



Cisco Unified CallManager Administration Guide

Release 5.0(2)

Corporate 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: 408 526-4100

Text Part Number: OL-9414-01



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 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.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0502R)

Cisco Unified CallManager Administration Guide
Copyright © 2006 Cisco Systems, Inc. All rights reserved.



Preface xxiii

Purpose xxiii

Audience xxiv

Organization xxiv

Related Documentation xxv

Conventions xxv

Obtaining Documentation xxvi

 Cisco.com xxvii

 Product Documentation DVD xxvii

 Ordering Documentation xxvii

Documentation Feedback xxvii

Cisco Product Security Overview xxviii

 Reporting Security Problems in Cisco Products xxviii

Obtaining Technical Assistance xxix

 Cisco Technical Support & Documentation Website xxix

 Submitting a Service Request xxx

 Definitions of Service Request Severity xxx

Obtaining Additional Publications and Information xxx

PART 1

Cisco Unified CallManager

CHAPTER 1

Introduction 1-1

Key Features and Benefits 1-1

Browsing to Cisco Unified CallManager Administration 1-2

 Web Browsers 1-2

 Cisco Unified CallManager Administration Logon 1-3

 Cisco Unified CallManager Administration Log Off 1-3

 Hypertext Transfer Protocol Over Secure Sockets Layer (HTTPS) 1-4

 Using Internet Explorer and HTTPS with Cisco Unified CallManager Administration 1-4

 Using Netscape and HTTPS with Cisco Unified CallManager Administration 1-5

Navigating the Cisco Unified CallManager Administration Application 1-6

Accessibility 1-7

Where to Find More Information 1-7

Related Topics 1-8

PART 2

System Configuration

CHAPTER 2

Server Configuration 2-1

Finding a Server 2-1

Configuring a Server 2-2

Deleting a Server 2-3

Server Configuration Settings 2-4

Related Topics 2-4

CHAPTER 3

Cisco Unified CallManager Configuration 3-1

Finding a Cisco Unified CallManager 3-1

Updating a Cisco Unified CallManager 3-2

Cisco Unified CallManager Configuration Settings 3-3

Cisco CallManager Service Activation/Deactivation 3-6

 Cisco CallManager Service Activation 3-6

 Cisco CallManager Service Deactivation 3-6

Related Topics 3-7

CHAPTER 4

Cisco Unified CallManager Group Configuration 4-1

Finding a Cisco Unified CallManager Group 4-1

Configuring a Cisco Unified CallManager Group 4-3

Cisco Unified CallManager Group Configuration Settings 4-3

Deleting a Cisco Unified CallManager Group 4-4

Related Topics 4-5

CHAPTER 5

Presence Group Configuration 5-1

CHAPTER 6

Date/Time Group Configuration 6-1

Finding a Date/Time Group 6-1

Configuring a Date/Time Group 6-3

Date/Time Group Configuration Settings 6-4

Deleting a Date/Time Group 6-5

Related Topics 6-6

CHAPTER 7**Region Configuration 7-1**[Finding a Region 7-1](#)[Configuring a Region 7-2](#)[Region Configuration Settings 7-5](#)[Deleting a Region 7-7](#)[Related Topics 7-8](#)

CHAPTER 8**Phone NTP Reference Configuration 8-1**[Finding the Phone NTP References 8-1](#)[Configuring the Phone NTP References 8-2](#)[Phone NTP Reference Configuration Settings 8-3](#)[Deleting the Phone NTP Reference 8-4](#)[Related Topics 8-4](#)

CHAPTER 9**Device Pool Configuration 9-1**[Finding a Device Pool 9-1](#)[Configuring a Device Pool 9-3](#)[Device Pool Configuration Settings 9-4](#)[Deleting a Device Pool 9-7](#)[Related Topics 9-8](#)

CHAPTER 10**DHCP Server Configuration 10-1**[Activating DHCP Monitor Service 10-1](#)[Starting DHCP Monitor Service 10-2](#)[Finding a DHCP Server 10-2](#)[Configuring a DHCP Server 10-4](#)[DHCP Server Configuration Settings 10-4](#)[Deleting a DHCP Server 10-5](#)[Related Topics 10-6](#)

CHAPTER 11**DHCP Subnet Configuration 11-1**[Finding a DHCP Subnet 11-1](#)[Configuring a DHCP Subnet 11-2](#)[DHCP Subnet Configuration Settings 11-3](#)[Deleting a DHCP Subnet 11-4](#)[Related Topics 11-5](#)

CHAPTER 12**LDAP System Configuration 12-1**

- Updating LDAP System Information 12-1
- LDAP System Configuration Settings 12-2
- Related Topics 12-3

CHAPTER 13**LDAP Directory Configuration 13-1**

- Finding an LDAP Directory 13-1
- Configuring an LDAP Directory 13-2
- LDAP Directory Configuration Settings 13-3
- Deleting an LDAP Directory 13-5
- Related Topics 13-6

CHAPTER 14**LDAP Authentication Configuration 14-1**

- Updating LDAP Authentication Information 14-1
- LDAP Authentication Configuration Settings 14-2
- Related Topics 14-3

CHAPTER 15**Location Configuration 15-1**

- Finding a Location 15-1
- Configuring a Location 15-3
- Location Configuration Settings 15-4
- Deleting a Location 15-5
- Resynchronizing a Location Bandwidth 15-6
- Related Topics 15-7

CHAPTER 16**Survivable Remote Site Telephony Configuration 16-1**

- Finding an SRST Reference 16-1
- Configuring an SRST Reference 16-2
- Deleting an SRST Reference 16-3
- SRST Reference Configuration Settings 16-4
- Related Topics 16-5

CHAPTER 17**MLPP Domain Configuration 17-1**

- Finding an MLPP Domain 17-1
- Configuring an MLPP Domain 17-2
- MLPP Domain Configuration Settings 17-3

