area of the device configuration window, enable **Wipe Device**.
  2. Issue an Apply Config, Restart, or Reset command from the Admin GUI to push the wipe to the device.
- Method 2: Settings application
  1. In the Settings application, choose **Backup & reset** > **Factory data reset**.

     Note If a PIN or Password is configured on the device, it will need to be entered before the reset can proceed.
- Method 3: Key-press sequences

  This method should be used if the device is secured with a PIN or Password lock and the PIN/password has been lost.

  Follow these steps to reset a Cisco DX70 on boot up:

  1. Power on the device and wait for the Mute LED to blink.
  2. Press and hold the **Volume Up** button until the **Mute** button is lit red.
  3. Release the **Volume Up** button, then press and hold the **Mute** button for 3 seconds.

  Follow these steps to reset a Cisco DX80 on boot up:

  1. Press and hold the **Volume Up** button and power on the device.
  2. Release the **Volume Up** button when the **Mute** button is lit red, then press the **Mute** button.

  Follow these steps to reset a Cisco DX650 on boot up:

  1. Press and hold the # key and power on the device.
  2. When the Message Waiting Indicator (MWI) flashes red once then stays lit, release the # key.

Reset Options and Load Upgrades

Cisco DX Series devices receive configuration changes and load upgrades from Cisco Unified Communications Manager. The following protocol describes how the device handles change requests:

- Reset waits for active call to end.
- If the device screen is on, user receives a popup dialog box that notifies the user about the changes and the need for restart. The dialog box provides the following options:
  - Restart: Dismisses the popup dialog box and restarts the device (default action).
  - Snooze: Dismisses the popup dialog box for an hour. The user can set the device to snooze for a maximum of 24 hours, after which the device will restart.

Note The popup dialog box has a countdown timer of 60 seconds. The default action begins if the user does not act.

After the user sets the device to snooze, the user has the option to manually reset the device at any time from the notifications list.

  - If the device screen is off, active audio keeps the request waiting.

Remote Lock

This feature allows you to lock a device from the Device Configuration window in Cisco Unified Communications Manager.

When the device receives a remote lock request, the device immediately terminates any active calls, and the device locks. If the device is not registered with the system at the time of the request, the device is locked the next time that it registers to the system.

Note After you issue a remote lock request, the request cannot be canceled.

Remote Lock Device

Procedure

Step 1 In the **Phone Configuration** window for the device, click **Lock**.

Step 2 Click **Lock** to accept the Lock confirmation message.
You can view the Lock status in the Device Lock/Wipe Status section of the **Phone Configuration** window for the device.

Remote Wipe

This feature allows you to erase the data on a device from the Device Configuration window in Cisco Unified Communications Manager.

When the device receives a remote wipe request, the device immediately terminates any active calls and erases the device data. If the device is not registered with the system at the time of the request, the data is erased the next time that the device registers to the system.

Note After you issue a remote wipe request, the request cannot be canceled.

Remote Wipe Device

Procedure

Step 1 In the **Phone Configuration** window for the device, click **Wipe**.

Step 2 Click **Wipe** to accept the Wipe confirmation message.
You can view the Wipe status in the Device Lock/Wipe Status section of the **Phone Configuration** window for the device.

Boot Alternate Image for Cisco DX70

Procedure

Step 1 Power on the device and wait for the Mute LED to blink.

Step 2 Press and hold the **Volume Down** button until the **Mute** button is lit red.

Step 3 Release the **Volume Down** button, then press and hold the **Mute** button for 3 seconds.

Boot Alternate Image for Cisco DX80

Procedure

Step 1 Press and hold the **Volume Down** button and power on the device.

Step 2 Release the **Volume Down** button when the **Mute** button is lit red, then press the **Mute** button.

Boot Alternate Image for Cisco DX650

Procedure

Step 1 Disconnect the power to turn the device off.

Step 2 Press and hold the * key, then connect the power supply.

Step 3 Keep the * key held until the message LED becomes solid.

Step 4 When the message LED flashes 3 times, release the * key.
The device uses the alternate image to boot.

Data Migration

The data migration feature ensures that a factory reset is not required when data incompatibility exists after a firmware upgrade.

Note Data may still be lost upon downgrade to an earlier release of firmware. If you upgrade to a newer firmware release, you may not be able to revert to an earlier release without losing data.

If you downgrade to earlier firmware and the device is not able to migrate data, you receive an alarm. Instruct the user to back up the user data or perform a remote wipe of the device. When the device registers to Cisco Unified Communications Manager, the device detects prior factory resets, overrides migration, downgrades, and reboots. When the device reboots, it loads the downgraded firmware.

Debugging Log Profiles

You can turn on debugging log profiles remotely for a device or group of devices.

Set Debugging Log Profile for Call Processing

Procedure

Step 1 Go to the Product Specific Configuration Layout area of the individual device configuration window or Common Phone Profile window.

Step 2 Check **Log Profile**, and choose Telephony.

Step 3 Save your changes.

Step 4 The user is notified that debug logging is enabled in the notification area. The user can expand the message for more information, but cannot dismiss the notification.

Reset Debugging Log Profile to Default

Procedure

Step 1 Go to the Product Specific Configuration Layout area of the individual device configuration window or Common Phone Profile window.

Step 2 Check **Log Profile**, and select **Default** to reset all debugs to the default values. This includes debugs that have been set manually from Android Debug Bridge.

Step 3 Save and apply your changes.

Step 4 Choose **Preset** to keep the current debug levels.

Step 5 Save your changes.

User Support

To successfully use some of the features on their devices, users must receive information from you or from your network team or be able to contact you for assistance. Make sure to provide end users with the names of people to contact for assistance and with instructions for contacting those people.

Cisco recommends that you create a web page on your internal support site that provides users with important information about their device.

Problem Report Tool

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

Note The Problem Report Tool logs are required by Cisco TAC when troubleshooting problems.

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

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

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

Configure Customer Support Upload URL

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

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

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

```
<?php

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

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

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

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

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

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

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

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

?>
```

Procedure

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

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

Step 3 Upload your script to your server.

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

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

Example:
http://example.com/prtscript.php

Step 6 Save your changes.

Take Screenshot From Web Browser

Procedure

Use your browser to go to this URL:http://<Endpoint IP Address>/CGI/Screenshot
You receive a prompt that asks for authentication. Use the associated user ID name and password.

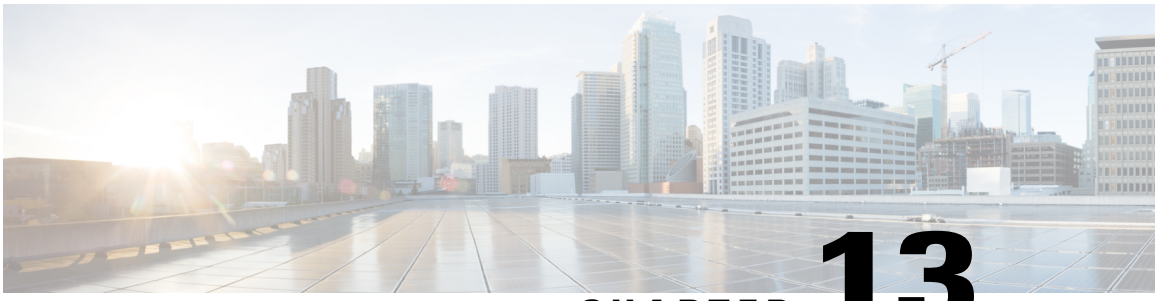
Take Screenshot From Device

Procedure

Press the **Vol Down** button and **Power/Lock** button for three seconds.

Application Support

Evaluate whether the issue is a device issue or a problem with the application. If the problem is application related, contact the application support center directly.



CHAPTER 13

Model Information Status and Statistics

- Model Information, page 141
- Device Status, page 142

Model Information

To display model information, choose **About device** in the Settings application. The Model Information screen includes the items that are listed in the following table.

Table 23: Model Information for Cisco DX Series Devices

Item	Description
Status	Submenu that provides additional information about the device.
Cisco user guide	Provides link to documentation.
Legal information	Includes open-source licenses.
Model number	Model number.
Android version	Indicates version of Android.
Kernel version	Linux kernel number.
Build number	Current software build.
SELinux status	Indicates enforcing or permissive.
Cisco load information	
Active load	Version of firmware that is currently installed.
Last upgrade	Date of the most recent firmware upgrade.

Item	Description
Note An "Upgrade Progress" message appears under "Cisco load information" group if the device is upgrading.	
Cisco Unified Communications Manager	
Active server	DNS or IP address of the server to which the device is registered.
Standby Server	DNS or IP address of the standby server.
Cisco Collaboration Problem Reporting Tool	
Cisco Collaboration Problem Reporting Tool	Tool for reporting problems. Tap to select and enter date, time, problem application problem description, and customer support email address. Tap **Create email report** to gather log information and send to support.

If the user is connected to a secure or authenticated server, a corresponding icon (lock or certificate) is displayed on the home screen to the right of the server option. If the user is not connected to a secure or authenticated server, no icon appears.

Device Status

To display the device status, choose **About device** > **Status** in the Settings application.

Table 24: Device Status

Item	Description
Status Messages	Provides the Status Messages screen, which shows a log of important system messages.
MDN	Indicates device mobile directory number.
IP address	Indicates device IP address.
Wi-Fi MAC address	Provides the MAC address of the current Wi-Fi connection.
Ethernet MAC address	Provides the MAC address of the current Ethernet connection.
Bluetooth address	Provides the MAC address of the Bluetooth chipset.
DHCP information	Displays DHCP information screen.
Up time	Run time for the device.
Current access point	Provides the Current access point screen, if applicable.

Item	Description
Ethernet Statistics	Provides the Ethernet statistics screen, which shows Ethernet traffic statistics.
WLAN statistics	Provides the WLAN statistics screen if applicable.
Call statistics (audio)	Provides counters and statistics for the audio portion of the current call.
Call statistics (video)	Provides counters and statistics for the video portion of the current call.
Call statistics (presentation)	Provides counters and statistics for the presentation portion of the current call.

Status Messages

The Status Messages screen lists the 50 most recent status messages that the device has generated. The following table describes the status messages that might appear. This table also includes actions you can take to address errors.

To display the Status messages screen, tap **Status messages**.

To remove current status messages, tap **Clear**.

To exit the Status messages screen, tap **OK**.

Table 25: Status Messages

Message	Description	Possible Explanation and Action
CFG TFTP Size Error	The configuration file is too large for file system.	Power cycle the device.
Checksum Error	Downloaded software file is corrupted.	Obtain a new copy of the device firmware and place it in the TFTPPath directory. Copy files into this directory only when the TFTP server software is shut down; otherwise, the files may be corrupted.

Message	Description	Possible Explanation and Action
DHCP timeout	DHCP server did not respond.	• Network is busy - The errors resolve themselves when the network load reduces. • No network connectivity between the DHCP server and the device - Verify the network connections. • DHCP server is down - Check configuration of DHCP server. • Errors persist - Consider assignment of a static IP address.
DNS timeout	DNS server did not respond.	• Network is busy - The errors resolve themselves when the network load reduces. • No network connectivity between the DNS server and the device - Verify the network connections. • DNS server is down - Check configuration of DNS server.
DNS unknown host	DNS could not resolve the name of the TFTP server or Cisco Unified Communications Manager.	• Verify that the hostnames of the TFTP server or Cisco Unified Communications Manager are configured properly in DNS. • Consider use of IP addresses rather than hostnames.
Duplicate IP	Another device is using the IP address that is assigned to the device.	• If the device has a static IP address, verify that you have not assigned a duplicate IP address. • If you are using DHCP, check the DHCP server configuration.

Message	Description	Possible Explanation and Action
Error update locale	One or more localization files could not be found in the TFTPPath directory or were not valid. The locale was not changed.	From Cisco Unified Communications Manager, check that the following files are located within subdirectories in TFTP File Management: • Located in subdirectory with same name network locale: ◦ tones.xml • Located in subdirectory with same name user locale: ◦ glyphs.xml ◦ dictionary.xml ◦ kate.xml
File not found <Cfg File>	The name-based and default configuration file was not found on the TFTP Server.	The configuration file is created when the device is added to the Cisco Unified Communications Manager database. If the device has not been added to the Cisco Unified Communications Manager database, the TFTP server generates a `CFG File Not Found` response. • The device is not registered with Cisco Unified Communications Manager. You must manually add the device to Cisco Unified Communications Manager if you are not allowing devices to auto-register. • If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server. • If you are using static IP addresses, check configuration of the TFTP server.
IP address released	The device is configured to release its IP address.	The device remains idle until it is power cycled or until you reset the DHCP address.
Load rejected HC	The application that was downloaded is not compatible with the device.	Occurs if you were attempting to install a version of software on this device that did not support hardware changes on this device. Check the load ID assigned to the device (from Cisco Unified Communications Manager, choose **Device** > **Phone**). Reenter the load that is displayed on the device.

Message	Description	Possible Explanation and Action
No default router	DHCP or static configuration did not specify a default router.	• If the device has a static IP address, verify that the default router has been configured. • If you are using DHCP, the DHCP server has not provided a default router. Check the DHCP server configuration.
No DNS server IP	A name was specified but DHCP or static IP configuration did not specify a DNS server address.	• If the device has a static IP address, verify that the DNS server has been configured. • If you are using DHCP, the DHCP server has not provided a DNS server. Check the DHCP server configuration.
No Trust List installed	The CTL file or the ITL file is not installed on the device.	The Trust List is not configured on Cisco Unified Communications Manager, which does not support security by default. For more information about the Trust List, see the *Cisco Unified Communications Manager Security Guide*.
Restart requested by Cisco Unified Communications Manager	The device is restarting based on a request from Cisco Unified Communications Manager.	Configuration changes have likely been made to the device in Cisco Unified Communications Manager, and **Apply** has been pressed so that the changes take effect.
TFTP access error	TFTP server is pointing to a directory that does not exist.	• If you are using DHCP, verify that the DHCP server is pointing to the correct TFTP server. • If you are using static IP addresses, check configuration of TFTP server.
TFTP error	The device does not recognize an error code that the TFTP server provided.	Contact Cisco Technical Assistance Center (TAC).
TFTP timeout	TFTP server did not respond.	• Network is busy - The errors resolve themselves when the network load diminishes. • No network connectivity between the TFTP server and the device - Verify the network connections. • TFTP server is down - Check configuration of TFTP server.

Message	Description	Possible Explanation and Action
Timed Out	Supplicant attempted 802.1X transaction but timed out due to the absence of an authenticator.	Authentication typically times out if 802.1X is not configured on the switch.
Trust List update failed, verification failure	Updating CTL and ITL files failed.	Message displayed in case of error.
Version error	The name of the load file is incorrect.	Make sure that the device load file has the correct name.
XmlDefault.cnf.xml, or .cnf.xml corresponding to the device name	Name of the configuration file.	None. This configuration file provides an informational message that indicates the name of the configuration file.

Ethernet Statistics

The Ethernet Statistics screen provides information about the device and network performance. The following table describes the information that appears on this screen.

To display Ethernet Statistics, choose **About device** > **Status** > **Ethernet statistics** in the Settings application.

To reset the Rx Frames, Tx Frames, and Rx Broadcasts statistics to 0, tap **Clear**.

To exit the Ethernet statistics screen, tap **OK**.

Table 26: Ethernet Statistics Message Information

Item	Description
Rx Frames	Number of packets received
Tx Frames	Number of packets sent
Rx Broadcasts	Number of broadcast packets received
Port 1	Speed and duplex for switch port
Port 2	Speed and duplex for PC port
CDP status	Current CDP status

WLAN Statistics

The WLAN Statistics screen provides statistics about the device and WLAN. The following table describes the information that appears on this screen.

To display the WLAN Statistics screen, choose **About device** > **Status** > **WLAN statistics**.

To exit the WLAN statistics screen, tap **OK**.