[Deleting an MLPP Domain](#) 17-3

[Related Topics](#) 17-4

CHAPTER 18

Enterprise Parameters Configuration 18-1

CHAPTER 19

Service Parameters Configuration 19-1

[Configuring Service Parameters for a Service on a Server](#) 19-2

[Displaying Parameters for a Service](#) 19-3

[Related Topics](#) 19-4

CHAPTER 20

SIP Phone Security Profile Configuration 20-1

CHAPTER 21

SIP Trunk Security Profile Configuration 21-1

CHAPTER 22

SCCP Phone Security Profile Configuration 22-1

CHAPTER 23

Application Server Configuration 23-1

[Configuring Application Servers](#) 23-1

[Deleting an Application Server](#) 23-2

[Application Server Configuration Settings](#) 23-3

[Finding an Application Server](#) 23-3

[Related Topics](#) 23-4

CHAPTER 24

License Unit Report 24-1

[Generating a License Unit Report](#) 24-1

[Related Topics](#) 24-2

CHAPTER 25

License Unit Calculator 25-1

[Calculating License Units](#) 25-1

[Related Topics](#) 25-1

CHAPTER 26

License File Upload 26-1

[Obtaining a License File](#) 26-1

[License File Contents](#) 26-2

[Uploading a License file](#) 26-3

[Related Topics](#) 26-4

CHAPTER 27

Autoregistration Configuration 27-1

- Enabling Autoregistration 27-1
- Disabling Autoregistration 27-2
- Autoregistration Configuration Settings 27-3
- Reusing Autoregistration Numbers 27-4
- Related Topics 27-5

PART 3

Call Routing Configuration

CHAPTER 28

Automated Alternate Routing Group Configuration 28-1

- Finding an AAR Group 28-1
- Configuring an AAR Group 28-2
- AAR Group Configuration Settings 28-3
- Deleting an AAR Group 28-4
- Related Topics 28-5

CHAPTER 29

Application Dial Rules Configuration 29-1

- Finding a Dial Rule 29-1
- Configuring Dial Rules 29-2
- Application Dial Rule Configuration Settings 29-3
- Deleting a Dial Rule 29-4
 - Reprioritizing a Dial Rule 29-4
- Related Topics 29-5

CHAPTER 30

Directory Lookup Dial Rules Configuration 30-1

- Finding a Directory Lookup Dial Rule 30-1
- Configuring Directory Lookup Dial Rules 30-2
- Directory Lookup Dial Rule Configuration Settings 30-3
- Deleting a Directory Lookup Dial Rule 30-4
- Related Topics 30-4

CHAPTER 31

SIP Dial Rules Configuration 31-1

- Finding a SIP Dial Rule 31-1
- Configuring SIP Dial Rules 31-3
- SIP Dial Rule Configuration Settings 31-3
 - Pattern Formats 31-5

SIP Dial Plan Rules Examples	31-6
Deleting a SIP Dial Rule	31-6
Resetting a SIP Dial Rule	31-7
Related Topics	31-7

CHAPTER 32

Route Filter Configuration	32-1
Finding a Route Filter	32-1
Configuring a Route Filter	32-3
Route Filter Configuration Settings	32-4
Adding Route Filter Clauses	32-4
Removing Route Filter Clauses	32-5
Deleting a Route Filter	32-5
Route Filter Tag Descriptions	32-6
Related Topics	32-9

CHAPTER 33

Route Group Configuration	33-1
Finding a Route Group	33-1
Configuring a Route Group	33-2
Route Group Configuration Settings	33-3
Adding Devices to a Route Group	33-5
Removing Devices from a Route Group	33-6
Deleting a Route Group	33-6
Related Topics	33-7

CHAPTER 34

Route List Configuration	34-1
Finding Route Lists	34-1
Adding a Route List	34-3
Adding Route Groups to a Route List	34-4
Removing Route Groups from a Route List	34-5
Changing the Order of Route Groups in a Route List	34-6
Deleting a Route List	34-6
Related Topics	34-7

CHAPTER 35

Route Pattern Configuration	35-1
Finding a Route Pattern	35-1
Configuring a Route Pattern	35-3

[Route Pattern Configuration Settings](#) 35-4

[Deleting a Route Pattern](#) 35-10

[Related Topics](#) 35-11

CHAPTER 36

Line Group Configuration 36-1

[Finding a Line Group](#) 36-1

[Configuring a Line Group](#) 36-2

[Line Group Configuration Settings](#) 36-3

[Adding Members to a Line Group](#) 36-8

[Removing Members from a Line Group](#) 36-9

[Deleting a Line Group](#) 36-9

[Related Topics](#) 36-10

CHAPTER 37

Hunt List Configuration 37-1

[Finding Hunt Lists](#) 37-1

[Adding a Hunt List](#) 37-3

[Adding Line Groups to a Hunt List](#) 37-4

[Removing Line Groups from a Hunt List](#) 37-5

[Changing the Order of Line Groups in a Hunt List](#) 37-5

[Deleting a Hunt List](#) 37-6

[Related Topics](#) 37-6

CHAPTER 38

Hunt Pilot Configuration 38-1

[Finding a Hunt Pilot](#) 38-1

[Configuring a Hunt Pilot](#) 38-3

[Deleting a Hunt Pilot](#) 38-4

[Hunt Pilot Configuration Settings](#) 38-4

[Related Topics](#) 38-11

CHAPTER 39

SIP Route Pattern Configuration 39-1

[Finding a SIP Route Pattern](#) 39-1

[Configuring a SIP Route Pattern](#) 39-3

[SIP Route Pattern Configuration Settings](#) 39-3

[Deleting a SIP Route Pattern](#) 39-6

[Related Topics](#) 39-7

CHAPTER 40**Time Period Configuration 40-1**

- Finding a Time Period 40-1
- Configuring a Time Period 40-2
- Deleting a Time Period 40-3
- Time Period Configuration Settings 40-4
- Related Topics 40-5

CHAPTER 41**Time Schedule Configuration 41-1**

- Finding a Time Schedule 41-1
- Configuring a Time Schedule 41-2
- Deleting a Time Schedule 41-3
- Time Schedule Configuration Settings 41-4
- Related Topics 41-5