Table 27: WLAN Statistics

Item	Description
tx bytes	Number of bytes transmitted
rx bytes	Number of bytes received
tx packets	Number of data packets transmitted
rx packets	Number of data packets received
tx packets dropped	Number of transmitted data packets dropped
rx packets dropped	Number of received data packets dropped
tx packet errors	Number of transmitted data packet errors
rx packet errors	Number of received data packet errors
Tx frames	Number of frames transmitted
tx multicast frames	Number of frames transmitted as broadcast or multicast
tx retry	Number of messages retransmitted a single time being acknowledged by the receiving device
tx multi retry	Number of transmit retries prior to success
tx failure	Number of frames that failed to be transmitted
rts success	A corresponding CTS was received
rts failure	Number of frames that failed to be received.
ack failure	Access point did not acknowledge a transmission
rx duplicate frames	Number of duplicate multicast packets transmitted
rx fragmented packets	Number of fragmented packets received
roaming count	Number of times roamed from current access point

Audio Call Statistics

Access Call Statistics (audio) on the device to display counters, statistics, and voice-quality metrics for the most recent call.

Note You can use a web browser to access the Streaming Statistics web page and remotely view the call statistics information. This web page contains additional RTP Control Protocol (RTCP) statistics that are not available on the device.

A single call can have multiple voice streams, but data is captured only for 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.

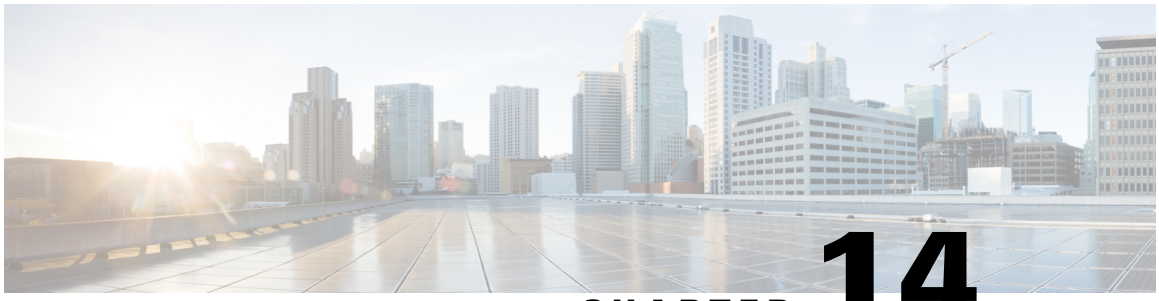
To display Call Statistics (audio) for information about the latest voice stream, choose **Settings** > **About device** > **Status** > **Call statistics (audio)**.

The following table lists and describes the items that the Call statistics (audio) screen provides.

Table 28: Call Statistics Items

Item	Description
Rcvr codec	Type of voice stream received (RTP streaming audio from codec): AAC-LD, G.722, iSAC, G.711 u-law, G.711 A-law, iLBC and G.729.
Sender codec	Type of voice stream transmitted (RTP streaming audio from codec): AAC-LD, G.722, iSAC, G.711 u-law, G.711 A-law, iLBC and G.729.
Rcvr size	Size of voice packets, in milliseconds, in the receiving voice stream (RTP streaming audio).
Sender size	Size of voice packets, in milliseconds, in the transmitting voice stream.
Rcvr packets	Number of RTP voice packets received since voice stream was opened. **Note** This number is not necessarily identical to the number of RTP voice packets received since the call began, because the call might have been placed on hold.
Sender packets	Number of RTP voice packets transmitted since voice stream was opened. **Note** This number is not necessarily identical to the number of RTP voice packets transmitted since the call began, because the call might have been placed on hold.
Avg jitter	Estimated average RTP packet jitter (dynamic delay that a packet encounters when going through the network), in milliseconds, observed since the receiving voice stream was opened.

Item	Description
Max jitter	Maximum jitter, in milliseconds, observed since the receiving voice stream was opened.
Rcvr discarded	Number of RTP packets in the receiving voice stream that have been discarded (bad packets, too late, and so on). **Note** The device discards payload type 19 comfort noise packets that Cisco gateways generate, which increments this counter.
Rcvr lost packets	Missing RTP packets (lost in transit).
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 three-second interval of active speech. If voice activity detection (VAD) is in use, a longer interval might be required to accumulate 3 seconds of active speech.
Max conceal ratio	Highest interval concealment ratio from start of the voice stream.
Conceal secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely conceal secs	Number of seconds that have more than 5 percent concealment events (lost frames) from the start of the voice stream.
Latency	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.
Sender DSCP	DSCP value for sender SIP signaling packets
Receiver DSCP	DSCP value for receiver SIP signaling packets
Sender RTCP DSCP	DSCP value for sender RTP packets
Receiver RTCP DSCP	DSCP value for sender RTP packets



CHAPTER 14

Remote Monitoring

- Enable and Disable Web Page Access, page 151
- Access Device Web Page, page 152
- Device Information, page 153
- Network Setup, page 154
- Security Information, page 159
- Ethernet Statistics, page 161
- WLAN Setup, page 163
- Device Logs, page 165
- Streaming Statistics, page 165

Enable and Disable Web Page Access

For security purposes, access to the web pages for the device is disabled by default. This prevents access to the web pages that are described in this chapter and to the Self Care Portal.

Procedure

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

Step 2 Specify the criteria to find the device and click **Find**, or click **Find** to display a list of all phones.

Step 3 Click the device name to open the **Phone Configuration** window for the device.

Step 4 Scroll down to the Product Specific Configuration section. From the **Web Access** drop-down list, choose **Enabled** to enable web page access or choose **Disabled** to disable web page access.

Step 5 Click **Save**.

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

Access Device Web Page

Procedure

Step 1 Use one of these methods to obtain the IP address of the device:

- Search for the device in Cisco Unified Communications Manager by choosing **Device** > **Phone**. Devices that are 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 device, choose **Settings** > **About device** > **Status** > **DHCP Information** and get the IP address for either Wi-Fi or Ethernet.

Step 2 Open a web browser and enter the following URL, where <IP_address> is the IP address of the device:
`http://<IP_address>`

The web page for the device includes these topics:

- Device Information - Provides device settings and related information.
- Network Setup - Provides network setup information.
- Security Information - Provides security information.
- Ethernet Statistics - Includes the following hyperlinks, which provide information about network traffic:
  - Ethernet Information - Provides information about Ethernet traffic.
  - Access - Provides information about network traffic to and from the device.
  - Network - Provides information about network traffic to and from the device.
- WLAN Setup
  - Current AP - Provides information about the current access point
  - WLAN Statistics - Provides information about WLAN traffic
- Device Logs - Includes the following hyperlinks, which provide information that you can use for troubleshooting:
  - Console Logs - Includes hyperlinks to individual log files.
  - Core Dumps - Includes hyperlinks to individual dump files.
  - Status Messages - Provides up to the ten most recent status messages that the device has generated since it was last powered up.
  - Debug Display - Provides debug messages that might be useful to Cisco Technical Assistance Center (TAC) if you require assistance with troubleshooting.
- Streaming Statistics - 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.

Device Information

The Device Information area on the device web page includes device settings and related information.

Table 29: Device Information Area Items

Item	Description
Ethernet Network State	Ethernet Network State
Wifi Network State	Wifi Network State
MAC Address	Ethernet MAC Address
WLAN MAC Address	IP address for Wi-Fi connection
Host Name	Unique, fixed name that is automatically assigned to the device based on its MAC address
Phone DN	Directory number that is assigned to the device
Version	Identifier of the firmware running on the device
Hardware Revision	Revision value of the device hardware
Serial Number	Unique serial number of the device
Model Number	Model number of the device
Message Waiting	Indicates whether a voice message is waiting on the primary line for the device.
UDI	Provides the following Cisco Unique Device Identifier (UDI) information about the device: • Device Type: Indicates hardware type. • Device Description: Provides the name of the device that is associated with the indicated model type. • Serial Number: Specifies the unique serial number of the device.
Time	Time obtained from the Date/Time Group in Cisco Unified Communications Manager to which the device belongs
Time Zone	Time zone obtained from the Date/Time Group in Cisco Unified Communications Manager to which the device belongs

Item	Description
Date	Date obtained from the Date/Time Group in Cisco Unified Communications Manager to which the device belongs

Network Setup

The Network Setup area on the device web page provides network setup information and information about other settings. The following table describes these items.

You can view and set many of these items from the Settings application on the device.

Table 30: Network Setup Items

Item	Description
Wifi Information	
Wifi DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the device obtains its Wifi IP address.
Wifi MAC Address	Wifi Media Access Control (MAC) address of the device.
Wifi Host Name	Hostname that the DHCP server assigned to the device.
Wifi Domain Name	Name of the Domain Name System (DNS) domain in which the device resides.
Wifi IP Address	Internet Protocol (IP) address of the device.
Wifi SubNet Mask	Subnet Mask used by the device.
Wifi Default Router	Default router used by the device.
Wifi DNS Server 1	Primary Domain Name System (DNS) server used by the device.
Wifi DNS Server 2	Optional backup DNS server used by the device.
Wifi EAP Authentication	Indicates EAP authentication setting
Wifi SSID	Indicates the current wifi SSID
Wifi Security Mode	Indicates the current wifi security mode
Wifi 80211 Mode	Indicates the current wifi 80211 mode
Ethernet Information	
Ethernet DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the device obtains its IP address.

Item	Description
Ethernet MAC Address	Media Access Control (MAC) address of the device.
Ethernet Host Name	Hostname that the DHCP server assigned to the device.
Ethernet Domain Name	Name of the Domain Name System (DNS) domain in which the device resides.
Ethernet IP Address	Internet Protocol (IP) address of the device.
Ethernet SubNet Mask	Subnet Mask used by the device.
Ethernet DNS Server 1	Primary Domain Name System (DNS) server used by the device.
Ethernet DNS Server 2	Optional backup DNS server used by the device.
Operational VLAN ID	Auxiliary Virtual Local Area Network (VLAN) configured on a Cisco Catalyst switch in which the device is a member.
Admin. VLAN ID	Auxiliary VLAN in which the device is a member.
PC VLAN	VLAN that is used to identify and remove 802.1P/Q tags from packets sent to the PC.
SW Port Speed	Speed and duplex of the switch port, where: • A - Auto Negotiate • 10H - 10BaseT/half duplex • 10F - 10BaseT/full duplex • 100H - 100BaseT/half duplex • 100F - 100BaseT/full duplex • 1000F - 1000BaseT/full duplex • No Link - No connection to the switch port
PC Port Speed	Speed and duplex of the switch port, where: • A - Auto Negotiate • 10H - 10-BaseT/half duplex • 10F - 10-BaseT/full duplex • 100H - 100-BaseT/half duplex • 100F - 100-BaseT/full duplex • 1000F - 1000-BaseT/full duplex • No Link - No connection to the switch port

Item	Description
IPv6 Information	
IP Addressing Mode	Indicates IP addressing mode.
IP Preference Mode Control	Indicates IP preference mode.
IPv6 Auto Configuration	Indicates if IPv6 auto configuration is enabled or disabled.
Duplicate Address Detection	Indicates if duplicate address detection is enabled or disabled.
Accept Redirect Messages	Indicates if accepting redirect messages is enabled or disabled.
Reply Multicast Echo Request	Indicates if replying to multicast echo requests is enabled or disabled.
IPv6 Address	Internet Protocol version 6 (IPv6) address of the phone.
IPv6 Prefix Length	Indicates IPv6 prefix length.
IPv6 Default Router	Indicates default router.
IPv6 DNS Server 1	Primary DNS server used by the device.
IPv6 DNS Server 2	optional backup DNS server used by the device
IPv6 Alternate TFTP	Indicates whether the device is using an alternative TFTP server.
IPv6 TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the device.
IPv6 TFTP Server 2	Backup Trivial File Transfer Protocol (TFTP) server used by the device.
CUCM Configuration	

Item	Description
CUCM Server 1-5	Hostnames or IP addresses, in prioritized order, of the Cisco Unified Communications Manager servers with which the device can register. An item can also show the IP address of an SRST router that is capable of providing limited Cisco Unified Communications Manager functionality, if such a router is available. For an available server, an item shows the Cisco Unified Communications Manager server IP address and one of the following states: • **Active** - Cisco Unified Communications Manager server from which the device is currently receiving call-processing services • **Standby** - Cisco Unified Communications Manager server to which the device switches if the current server becomes unavailable • **Blank** - No current connection to this Cisco Unified Communications Manager server An item may also include the Survivable Remote Site Telephony (SRST) designation, which identifies an SRST router that is 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 window in Cisco Unified Communications Manager Administration.
Information URL	This feature is not supported on Cisco DX Series devices.
Directories URL	This feature is not supported on Cisco DX Series devices.
Messages URL	This feature is not supported on Cisco DX Series devices.
Services URL	This feature is not supported on Cisco DX Series devices.
Forwarding Delay	The time that is spent in the listening and learning state.
Idle URL	This feature is not supported on Cisco DX Series devices.
Idle URL time	This feature is not supported on Cisco DX Series devices.
Proxy Server URL	This feature is not supported on Cisco DX Series devices.
Authentication URL	This feature is not supported on Cisco DX Series devices.
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the device.
TFTP Server 2	Backup Trivial File Transfer Protocol (TFTP) server used by the device.
Alternate TFTP	Indicates whether the device is using an alternative TFTP server.

Item	Description
User Locale	User locale that is associated with the device user. Identifies a set of detailed information to support users, including language, font, date, and time formatting, and alphanumeric keyboard text information.
Network Locale	Network locale that is associated with the device user. Identifies a set of detailed information to support the device in a specific location, including definitions of the tones and cadences that the device uses.
User Locale Version	Version of the user locale that is loaded on the device.
Network Locale Version	Version of the network locale that is loaded on the device.
PC Port Disabled	Indicates whether the PC port on the device is enabled or disabled.
GARP Enabled	Indicates whether the device learns MAC addresses from Gratuitous ARP responses.
Video Capability Enabled	Indicates whether the device can participate in video calls.
Voice Vlan Access Enabled	Indicates whether the device allows a device attached to the PC port to access the Voice VLAN.
Auto Select Line	Indicates whether auto select line is enabled for the device.
Dscp For Call Control	DSCP IP classification for call control signaling.
Dscp For Setup.	DSCP IP classification for the device configuration transfer.
Dscp For Services	DSCP IP classification for the device-based services.
Security Mode	The security mode that is set for the device.
Web Access	Indicates whether web access is enabled (Yes) or disabled (No) for the device.
Span PC Port	Indicates whether the device will forward packets that are transmitted and received on the network port to the access port.
CDP on PC Port	Indicates whether CDP is supported on the PC port (default is enabled). When CDP is disabled in Cisco Unified Communications Manager, a warning is displayed, indicating that disabling CDP on the PC port prevents CVTA from working. The current PC and switch port CDP values are shown in the Settings application.

Item	Description
CDP on SW Port	Indicates whether CDP is supported on the switch port (default is enabled). Enable CDP on the switch port for VLAN assignment for the device, power negotiation, QoS management, and 802.1x security. Enable CDP on the switch port when the device is connected to a Cisco switch. When CDP is disabled in Cisco Unified Communications Manager, a warning is presented, indicating that CDP is disabled on the switch port only if the device is connected to a non-Cisco switch. The current PC and switch port CDP values are shown in the Settings application.
LLDP-MED SW Port	Indicates whether Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) is enabled on the switch port.
LLDP PC Port	Indicates whether Link Layer Discovery Protocol (LLDP) is enabled on the PC port.
LLDP Power Priority	Advertises the device power priority to the switch, enabling the switch to appropriately provide power to the device. Settings include: • Unknown - Default • Low • High • Critical
LLDP Asset ID	Identifies the asset ID that is assigned to the device for inventory management.
Switch Port Remote Configuration	Allows the administrator to configure the speed and function of the device table port remotely by using Cisco Unified Communications Manager Administration.
PC Port Remote Configuration	Allows the administrator to configure the speed and function of the device table port remotely by using Cisco Unified Communications Manager Administration.

Security Information

The Security Information area on the device web page includes information about the CTL and ITL files, and 802.1X authentication.