CHAPTER 42**Partition Configuration 42-1**

- Finding a Partition 42-1
- Configuring a Partition 42-2
- Deleting a Partition 42-3
- Partition Configuration Settings 42-4
- Searching for a Partition 42-6
- Related Topics 42-6

CHAPTER 43**Calling Search Space Configuration 43-1**

- Finding a Calling Search Space 43-1
- Configuring a Calling Search Space 43-2
- Calling Search Space Configuration Settings 43-3
- Deleting a Calling Search Space 43-5
- Related Topics 43-6

CHAPTER 44**Client Matter Codes 44-1**

CHAPTER 45**Forced Authorization Code 45-1**

CHAPTER 46**Translation Pattern Configuration 46-1**

- Finding a Translation Pattern 46-1
- Configuring a Translation Pattern 46-3

Translation Pattern Configuration Settings 46-4

Deleting a Translation Pattern 46-9

Related Topics 46-9

CHAPTER 47

Call Park 47-1

CHAPTER 48

Call Pickup Group 48-1

CHAPTER 49

Directory Number Configuration 49-1

Directory Number Configuration Overview 49-1

Finding a Directory Number 49-2

Configuring a Directory Number 49-2

Removing a Directory Number from a Phone 49-4

Creating a Cisco Unity or Cisco Unity Connection Voice Mailbox 49-4

Directory Number Configuration Settings 49-6

Related Topics 49-23

CHAPTER 50

Meet-Me Number/Pattern Configuration 50-1

Finding a Meet-Me Number/Pattern 50-1

Configuring a Meet-Me Number/Pattern 50-2

Meet-Me Number/Pattern Configuration Settings 50-3

Deleting a Meet-Me Number/Pattern 50-4

Related Topics 50-5

CHAPTER 51

Route Plan Report 51-1

Viewing Route Plan Records 51-1

Deleting Unassigned Directory Numbers 51-3

Updating Unassigned Directory Numbers 51-3

Viewing Route Plan Reports in a File 51-4

Related Topics 51-5

CHAPTER 52

Installing Dial Plans 52-1

Finding a Dial Plan 52-2

Editing a Dial Plan 52-3

Installing a Dial Plan on Cisco Unified CallManager 52-3

Configuring Route Pattern Details for a non-NANP Dial Plan 52-4

Upgrading a Dial Plan 52-4

Uninstalling a Dial Plan	52-6
Restarting the Cisco CallManager Service	52-6
Related Topics	52-7

PART 4**Media Resource Configuration****CHAPTER 53****Annunciator Configuration 53-1**

Before You Begin	53-1
Finding an Annunciator	53-1
Updating an Annunciator	53-2
Annunciator Configuration Settings	53-3
Resetting an Annunciator	53-4
Related Topics	53-4

CHAPTER 54**Conference Bridge Configuration 54-1**

Finding a Conference Bridge	54-2
Understanding Software Conference Bridge Configuration	54-3
Software Conference Bridge Configuration Settings	54-3
Adding a Hardware Conference Device	54-4
Hardware Conference Bridge Configuration Settings	54-5
Adding a Cisco IOS Conference Bridge Device	54-5
Cisco IOS Conference Bridge Configuration Settings	54-6
Adding a Cisco Video Conference Bridge Device	54-6
Cisco Video Conference Bridge Configuration Settings	54-7
Adding a Cisco Unified CallManager Conference Bridge (WS-SVC-CMM) Device	54-8
Cisco Unified CallManager Conference Bridge (WS-SVC-CMM) Configuration Settings	54-9
Updating a Conference Device	54-10
Deleting a Conference Device	54-10
Where to Find More Information	54-11

CHAPTER 55**Media Termination Point Configuration 55-1**

Finding a Media Termination Point	55-2
Configuring a Media Termination Point	55-3
Cisco IOS Media Termination Point Configuration Settings	55-4
Deleting a Media Termination Point	55-4
Related Topics	55-5

CHAPTER 56**Music On Hold Audio Source Configuration 56-1**

CHAPTER 57**Music On Hold Fixed Audio Source Configuration 57-1**

CHAPTER 58**Music On Hold Server Configuration 58-1**

CHAPTER 59**Transcoder Configuration 59-1**[Finding a Transcoder 59-1](#)[Configuring a Transcoder 59-3](#)[Resetting a Transcoder 59-3](#)[Deleting a Transcoder 59-4](#)[Transcoder Configuration Settings 59-5](#)[Related Topics 59-6](#)

CHAPTER 60**Media Resource Group Configuration 60-1**[Finding a Media Resource Group 60-1](#)[Configuring a Media Resource Group 60-3](#)[Media Resource Group Configuration Settings 60-4](#)[Deleting a Media Resource Group 60-5](#)[Related Topics 60-6](#)

CHAPTER 61**Media Resource Group List Configuration 61-1**[Finding a Media Resource Group List 61-1](#)[Configuring a Media Resource Group List 61-2](#)[Media Resource Group List Configuration Settings 61-3](#)[Deleting a Media Resource Group List 61-4](#)[Related Topics 61-5](#)

PART 5

Voice Mail Configuration

CHAPTER 62**Cisco Voice-Mail Port Configuration 62-1**[Finding a Cisco Voice-Mail Port 62-1](#)[Configuring Cisco Voice-Mail Ports 62-3](#)[Cisco Voice-Mail Port Configuration Settings 62-4](#)[Deleting a Cisco Voice-Mail Port 62-6](#)[Related Topics 62-7](#)

CHAPTER 63**Cisco Voice Mail Port Wizard 63-1**

- [Adding a New Cisco Voice-Mail Server and Ports 63-1](#)
- [Adding Ports to an Existing Cisco Voice-Mail Server 63-5](#)
- [Deleting Ports from an Existing Cisco Voice-Mail Server 63-6](#)
- [Related Topics 63-6](#)

CHAPTER 64**Message Waiting Configuration 64-1**

- [Finding a Message Waiting Number 64-1](#)
- [Configuring Message Waiting 64-3](#)
- [Message Waiting Configuration Settings 64-3](#)
- [Related Topics 64-5](#)

CHAPTER 65**Cisco Voice-Mail Pilot Configuration 65-1**

- [Finding a Cisco Voice-Mail Pilot 65-1](#)
- [Configuring the Voice-Mail Pilot Number 65-3](#)
- [Voice-Mail Pilot Configuration Settings 65-3](#)
- [Deleting a Voice-Mail Pilot Number 65-4](#)
- [Related Topics 65-4](#)

CHAPTER 66**Voice-Mail Profile Configuration 66-1**

- [Finding Voice-Mail Profiles 66-1](#)
- [Configuring a Voice-Mail Profile 66-2](#)
- [Voice-Mail Profile Configuration Settings 66-3](#)
- [Deleting a Voice-Mail Profile 66-3](#)
- [Related Topics 66-4](#)

PART 6

Device Configuration

CHAPTER 67**CTI Route Point Configuration 67-1**

- [Finding CTI Route Points 67-1](#)
- [Configuring a CTI Route Point 67-2](#)
- [CTI Route Point Configuration Settings 67-3](#)
- [Deleting a CTI Route Point 67-4](#)
- [Resetting a CTI Route Point 67-5](#)
- [Related Topics 67-5](#)

CHAPTER 68**Gatekeeper Configuration 68-1**

- Finding a Gatekeeper 68-1
- Configuring a Gatekeeper 68-3
- Gatekeeper Configuration Settings 68-3
- Deleting a Gatekeeper 68-4
- Resetting a Gatekeeper 68-5
- Related Topics 68-6

CHAPTER 69**Gateway Configuration 69-1**

- Adding Gateways to Cisco Unified CallManager 69-1
 - Adding a Cisco IOS MGCP Gateway 69-2
 - Adding Ports to an MGCP Gateway 69-4
 - Adding FXS Ports to an MGCP Gateway 69-4
 - Adding FXO Ports to an MGCP Gateway 69-5
 - Adding Digital Access T1 Ports to an MGCP Gateway 69-7
 - Adding a Digital Access PRI Device to an MGCP Gateway 69-7
 - Adding a BRI Port to an MGCP Gateway 69-8
 - Adding a Cisco IOS SCCP Gateway 69-8
 - Adding a Non-IOS MGCP Gateway 69-9
 - Adding a Cisco IOS H.323 Gateway 69-10
 - Adding an Analog Access Gateway and Ports 69-11
 - Adding a Cisco VG248 Analog Phone Gateway 69-12
- Gateway Configuration Settings 69-13
 - MGCP Gateway Configuration Settings 69-14
 - FXS/FXO Port Configuration Settings 69-16
 - Digital Access PRI Port Configuration Settings 69-20
 - BRI Gateway Configuration Settings 69-33
 - Digital Access T1 Configuration Settings 69-40
 - H.323 Gateway Configuration Settings 69-44
 - Analog Access Gateway Configuration Settings 69-53
 - Cisco VG248 Gateway Configuration Settings 69-56
 - Cisco IOS SCCP Gateway Configuration Settings 69-57
- Port Configuration Settings 69-59
 - POTS Port Configuration Settings 69-60
 - Loop-Start Port Configuration Settings 69-62
 - Ground-Start Port Configuration Settings 69-63
 - E & M Port Configuration Settings 69-63

Finding Specific Gateways	69-66
Searching by Device Name	69-66
Searching by Description	69-67
Searching by Directory Number/Route Pattern	69-68
Searching by Calling Search Space	69-69
Searching by Device Pool	69-70
Searching by Route Group	69-71
Searching by Device Type	69-72
Modifying Gateways and Ports	69-74
Using Dependency Records	69-74
Deleting Gateways	69-74
Resetting and Restarting Gateways	69-75
Updating Gateways and Ports	69-76
Related Topics	69-76

CHAPTER 70

Cisco Unified IP Phone Configuration	70-1
Configuring Cisco Unified IP Phones	70-2
Displaying the MAC Address of a Phone	70-4
Resetting a Phone	70-4
Deleting a Phone	70-5
Phone Configuration Settings	70-6
Configuring Speed-Dial Buttons	70-23
Speed-Dial and Abbreviated-Dial Configuration Settings	70-23
BLF/SpeedDial Configuration Settings	70-24
Configuring Cisco Unified IP Phone Services	70-24
Subscribing to a Service	70-25
Updating Services	70-26
Unsubscribing from a Service	70-26
Configuring Service URL Buttons	70-27
Adding a Service URL Button	70-27
Modifying Phone Button Template Button Items	70-28
Finding a Phone	70-29
Related Topics	70-30

CHAPTER 71

Trunk Configuration	71-1
Finding a Trunk	71-1
Configuring a Trunk	71-2
Trunk Configuration Settings	71-3

[Deleting a Trunk](#) 71-27

[Resetting a Trunk](#) 71-27

[Related Topics](#) 71-28

CHAPTER 72

Device Defaults Configuration 72-1

[Updating Device Defaults](#) 72-1

[Device Defaults Configuration Settings](#) 72-2

[Related Topics](#) 72-2

CHAPTER 73

Device Firmware Load Information 73-1

[Finding Devices With Non-Default Firmware Loads](#) 73-1

CHAPTER 74

Default Device Profile Configuration 74-1

[Configuring a New Default Device Profile](#) 74-1

[Default Device Profile Configuration Settings](#) 74-2

[Deleting a Default Device Profile](#) 74-5

[Subscribing Services to a Default Device Profile](#) 74-5

[Related Topics](#) 74-5

CHAPTER 75

Device Profile Configuration 75-1

[Finding a Device Profile](#) 75-2

[Configuring a New User Device Profile](#) 75-2

[Deleting a User Device Profile](#) 75-5

[Updating Autogenerated Device Profiles](#) 75-6

[Configuring New Directory Numbers for Autogenerated Device Profiles](#) 75-7

[Related Topics](#) 75-8

CHAPTER 76

Phone Button Template Configuration 76-1

[Finding a Phone Button Template](#) 76-1

[Configuring Phone Button Templates](#) 76-2

[Configuring a Cisco IP Phone 7914 Expansion Module Phone Button Template](#) 76-4