Table 31: Security Information Items

Item	Description
Signaling Security Mode	Indicates signaling security mode.
LSC	Indicates whether LSC is installed on the device.
CAPF Server (IPv4)	Indicates CAPF server address for IPv4
CAPF Server (IPv6)	Indicates CAPF server address for IPv6
CAPF Port	Indicates CAPF port
CTL File	
CTL Signature	Displays CTL signature
CUCM Server/TFTP Server	Indicates CUCM/TFTP server addresses
Application Server	Indicates application server
CAPF Server	Indicates CAPF server
ITL File	
ITL Signature	Displays ITL signature
CAPF Server	Indicates CAPF server
TVS	Indicates TVS addresses
CUCM Server/TFTP Server	Indicates CUCM/TFTP server addresses
Configuration File	Indicates whether ITL configuration file is installed on the device
802.1X Authentication	
Device Authentication	Indicates whether 802.1X device authentication is enabled.
Transaction Status	Indicates whether 802.1X transaction status is enabled.
Protocol	Indicates 802.1X protocol.
Device ID	Displays device ID.

Ethernet Statistics

The following Ethernet statistics hyperlinks on the device web page provide information about network traffic. To display a network statistics area, access the device web page.

- Ethernet Information: Provides information about Ethernet traffic. The first table describes the items in this area.
- Access area: Provides information about network traffic to and from the device. The second table describes the items in this area.
- Network area: Provides information about network traffic to and from the device. The second table describes the items in this area.

Table 32: Ethernet Information Items

Item	Description
Tx Frames	Total number of packets transmitted by the device
Tx broadcast	Total number of broadcast packets transmitted by the device
Tx multicast	Total number of multicast packets transmitted by the device
Tx unicast	Total number of unicast packets transmitted by the device
Rx Frames	Total number of packets received by the device
Rx broadcast	Total number of broadcast packets received by the device
Rx multicast	Total number of multicast packets received by the device
Rx unicast	Total number of unicast packets received by the device
Rx PacketNoDes	Total number of shed packets caused by no Direct Memory Access (DMA) descriptor

Table 33: Access and Network Items

Item	Description
Rx totalPkt	Total number of packets received by the device
Rx crcErr	Total number of packets received with CRC failed
Rx alignErr	Total number of packets received between 64 and 1522 bytes in length with a bad Frame Check Sequence (FCS)
Rx multicast	Total number of multicast packets received by the device

Item	Description
Rx broadcast	Total number of broadcast packets received by the device
Rx unicast	Total number of unicast packets received by the device
Rx shortErr	Total number of FCS error packets or Align error packets received that are less than 64 bytes in size
Rx shortGood	Total number of good packets received that are less than 64 bytes size
Rx longGood	Total number of good packets received that are greater than 1522 bytes in size
Rx longErr	Total number of FCS error packets or Align error packets received that are greater than 1522 bytes in size
Rx size64	Total number of packets received, including bad packets, that are between 0 and 64 bytes in size
Rx size65to127	Total number of packets received, including bad packets, that are between 65 and 127 bytes in size
Rx size128to255	Total number of packets received, including bad packets, that are between 128 and 255 bytes in size
Rx size256to511	Total number of packets received, including bad packets, that are between 256 and 511 bytes in size
Rx size512to1023	Total number of packets received, including bad packets, that are between 512 and 1023 bytes in size
Rx size1024to1518	Total number of packets received, including bad packets, that are between 1024 and 1518 bytes in size
Rx tokenDrop	Total number of packets dropped due to lack of resources (for example, FIFO overflow)
Tx excessDefer	Total number of packets delayed from transmitting due to medium being busy
Tx lateCollision	Number of times that collisions occurred later than 512 bit times after the start of packet transmission
Tx totalGoodPkt	Total number of good packets (multicast, broadcast, and unicast) received by the device
Tx Collisions	Total number of collisions that occurred while a packet was being transmitted
Tx excessLength	Total number of packets not transmitted because the packet experienced 16 transmission attempts
Tx broadcast	Total number of broadcast packets transmitted by the device

Item	Description
Tx multicast	Total number of multicast packets transmitted by the device
LLDP FramesOutTotal	Total number of LLDP frames sent out from the device
LLDP AgeoutsTotal	Total number of LLDP frames that have been timed 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 received with one or more detectable errors
LLDP FramesInTotal	Total number of LLDP frames received on the device
LLDP TLVDiscardedTotal	Total number of LLDP TLVs that are discarded
LLDP TLVUnrecognizedTotal	Total number of LLDP TLVs that are not recognized on the device
CDP Neighbor Device ID	Identifier of a device connected to this port discovered by CDP
CDP Neighbor IP Address	IP address of the neighbor device discovered by CDP
CDP Neighbor Port	Neighbor device port to which the device is connected discovered by CDP
LLDP Neighbor Device ID	Identifier of a device connected to this port discovered by LLDP
LLDP Neighbor IP Address	IP address of the neighbor device discovered by LLDP
LLDP Neighbor Port	Neighbor device port to which the device is connected discovered by LLDP
Port Information	Speed and duplex information

WLAN Setup

The following WLAN Setup hyperlinks on the device web page provide wireless network setup information and information about other settings.

- Current AP
- WLAN Statistics

Table 34: Current AP

Item	Description
AP Name	Provides the current access point name.

Item	Description
MAC Address	Provides the MAC address of the access point.
Current Channel	The latest channel where this AP was observed.
Last RSSI	The latest RSSI in which this AP was observed.
Beacon Interval	Number of time units between beacons. A time unit is 1.024 ms.
Min Rate	Minimum data rate that the AP requires.
Max Rate	Maximum data rate that the AP requires.
WMM Supported	Support for Wi-Fi multimedia extensions.
UAPSD Supported	The AP supports Unscheduled Automatic Power Save Delivery. May only be available if WMM is supported. This feature is critical for talk time and for achieving maximum call density.
Noise	Indicates the current noise level.
Load	Indicates the current load.
Quality	Indicates voice quality.

Table 35: WLAN Statistics

Item	Description
NetDevice Stats	
Tx bytes	Total number of bytes that the device transmits.
Rx Bytes	Total number of bytes that the device receives.
Tx Packets	Total number of packets that the device transmits.
Rx Packets	Total number of packets that the device receives.
Tx Packets Dropped	Total number of transmitted packets that the device dropped.
Rx Packets Dropped	Total number of received packets that the device dropped.
Tx Packets Error	Total number of transmitted error packets.
Rx Packets Error	Total number of received error packets.
Firmware Stats	
Multicast Tx Frames	Total number of multicast packets that the device transmitted.
Failed	Transmission of packet failed.
Retry	Counter of total retries.

Item	Description
Multiple Retry	Transmission of packet required two or more retries before success.
Frame Dup	Number of duplicate packets received by the device.
Rts Success	A corresponding CTS was received.
Rts Failure	A corresponding CTS was not received.
Ack Failure	AP did not acknowledge a transmission.
Rx Frag	Number of fragmented packets that the device received.
Multicast Rx Frame	Number of multicast packets that the device received.
FCS Error	Increments when a Frame Checksum (FCS) error is detected in a received MPDU.
Tx Frames	Number of packets that the device sent.
Roaming Stats	
current/total	Current roaming time/total roaming time in ms.

Device Logs

The following device log hyperlinks on the device web page provide information you can use to help monitor and troubleshoot the device. To access a device log area, access the device web page.

- Console Logs: Includes hyperlinks to individual log files. The console log files include the current syslog, archived logs from the inactive load, logs from the last reboot, archived logs for the current load, and compressed collections of logs that the Problem Report Tool generates.
- Core Dumps: Includes hyperlinks to individual dump files. The core dumps (tombstone_xx) include data from application crashes. The ANR file (traces.txt) includes data for applications that the device determines are not responding and the user chooses to terminate the application.
- Status Messages: Includes up to the 50 most recent status messages that the device has generated since it was last powered up. You can also see this information from the Status Messages screen on the device.
- Debug Display: Includes debug messages that might be useful to Cisco TAC if you require assistance with troubleshooting.

Streaming Statistics

The device streams information when it is on a call or is running a service that sends or receives audio or data.

The streaming statistics areas on the device web page provide information about the streams.