[Phone Button Template Configuration Settings](#) 76-4

[Deleting a Phone Button Template](#) 76-5

[Related Topics](#) 76-6

CHAPTER 77**Softkey Template Configuration 77-1**

- Finding a Softkey Template 77-1
- Adding Nonstandard Softkey Templates 77-2
- Adding Application Softkeys to Nonstandard Softkey Templates 77-3
- Configuring Softkey Positions in a Nonstandard Softkey Template 77-4
- Modifying Softkey Templates 77-5
 - Renaming a Softkey Template 77-5
 - Deleting a Softkey Template 77-6
 - Updating a Softkey Template 77-7
- Assigning Softkey Templates to IP Phones 77-8
- Related Topics 77-8

CHAPTER 78**Cisco Unified IP Phone Services Configuration 78-1**

- Finding a Cisco Unified IP Phone Service 78-2
- Configuring a Cisco Unified IP Phone Service 78-3
- Cisco Unified IP Phone Service Configuration Settings 78-4
- Deleting a Cisco Unified IP Phone Service 78-5
- Configuring a Cisco Unified IP Phone Service Parameter 78-5
- Cisco Unified IP Phone Service Parameter Settings 78-7
- Deleting a Cisco Unified IP Phone Service Parameter 78-7
- Adding a Cisco Unified IP Phone Service to a Phone Button 78-8
- Related Topics 78-8

CHAPTER 79**SIP Profile Configuration 79-1**

- Finding SIP Profiles 79-1
- Configuring SIP Profiles 79-2
- SIP Profile Configuration Settings 79-2
- Deleting SIP Profiles 79-8
- Resetting a SIP Profile 79-9
- Related Topics 79-9

CHAPTER 80**Common Phone Profile Configuration 80-1**

- Finding Common Phone Profiles 80-1
- Configuring Common Phone Profiles 80-2
- Common Phone Profile Configuration Settings 80-3

Deleting Common Phone Profiles 80-3

Related Topics 80-4

PART 7

Application Configuration

CHAPTER 81

Cisco Unified CallManager Assistant Configuration Wizard 81-1

CHAPTER 82

Cisco Unified CallManager Attendant Console Pilot Point Configuration 82-1

CHAPTER 83

Cisco Unified CallManager Attendant Console User Configuration 83-1

CHAPTER 84

Cisco Unified CallManager Attendant Console User File Upload 84-1

CHAPTER 85

Plug-in Configuration 85-1

Installing Plug-ins 85-1

Updating the Plug-in URL 85-2

Update Plug-in URL Configuration Settings 85-3

PART 8

User Management Configuration

CHAPTER 86

Application User Configuration 86-1

Finding an Application User 86-1

Adding an Application User 86-3

Application User Configuration Settings 86-3

Changing an Application User Password 86-7

Configuring Application Profiles for Application Users 86-7

Associating Devices to an Application User 86-8

Related Topics 86-9

CHAPTER 87

End User Configuration 87-1

Finding an End User 87-1

Adding an End User 87-3

Creating a Cisco Unity or Cisco Unity Connection Voice Mailbox 87-3

End User Configuration Settings 87-5

Changing an End User Password 87-8

Changing an End User PIN 87-9

Configuring User-Related Information for End Users 87-9

Associating Devices to an End User	87-10
Associating Cisco Extension Mobility Profiles	87-12
Deleting an End User	87-13
Related Topics	87-13

CHAPTER 88**Role Configuration 88-1**

Finding a Role	88-2
Configuring a Role	88-3
Deleting a Role	88-4
Role Configuration Settings	88-4
Related Topics	88-5

CHAPTER 89**User Group Configuration 89-1**

Finding a User Group	89-1
Configuring a User Group	89-3
Deleting a User Group	89-3
Adding Users to a User Group	89-4
Deleting Users from a User Group	89-6
Assigning Roles to a User Group	89-6
Viewing a User's Roles, User Groups, and Permissions	89-7
Related Topics	89-8

CHAPTER 90**User/Phone Add Configuration 90-1**

Adding an End User and Phone	90-2
User and Device Configuration Settings	90-2
Related Topics	90-4

CHAPTER 91**Application User CAPF Profile Configuration 91-1****CHAPTER 92****End User CAPF Profile Configuration 92-1****CHAPTER 93****SIP Realm Configuration 93-1**

PART 9

Cisco Unified CallManager Bulk Administration

CHAPTER 94

Bulk Administration Tool 94-1

PART 10

Appendixes

APPENDIX A

Dependency Records A-1

Enabling Dependency Records A-1

Disabling Dependency Records A-2

Accessing Dependency Records A-2

Dependency Records Buttons A-4

APPENDIX B

Cisco Unity Voice-Mail Port Adjustments B-1

Cisco Unity Voice-Mail Port Changes B-1

Changes After Upgrading to Cisco Unified CallManager 4.0 or Later Releases B-1

Before Upgrading to Cisco Unified CallManager 4.0 or Later Releases B-3

Cisco Unity Failover Voice-Mail Port Setup B-3

APPENDIX C

Configuring Non-Cisco SIP Phones C-1

SIP Phone Configuration Differences C-1

Third-Party SIP Phone Configuration Checklist C-3

Where to Find More Information C-4

INDEX



Preface

This preface describes the purpose, audience, organization, and conventions of this guide and provides information on how to obtain related documentation.



Note

This document may not represent the latest Cisco product information available. You can obtain the most current documentation by accessing Cisco's product documentation page at this URL:

<http://www.cisco.com/univercd/home/home.htm>

The preface covers these topics:

- [Purpose, page xxiii](#)
- [Audience, page xxiv](#)
- [Organization, page xxiv](#)
- [Related Documentation, page xxv](#)
- [Conventions, page xxv](#)
- [Obtaining Documentation, page xxvi](#)
- [Documentation Feedback, page xxvii](#)
- [Cisco Product Security Overview, page xxviii](#)
- [Obtaining Technical Assistance, page xxix](#)
- [Obtaining Additional Publications and Information, page xxx](#)

Purpose

The *Cisco Unified CallManager Administration Guide* provides instructions for administering the Cisco Unified CallManager system. This guide includes descriptions of procedural tasks that you complete by using Cisco Unified CallManager Administration. The *Cisco Unified CallManager Administration Guide* also provides references for commands to assist you in using Cisco Unified CallManager. This book acts as a companion to the *Cisco Unified CallManager System Guide*, which provides conceptual information about Cisco Unified CallManager and its components as well as tips for setting up features by using Cisco Unified CallManager Administration.

Audience

The *Cisco Unified CallManager Administration Guide* provides information for network administrators who are responsible for managing the Cisco Unified CallManager system. This guide requires knowledge of telephony and IP networking technology.

Organization

The following table provides the organization of this guide.

Part	Description
Part 1	“Cisco Unified CallManager” Contains information about general topics that are related to the configuration and operation of Cisco Unified CallManager.
Part 2	“System Configuration” Contains information on how to configure the items in the Cisco Unified CallManager Administration System menu.
Part 3	“Call Routing Configuration” Contains information on how to configure call routing functions and features in Cisco Unified CallManager.
Part 4	“Media Resource Configuration” Contains information on how to configure media resources that are used in conjunction with Cisco Unified CallManager.
Part 5	“Voice Mail Configuration” Contains information on how to configure voice mail and messaging functions with Cisco Unified CallManager Administration.
Part 6	“Device Configuration” Contains information on how to configure devices in Cisco Unified CallManager.
Part 7	“Application Configuration” Contains information on how to configure plugin applications and application interfaces.
Part 8	“User Management Configuration” Contains information on how to configure application users, end users, roles, user groups, user-related CAPF profiles, and SIP realms in Cisco Unified CallManager.
Part 9	“Cisco Unified CallManager Bulk Administration” Contains information about Cisco Unified CallManager Bulk Administration.
Part 10	“Appendixes” Contains information about dependency records, adjustments for Cisco Unity voice-mail ports upon upgrade, and configuration of non-Cisco SIP phones.

Related Documentation

Refer to the following documents for further information about related Cisco IP telephony applications and products:

- *Installing Cisco Unified CallManager Release 5.0(2)*
- *Upgrading Cisco Unified CallManager Release 5.0(2)*
- *Release Notes for Cisco Unified CallManager Release 5.0(2)*
- *Cisco Unified CallManager System Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*
- *Cisco Unified CallManager Serviceability System Guide*
- *Cisco Unified CallManager Features and Services Guide*
- *Troubleshooting Guide for Cisco Unified CallManager*
- *Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager*
- *Cisco Unified CallManager Bulk Administration Guide*
- *Cisco Unified CallManager Security Guide*

Conventions

This document uses the following conventions.

Convention	Description
boldface font	Commands and keywords are in boldface .
<i>italic</i> font	Arguments for which you supply values are in <i>italics</i> .
[]	Elements in square brackets are optional.
{ x y z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in <code>screen font</code> .
boldface screen font	Information you must enter is in boldface screen font.
<i>italic screen</i> font	Arguments for which you supply values are in <i>italic screen</i> font.
→	This pointer highlights an important line of text in an example.

Convention	Description
^	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.

Notes use the following conventions:

**Note**

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

Timesavers use the following conventions:

**Timesaver**

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Tips use the following conventions:

**Tip**

Means *the information contains useful tips*.

Cautions use the following conventions:

**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 conventions:

**Warning**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

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

A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>. If you require further assistance please contact us by sending email to export@cisco.com.

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>



PART 1

Cisco Unified CallManager





Introduction

Cisco Unified CallManager serves as the software-based call-processing component of the Cisco Unified Communications family of products. A wide range of Cisco Media Convergence Servers provides high-availability server platforms for Cisco Unified CallManager call processing, services, and applications.

The Cisco Unified CallManager system extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. Additional data, voice, and video services, such as unified messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems, interact through Cisco Unified CallManager open telephony application programming interface (API).

Cisco Unified CallManager provides signaling and call control services to Cisco integrated telephony applications as well as third-party applications. Cisco Unified CallManager performs the following primary functions:

- Call processing
- Signaling and device control
- Dial plan administration
- Phone feature administration
- Directory services
- Operations, administration, maintenance, and provisioning (OAM&P)
- Programming interface to external voice-processing applications such as Cisco IP Communicator, Cisco Unified IP Interactive Voice Response (IP IVR), and Cisco Unified CallManager Attendant Console

Additional Information

See the [“Related Topics” section on page 1-8](#).

Key Features and Benefits

The Cisco Unified CallManager system includes a suite of integrated voice applications that perform voice-conferencing and manual attendant console functions. This suite of voice applications means that no need exists for special-purpose voice-processing hardware. Supplementary and enhanced services such as hold, transfer, forward, conference, multiple line appearances, automatic route selection, speed dial, last-number redial, and other features extend to IP phones and gateways. Because

Cisco Unified CallManager is a software application, enhancing its capabilities in production environments requires only upgrading software on the server platform, thereby avoiding expensive hardware upgrade costs.

Distribution of Cisco Unified CallManager and all Cisco Unified IP Phones, gateways, and applications across an IP network provides a distributed, virtual telephony network. This architecture improves system availability and scalability. Call admission control ensures that voice quality of service (QoS) is maintained across constricted WAN link and automatically diverts calls to alternate public switched telephone network (PSTN) routes when WAN bandwidth is not available.

A web-browsable interface to the configuration database provides the capability for remote device and system configuration. This interface also provides access to HTML-based online help for users and administrators.