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

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

Table 36: Streaming Statistics Area Items

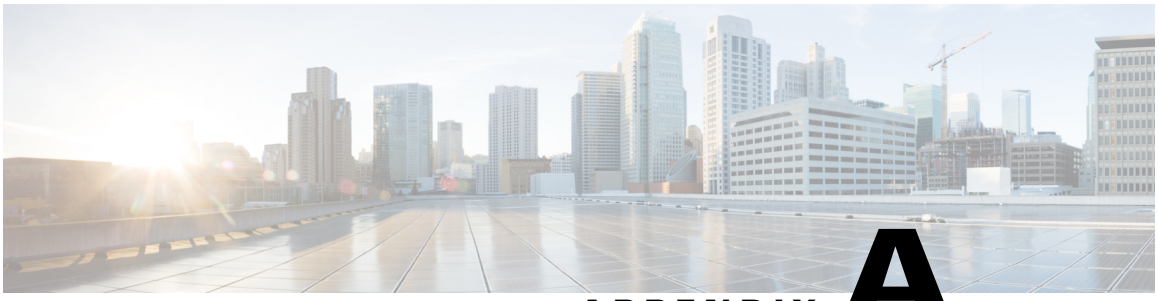
Item	Description
Remote Address	IP address and UDP port of the destination of the stream.
Local Address	IP address and UDP port of the device.
Start Time	Internal time stamp that indicates when Cisco Unified Communications Manager requested that the device start transmitting packets.
Stream Status	Indication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

Item	Description
Receiver Packets	Total number of RTP data packets received by the device 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.
Receiver 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.
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 voice activity detection (VAD) is in use, a longer interval might be required to accumulate 3 seconds of active speech.
Max Conceal Ratio	Highest interval concealment ratio from start of the voice stream.
Conceal Secs	Number of seconds that have concealment events (lost frames) from the start of the voice stream (includes severely concealed seconds).
Severely Conceal Secs	Number of seconds that have more than five percent concealment events (lost frames) from the start of the voice stream.
Latency (see note)	Estimate of the network latency, expressed in milliseconds. Represents a running average of the round-trip delay, measured when RTCP receiver report blocks are received.
Max Jitter	Maximum value of instantaneous jitter, in milliseconds.
Sender Size	RTP packet size, in milliseconds, for the transmitted stream.
Sender Reports Received (see note)	Number of times RTCP Sender Reports have been received.
Sender Report Time Received (see note)	Last time at which an RTCP Sender Report was received.
Receiver Size	RTP packet size, in milliseconds, for the received stream.
Receiver Discarded	RTP packets received from network but discarded from jitter buffers.
Receiver Reports Received (see note)	Number of times RTCP Receiver Reports have been received.
Receiver Report Time Received (see note)	Last time at which an RTCP Receiver Report was received.

Item	Description
Receiver Encrypted	Indicates if the receiver stream is encrypted.
Sender Encrypted	Indicates if the sender stream is encrypted.
Sender Frames	Number of video frames that by the device transmitted since the video stream opened.
Sender Partial Frames	Number of P-frames that the device sent since the video stream opened.
Sender IFrames	Number of I-frames that the device sent since the video stream opened.
Sender Frame Rate	Rate at which video frames are transmitted (in frames per second).
Sender Bandwidth	Bandwidth of the transmitted video steam in kbps (kilo bits per second).
Sender Resolution	Resolution of the video stream that the device transmits.
Receiver Frames	Number of video frames that the device received since the video stream opened.
Receiver Partial Frames	Number of P-frames that the device received since the video stream opened.
Receiver IFrames	Number of I-frames that the device received since the video stream opened.
Receiver IFrames Req	Number of IDR requests that the device sent to the remote endpoint since the video stream opened.
Receiver Frame Rate	Rate at which video frames are received (in frames per second).
Receiver Frames Lost	Number of frames lost that the video decoder reported since the video stream opened.
Receiver Frames Errors	Number of errors that the video decoder reported since the video stream opened.
Receiver Bandwidth	Bandwidth of the received video steam in kbps (kilo bits per second).
Receiver Resolution	Resolution of the video stream that the phone received from the remote endpoint.
Domain Name	Indicates the domain name.
Sender Joins	Number of times the device has started transmitting a stream
Receiver Joins	Number of times the device has started receiving a stream
Byes	Number of times the device has stopped transmitting a stream

Item	Description
Sender Start Time	Time stamp that indicates when the first RTP packet is sent to the network.
Receiver Start Time	Time stamp that indicates when the first RTP packet is received from the network.
Sender DSCP	DSCP value for sender SIP signaling packets
Receiver DSCP	DSCP value for receiver SIP signaling packets
Sender RTCP DSCP	DSCP value for sender RTP packets
Receiver RTCP DSCP	DSCP value for sender RTP packets
Is Video	Indicates a video call.
Is Presentation	Indicates a presentation call.
Sender Active	Indicates the sender is active.
Receiver Active	Indicates the receiver is active.

Note When the RTP Control Protocol is disabled, no data is generated for this field and therefore it displays as 0.



APPENDIX A

Certificate Authority Trust List

- Certificate Authority Trust List, page 171

Certificate Authority Trust List

The following is the list of trusted Certificate Authorities embedded in the devices. For Mobile and Remote Access through Expressway, the Expressway server must be signed against one of these Certificate Authorities.

```
---------------------------------------------------------------------
subject=  C=NL O=Staat der Nederlanden CN=Staat der Nederlanden Root CA
---------------------------------------------------------------------
subject=  C=US O=VeriSign, Inc. OU=VeriSign Trust Network OU=(c) 1999 VeriSign, Inc. - For authorized
 use only CN=VeriSign Class 3 Public Primary Certification Authority - G3
---------------------------------------------------------------------
subject=  C=HU L=Budapest O=NetLock Halozatbiztonsagi Kft. OU=Tanusitvanykiadok CN=NetLock
Minositett Kozjegyzoi (Class QA) Tanusitvanykiado emailAddress=info@netlock.hu
---------------------------------------------------------------------
subject=  C=TR L=Gebze - Kocaeli O=T\xC3\xBCrkiye Bilimsel ve Teknolojik Ara\xC5\x9Ft\xC4\xB1rma
 Kurumu - T\xC3\x9CB\xC4\xB0TAK OU=Ulusal Elektronik ve Kriptoloji Ara\xC5\x9Ft\xC4\xB1rma
Enstit\xC3\xBCs\xC3\xBC - UEKAE OU=Kamu Sertifikasyon Merkezi CN=T\xC3\x9CB\xC4\xB0TAK
UEKAE K\xC3\xB6k Sertifika Hizmet Sa\xC4\x9Flay\xC4\xB1c\xC4\xB1s\xC4\xB1 - S\xC3\xBCr\xC3\xBCm
 3
---------------------------------------------------------------------
subject=  C=BM O=QuoVadis Limited CN=QuoVadis Root CA 3
---------------------------------------------------------------------
subject=  C=US O=VeriSign, Inc. OU=VeriSign Trust Network OU=(c) 1999 VeriSign, Inc. - For authorized
 use only CN=VeriSign Class 1 Public Primary Certification Authority - G3
---------------------------------------------------------------------
subject=  C=DK O=TDC Internet OU=TDC Internet Root CA
---------------------------------------------------------------------
subject=  C=US O=VeriSign, Inc. OU=VeriSign Trust Network OU=(c) 2007 VeriSign, Inc. - For authorized
 use only CN=VeriSign Class 3 Public Primary Certification Authority - G4
---------------------------------------------------------------------
subject=  C=ZA ST=Western Cape L=Cape Town O=Thawte Consulting cc OU=Certification Services
Division CN=Thawte Server CA emailAddress=server-certs@thawte.com
---------------------------------------------------------------------
subject=  O=RSA Security Inc OU=RSA Security 2048 V3
---------------------------------------------------------------------
subject=  C=US O=VeriSign, Inc. OU=Class 1 Public Primary Certification Authority - G2 OU=(c) 1998
```