Cisco Unified CallManager release 5.0, designed to work like an appliance, refers to the following functions:

- Cisco Unified CallManager servers can get preinstalled with software to ease customer and partner deployment and automatically search for updates and notify administrators when key security fixes and software upgrades are available for their system. This process comprises Electronic Software Upgrade Notification.
- You can upgrade Cisco Unified CallManager servers while they continue to process calls, so upgrades take place with minimal downtime.
- Cisco Unified CallManager supports the Asian and Middle Eastern markets by providing support for Unicode on higher resolution phone displays.
- Cisco Unified CallManager provides Fault, Configuration, Accounting, Performance, and Security (FCAPS).

Additional Information

See the [“Related Topics” section on page 1-8](#).

Browsing to Cisco Unified CallManager Administration

You access the Cisco Unified CallManager Administration program from a PC that is not the web server or has Cisco Unified CallManager installed. No browser software exists on the server. See the [“Web Browsers” section on page 1-2](#) for more information on browsing to the server.

Additional Information

See the [“Related Topics” section on page 1-8](#).

Web Browsers

Cisco Unified CallManager Administration supports the following Microsoft Windows operating system browsers:

- Microsoft Internet Explorer (IE) 6.0 or higher
- Netscape 7.1 or higher

From any user PC in your network, browse into a server that is running Cisco Unified CallManager Administration and log in with administrative privileges.

**Note**

Simultaneous logon to Cisco Unified CallManager Administration by a large number of users can cause performance to suffer. Try to limit the number of users and administrators that are logged on simultaneously.

Cisco Unified CallManager Administration Logon

Use the following procedure to log on to Cisco Unified CallManager Administration.

Procedure

Use the following procedure to browse into the server and log on to Cisco Unified CallManager Administration.

-
- Step 1** Start your preferred operating system browser.
- Step 2** In the address bar of the web browser, enter the following case-sensitive URL:
`https://<Unified CM-server-name>:{8443}/ccmadmin/showHome.do`
where: *<Unified CM-server-name>* equals the name or IP address of the server

**Note**

You can optionally specify a port number.

- Step 3** A Security Alert dialog box displays. Click the appropriate button.
- Step 4** At the Logon window, enter the application user password that you specified during Cisco Unified CallManager installation and click **Submit**.
The Cisco Unified CallManager Administration window displays (see [Figure 1-1](#)).

**Note**

For security purposes, Cisco Unified CallManager Administration logs you out after 30 minutes, and you must log back in.

Additional Information

See the [“Related Topics”](#) section on page 1-8.

Cisco Unified CallManager Administration Log Off

Procedure

Use the following procedure to log off Cisco Unified CallManager Administration.

-
- Step 1** From the main Cisco Unified CallManager Administration window, click the **Log Off** button that is in the upper, right corner (see [Figure 1-1](#)).
- Step 2** The Logon window displays.
-

Additional Information

See the [“Related Topics” section on page 1-8](#).

Hypertext Transfer Protocol Over Secure Sockets Layer (HTTPS)

Hypertext Transfer Protocol over Secure Sockets Layer (SSL), which secures communication between the browser client and the web server (for Microsoft Windows users), uses a certificate and a public key to encrypt the data that is transferred over the internet. HTTPS also ensures that the user login password transports securely via the web. The following Cisco Unified CallManager applications support HTTPS, which ensures the identity of the server: Cisco Unified CallManager Administration, Cisco Unified CallManager Serviceability, the Cisco Unified CallManager User Options, Trace Collection Tool, the Real-Time Monitoring Tool (RTMT), and the XML (AXL) application programming interface.

A self-signed certificate gets generated on the web server at installation (the certificate also gets migrated during upgrades).

**Note**

If you access the web application by using the hostname and install the certificate in the trusted folder and then try to access the application by using the localhost or IP address, the Security Alert dialog box displays to indicate that the name of the security certificate does not match the name of the site.

If you use the localhost, the IP address, or the hostname in the URL to access the application that supports HTTPS, you must save the certificate in the trusted folder for each of type of URL (with the local host, IP address, and so on); otherwise, the Security Alert dialog box displays for each type.

Using Internet Explorer and HTTPS with Cisco Unified CallManager Administration

The following section describes how to save the CA Root certificate in the trusted folder, so the Security Alert dialog box does not display each time that you access the web application. The first time that you (or a user) accesses Cisco Unified CallManager Administration or other Cisco Unified CallManager SSL-enabled virtual directories after the Cisco Unified CallManager 5.0 installation/upgrade from a browser client, a Security Alert dialog box asks whether you trust the server. When the dialog box displays, you must perform one of the following tasks:

- By clicking Yes, you choose to trust the certificate for the current web session only. If you trust the certificate for the current session only, the Security Alert dialog box displays each time that you access the application; that is, until you install the certificate in the trusted folder.
- By clicking View Certificate > Install Certificate, you indicate that you intend to perform certificate installation tasks, so you always trust the certificate. If you install the certificate in the trusted folder, the Security Alert dialog box does not display each time that you access the web application.
- By clicking No, you cancel the action. No authentication occurs, and you cannot access the web application. To access the web application, you must click Yes or install the certificate via the View Certificate > Install Certificate option.

For other tasks that you can perform in the Security Alert dialog box, refer to the *Cisco Unified CallManager Security Guide*.

Procedure

- Step 1** Browse to the application on the web server.
- Step 2** When the Security Alert dialog box displays, click **View Certificate**.
- Step 3** In the Certificate pane, click **Install Certificate**.
- Step 4** Click **Next**.
- Step 5** Click the **Place all certificates in the following store** radio button; click **Browse**.
- Step 6** Browse to **Trusted Root Certification Authorities**.
- Step 7** Click **Next**.
- Step 8** Click **Finish**.
- Step 9** To install the certificate, click **Yes**.
A message states that the import was successful. Click **OK**.
- Step 10** In the lower, right corner of the dialog box, click **OK**.
- Step 11** To trust the certificate, so you do not receive the dialog box again, click **Yes**.



Note If you use the localhost, the IP address, or the hostname in the URL to access the application that supports HTTPS, you must save the certificate in the trusted folder for each of type of URL (with the local host, IP address, and so on); otherwise, the Security Alert dialog box displays for each type.