VeriSign, Inc. - For authorized use only OU=VeriSign Trust Network
---
subject= C=US O=The Go Daddy Group, Inc. OU=Go Daddy Class 2 Certification Authority
---
subject= C=US O=AffirmTrust CN=AffirmTrust Networking
---
subject= C=SK L=Bratislava O=Disig a.s. CN=CA Disig
---
subject= C=FR O=Certinomis OU=0002 433998903 CN=Certinomis - Autorit\xC3\xA9 Racine
---
subject= C=SE O=AddTrust AB OU=AddTrust External TTP Network CN=AddTrust External CA Root
---
subject= L=ValiCert Validation Network O=ValiCert, Inc. OU=ValiCert Class 2 Policy Validation Authority CN=http: www.valicert.com emailAddress=info@valicert.com
---
subject= C=US O=GeoTrust Inc. CN=GeoTrust Primary Certification Authority
---
subject= O=Cisco CN=ACT2 ECC SUDI CA
---
subject= C=EU O=AC Camerfirma SA CIF A82743287 OU=http: www.chambersign.org CN=Global Chambersign Root
---
subject= C=US O=VeriSign, Inc. OU=VeriSign Trust Network OU=(c) 2008 VeriSign, Inc. - For authorized use only CN=VeriSign Universal Root Certification Authority
---
subject= C=JP O=SECOM Trust.net OU=Security Communication RootCA1
---
subject= C=FI O=Sonera CN=Sonera Class2 CA
---
subject= C=US O=America Online Inc. CN=America Online Root Certification Authority 1
---
subject= C=US O=Equifax Secure OU=Equifax Secure eBusiness CA-2
---
subject= C=US O=GeoTrust Inc. OU=(c) 2008 GeoTrust Inc. - For authorized use only CN=GeoTrust Primary Certification Authority - G3
---
subject= C=US O=SecureTrust Corporation CN=Secure Global CA
---
subject= C=GB O=Trustis Limited OU=Trustis FPS Root CA
---
subject= C=JP O=Japan Certification Services, Inc. CN=SecureSign RootCA11
---
subject= C=IL O=StartCom Ltd. OU=Secure Digital Certificate Signing CN=StartCom Certification Authority
---
subject= C=US O=Digital Signature Trust OU=DST ACES CN=DST ACES CA X6
---
subject= emailAddress=pki@sk.ee C=EE O=AS Sertifitseerimiskeskus CN=Juur-SK
---
subject= C=US ST=Arizona L=Scottsdale O=GoDaddy.com, Inc. CN=Go Daddy Root Certificate Authority - G2
---
subject= C=US ST=UT L=Salt Lake City O=The USERTRUST Network OU=http: www.usertrust.com CN=UTN-USERFirst-Hardware
---
subject= C=NO O=Buypass AS-983163327 CN=Buypass Class 2 Root CA
---
subject= C=EU L=Madrid (see current address at www.camerfirma.com address) serialNumber=A82743287 O=AC Camerfirma S.A. CN=Global Chambersign Root - 2008

```
---------------------------------------------------------------------
subject=  C=US O=VeriSign, Inc. OU=VeriSign Trust Network OU=(c) 2006 VeriSign, Inc. - For authorized
 use only CN=VeriSign Class 3 Public Primary Certification Authority - G5
---------------------------------------------------------------------
subject=  O=Cisco CN=Cisco ECC Root CA
---------------------------------------------------------------------
subject=  C=DE O=T-Systems Enterprise Services GmbH OU=T-Systems Trust Center CN=T-TeleSec
GlobalRoot Class 3
---------------------------------------------------------------------
subject=  C=US O=DigiCert Inc OU=www.digicert.com CN=DigiCert Assured ID Root CA
---------------------------------------------------------------------
subject=  C=CH O=SwissSign AG CN=SwissSign Platinum CA - G2
---------------------------------------------------------------------
subject=  C=US ST=UT L=Salt Lake City O=The USERTRUST Network OU=http:  www.usertrust.com
CN=UTN - DATACorp SGC
---------------------------------------------------------------------
subject= C=CH O=WISeKey OU=Copyright (c) 2005 OU=OISTE Foundation Endorsed CN=OISTE WISeKey
 Global Root GA CA
---------------------------------------------------------------------
subject=  C=NL O=Staat der Nederlanden CN=Staat der Nederlanden Root CA - G2
---------------------------------------------------------------------
subject=  O=Cisco CN=Cisco Licensing Root CA
---------------------------------------------------------------------
subject=  C=US ST=UT L=Salt Lake City O=The USERTRUST Network OU=http:  www.usertrust.com
CN=UTN-USERFirst-Network Applications
---------------------------------------------------------------------
subject=  C=ch O=Swisscom OU=Digital Certificate Services CN=Swisscom Root CA 1
---------------------------------------------------------------------
subject=  C=JP O=SECOM Trust Systems CO.,LTD. OU=Security Communication RootCA2
---------------------------------------------------------------------
subject=  C=US O=DigiCert Inc OU=www.digicert.com CN=DigiCert High Assurance EV Root CA
---------------------------------------------------------------------
subject=  C=HU L=Budapest O=NetLock Kft. OU=Tan\xC3\xBAs\xC3\xADtv\xC3\xA1nykiad\xC3\xB3k
(Certification Services) CN=NetLock Arany (Class Gold) F\xC5\x91tan\xC3\xBAs\xC3\xADtv\xC3\xA1ny
---------------------------------------------------------------------
subject=  C=NO O=Buypass AS-983163327 CN=Buypass Class 3 CA 1
---------------------------------------------------------------------
subject=  C=US O=VeriSign, Inc. OU=VeriSign Trust Network OU=(c) 1999 VeriSign, Inc. - For authorized
 use only CN=VeriSign Class 2 Public Primary Certification Authority - G3
---------------------------------------------------------------------
subject=  C=PL O=Unizeto Sp. z o.o. CN=Certum CA
---------------------------------------------------------------------
subject=  C=ZA ST=Western Cape L=Cape Town O=Thawte Consulting cc OU=Certification Services
Division CN=Thawte Premium Server CA emailAddress=premium-server@thawte.com
---------------------------------------------------------------------
subject=  C=TW O=Chunghwa Telecom Co., Ltd. OU=ePKI Root Certification Authority
---------------------------------------------------------------------
subject=  C=US O=VeriSign, Inc. OU=Class 2 Public Primary Certification Authority
---------------------------------------------------------------------
subject=  L=ValiCert Validation Network O=ValiCert, Inc. OU=ValiCert Class 3 Policy Validation Authority
 CN=http:  www.valicert.com  emailAddress=info@valicert.com
---------------------------------------------------------------------
subject= C=DE O=TC TrustCenter GmbH OU=TC TrustCenter Universal CA CN=TC TrustCenter Universal
 CA I
---------------------------------------------------------------------
subject=  C=EU O=AC Camerfirma SA CIF A82743287 OU=http:  www.chambersign.org CN=Chambers
of Commerce Root
---------------------------------------------------------------------
```

subject= C=US O=VISA OU=Visa International Service Association CN=Visa eCommerce Root
---
subject= C=FR O=Certplus CN=Class 2 Primary CA
---
subject= C=US O=VeriSign, Inc. OU=Class 3 Public Primary Certification Authority
---
subject= C=FI O=Sonera CN=Sonera Class1 CA
---
subject= OU=GlobalSign Root CA - R2 O=GlobalSign CN=GlobalSign
---
subject= C=EU L=Madrid (see current address at www.camerfirma.com address) serialNumber=A82743287 O=AC Camerfirma S.A. CN=Chambers of Commerce Root - 2008
---
subject= C=PL O=Unizeto Technologies S.A. OU=Certum Certification Authority CN=Certum Trusted Network CA
---
subject= C=US O=Equifax Secure Inc. CN=Equifax Secure Global eBusiness CA-1
---
subject= C=JP O=Japanese Government OU=ApplicationCA
---
subject= C=DE O=TC TrustCenter GmbH OU=TC TrustCenter Class 3 CA CN=TC TrustCenter Class 3 CA II
---
subject= C=US O=VeriSign, Inc. OU=Class 3 Public Primary Certification Authority - G2 OU=(c) 1998 VeriSign, Inc. - For authorized use only OU=VeriSign Trust Network
---
subject= C=DE O=Deutsche Telekom AG OU=T-TeleSec Trust Center CN=Deutsche Telekom Root CA 2
---
subject= C=US O=America Online Inc. CN=America Online Root Certification Authority 2
---
subject= C=DK O=TDC CN=TDC OCES CA
---
subject= C=US O=SecureTrust Corporation CN=SecureTrust CA
---
subject= C=HU L=Budapest O=NetLock Halozatbiztonsagi Kft. OU=Tanusitvanykiadok CN=NetLock Uzleti (Class B) Tanusitvanykiado
---
subject= C=CN O=CNNIC CN=CNNIC ROOT
---
subject= CN=EBG Elektronik Sertifika Hizmet Sa\xC4\x9Flay\xC4\xB1c\xC4\xB1s\xC4\xB1 O=EBG Bili\xC5\x9Fim Teknolojileri ve Hizmetleri A.\xC5\x9E. C=TR
---
subject= C=US O=GeoTrust Inc. OU=(c) 2007 GeoTrust Inc. - For authorized use only CN=GeoTrust Primary Certification Authority - G2
---
subject= C=US O=VeriSign, Inc. OU=Class 1 Public Primary Certification Authority
---
subject= C=US O=thawte, Inc. OU=Certification Services Division OU=(c) 2006 thawte, Inc. - For authorized use only CN=thawte Primary Root CA
---
subject= C=US ST=Arizona L=Scottsdale O=Starfield Technologies, Inc. CN=Starfield Services Root Certificate Authority - G2
---
subject= O=Cisco CN=Cisco Root CA M2
---
subject= C=US O=Wells Fargo OU=Wells Fargo Certification Authority CN=Wells Fargo Root Certificate Authority
---

subject= C=DE O=TC TrustCenter GmbH OU=TC TrustCenter Universal CA CN=TC TrustCenter Universal CA III
---
subject= C=US O=GTE Corporation OU=GTE CyberTrust Solutions, Inc. CN=GTE CyberTrust Global Root
---
subject= C=US O=Entrust.net OU=www.entrust.net CPS incorp. by ref. (limits liab.) OU=(c) 1999 Entrust.net Limited CN=Entrust.net Secure Server Certification Authority
---
subject= C=CH O=SwissSign AG CN=SwissSign Silver CA - G2
---
subject= C=NO O=Buypass AS-983163327 CN=Buypass Class 2 CA 1
---
subject= C=US O=VeriSign, Inc. OU=Class 3 Public Primary Certification Authority
---
subject= C=US O=DigiCert Inc OU=www.digicert.com CN=DigiCert Global Root CA
---
subject= C=US O=thawte, Inc. OU=(c) 2007 thawte, Inc. - For authorized use only CN=thawte Primary Root CA - G2
---
subject= C=HU ST=Hungary L=Budapest O=NetLock Halozatbiztonsagi Kft. OU=Tanusitvanykiadok CN=NetLock Kozjegyzoi (Class A) Tanusitvanykiado
---
subject= C=US O=Starfield Technologies, Inc. OU=Starfield Class 2 Certification Authority
---
subject= C=DE O=TC TrustCenter GmbH OU=TC TrustCenter Class 2 CA CN=TC TrustCenter Class 2 CA II
---
subject= C=ES CN=Autoridad de Certificacion Firmaprofesional CIF A62634068
---
subject= C=FR O=Dhimyotis CN=Certigna
---
subject= C=US ST=UT L=Salt Lake City O=The USERTRUST Network OU=http: www.usertrust.com CN=UTN-USERFirst-Client Authentication and Email
---
subject= C=BE O=GlobalSign nv-sa OU=Root CA CN=GlobalSign Root CA
---
subject= C=US O=Entrust, Inc. OU=www.entrust.net CPS is incorporated by reference OU=(c) 2006 Entrust, Inc. CN=Entrust Root Certification Authority
---
subject= C=US O=VeriSign, Inc. OU=Class 2 Public Primary Certification Authority - G2 OU=(c) 1998 VeriSign, Inc. - For authorized use only OU=VeriSign Trust Network
---
subject= C=US ST=Arizona L=Scottsdale O=Starfield Technologies, Inc. CN=Starfield Root Certificate Authority - G2
---
subject= C=US O=VeriSign, Inc. OU=Class 4 Public Primary Certification Authority - G2 OU=(c) 1998 VeriSign, Inc. - For authorized use only OU=VeriSign Trust Network
---
subject= C=US OU=www.xrampsecurity.com O=XRamp Security Services Inc CN=XRamp Global Certification Authority
---
subject= C=US O=AffirmTrust CN=AffirmTrust Premium ECC
---
subject= C=US O=VeriSign, Inc. OU=VeriSign Trust Network OU=(c) 1999 VeriSign, Inc. - For authorized use only CN=VeriSign Class 4 Public Primary Certification Authority - G3
---
subject= C=BM O=QuoVadis Limited CN=QuoVadis Root CA 2
---

subject= C=CO O=Sociedad Cameral de Certificaci\xC3\xB3n Digital - Certic\xC3\xA1mara S.A. CN=AC Ra\xC3\xADz Certic\xC3\xA1mara S.A.
---
subject= C=US O=VeriSign, Inc. OU=Class 1 Public Primary Certification Authority
---
subject= C=TW O=TAIWAN-CA OU=Root CA CN=TWCA Root Certification Authority
---
subject= C=GB ST=Greater Manchester L=Salford O=Comodo CA Limited CN=AAA Certificate Services
---
subject= C=US O=Equifax OU=Equifax Secure Certificate Authority
---
subject= C=AT O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH OU=A-Trust-nQual-03 CN=A-Trust-nQual-03
---
subject= C=IE O=Baltimore OU=CyberTrust CN=Baltimore CyberTrust Root
---
subject= OU=GlobalSign Root CA - R3 O=GlobalSign CN=GlobalSign
---
subject= C=HK O=Hongkong Post CN=Hongkong Post Root CA 1
---
subject= C=US O=AffirmTrust CN=AffirmTrust Premium
---
subject= C=CH O=SwissSign AG CN=SwissSign Gold CA - G2
---
subject= C=US O=Equifax Secure Inc. CN=Equifax Secure eBusiness CA-1
---
subject= O=Digital Signature Trust Co. CN=DST Root CA X3
---
subject= C=NO O=Buypass AS-983163327 CN=Buypass Class 3 Root CA
---
subject= C=US O=GeoTrust Inc. CN=GeoTrust Global CA
---
subject= C=BM O=QuoVadis Limited OU=Root Certification Authority CN=QuoVadis Root Certification Authority
---
subject= O=Cisco Systems CN=Cisco Root CA 2048
---
subject= C=US ST=UT L=Salt Lake City O=The USERTRUST Network OU=http: www.usertrust.com CN=UTN-USERFirst-Object
---
subject= C=HU L=Budapest O=NetLock Halozatbiztonsagi Kft. OU=Tanusitvanykiadok CN=NetLock Expressz (Class C) Tanusitvanykiado
---
subject= O=Cisco Systems CN=Cisco Manufacturing CA
---
subject= L=ValiCert Validation Network O=ValiCert, Inc. OU=ValiCert Class 1 Policy Validation Authority CN=http: www.valicert.com emailAddress=info@valicert.com
---
subject= C=US O=Wells Fargo WellsSecure OU=Wells Fargo Bank NA CN=WellsSecure Public Root Certificate Authority
---
subject= C=US O=thawte, Inc. OU=Certification Services Division OU=(c) 2008 thawte, Inc. - For authorized use only CN=thawte Primary Root CA - G3
---
subject= C=IT L=Milan O=Actalis S.p.A. 03358520967 CN=Actalis Authentication Root CA
---
subject= O=Cisco CN=ACT2 SUDI CA

```
subject=  C=US O=AffirmTrust CN=AffirmTrust Commercial
---------------------------------------------------------------------------
subject=  C=RO O=certSIGN OU=certSIGN ROOT CA
---------------------------------------------------------------------------
subject=  C=GR O=Hellenic Academic and Research Institutions Cert. Authority CN=Hellenic Academic
and Research Institutions RootCA 2011
---------------------------------------------------------------------------
subject=  C=JP O=SECOM Trust Systems CO.,LTD. OU=Security Communication EV RootCA1
---------------------------------------------------------------------------
```

Certificate Authority Trust List