Additional Information

See the [“Related Topics”](#) section on page 1-8.

Using Netscape and HTTPS with Cisco Unified CallManager Administration

When you use HTTPS with Netscape, you can view the certificate credentials, trust the certificate for one session, trust the certificate until it expires, or not trust the certificate at all.



Tip If you trust the certificate for one session only, you must repeat the following procedure each time that you access the HTTPS-supported application. If you do not trust the certificate, you cannot access the application.

Perform the following procedure to save the certificate to the trusted folder:

Procedure

- Step 1** Browse to the application, for example, Cisco Unified CallManager Administration, by using Netscape. The certificate authority dialog box displays.

- Step 2** Click one of the following radio buttons:
- Accept this certificate for this session
 - Do not accept this certificate and do not connect
 - Accept this certificate forever (until it expires)



Note If you choose Do not accept, the application does not display.



Note To view the certificate credentials before you continue, click **Examine Certificate**. Review the credentials, and click **Close**.

- Step 3** Click **OK**.
The Security Warning dialog box displays.
- Step 4** Click **OK**.

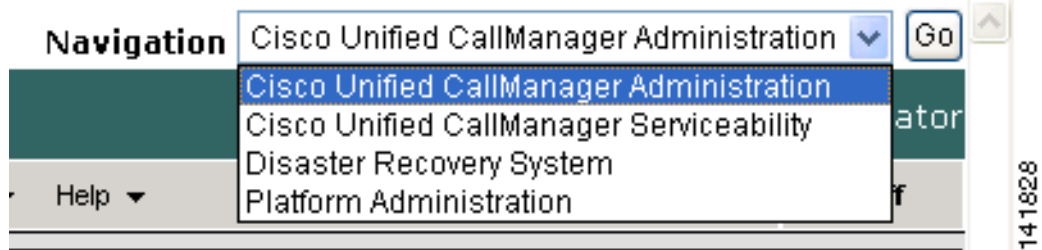
Additional Information

See the [“Related Topics” section on page 1-8](#).

Navigating the Cisco Unified CallManager Administration Application

After you log on, the main Cisco Unified CallManager Administration window displays. The window includes the drop-down list box in the upper, right corner called **Navigation** (see [Figure 1-1](#)). To access the applications in the drop-down list box, choose the program that you want and click **Go**. The choices in the drop-down list box include the following Cisco Unified CallManager applications:

- Cisco Unified CallManager Administration—Shows the default when you access Cisco Unified CallManager. Use Cisco Unified CallManager Administration to configure system parameters, route plans, devices, and much more.
- Cisco Unified CallManager Serviceability—Takes you to the main Cisco Unified CallManager Serviceability window that is used to configure trace files and alarms and to activate and deactivate services.
- Disaster Recovery System—Takes you to the Cisco Disaster Recovery System, a program that provides full data backup and restore capabilities for all servers in a Cisco Unified CallManager cluster.
- Platform Administration—Takes you to a logon window, so you can configure and administer the Cisco Unified CallManager platform.

Figure 1-1 Cisco Unified CallManager Administration Navigation

These applications include additional security, so you must enter a userid and password before you can access these programs.

Additional Information

See the [“Related Topics”](#) section on page 1-8.

Accessibility

Cisco Unified CallManager Administration and Cisco Unified CallManager User Options provide functionality for users that allows them to access buttons on the window without using a mouse. You can perform the following procedures from any point on the window, so the user does not have to scroll or tab through various fields.

Accessing the Icons in the Window

Many of the windows in Cisco Unified CallManager and Cisco PCA have icons that display at the top of the window; for example, an icon of a disk for Save, an icon that is a plus sign (+) for Add, and so on. To access these icons, perform the following procedure.

1. Press **Alt**, press **1**, then press **Tab**. The cursor will highlight the first icon from the left. To move to the next icon, press **Tab** again.
2. Press **Enter**. The system performs the function of the icon; for example, Add.

Accessing the Buttons in the Window

Many of the windows in Cisco Unified CallManager and Cisco PCA have buttons that display at the bottom of the window; for example, a button for Save, a button for Add, and so on. To access these buttons, perform the following procedure.

1. Press **Alt**, press **2**, and then press **Tab**. The cursor will highlight the first button from the left. To move to the next button, press **Tab** again.
2. Press **Enter**. The function of the button gets performed; for example, Save.

Where to Find More Information

- *Cisco Unified CallManager System Guide*
- *Cisco Unified CallManager Features and Services Guide*

- *Cisco Unified CallManager Serviceability System Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*
- *Cisco CDR Analysis and Reporting Administration Guide*
- *Cisco Unified Communications Solution Reference Network Design*
- *Installing Cisco Unified CallManager Release 5.0(2)*
- *Upgrading Cisco Unified CallManager Release 5.0(2)*
- *Cisco Unified CallManager Security Guide*
- *Cisco Unified Communications Operating System Administration Guide*
- *Disaster Recovery System Administration Guide*

Related Topics

- [Introduction, page 1-1](#)
- [Key Features and Benefits, page 1-1](#)
- [Browsing to Cisco Unified CallManager Administration, page 1-2](#)
- [Using Internet Explorer and HTTPS with Cisco Unified CallManager Administration, page 1-4](#)
- [Hypertext Transfer Protocol Over Secure Sockets Layer \(HTTPS\), page 1-4](#)
- [Navigating the Cisco Unified CallManager Administration Application, page 1-6](#)
- [Accessibility, page 1-7](#)
- [Where to Find More Information, page 1-7](#)



PART 2

System Configuration





Server Configuration

Use the server configuration to specify the address of the server where Cisco Unified CallManager is installed. If your network uses Domain Name System (DNS) services, you can specify the host name of the server. If your network does not use DNS services, you must specify the Internet Protocol (IP) address of the server.



Note

You must update the DNS server with the appropriate Cisco Unified CallManager name and address information before using that information to configure the Cisco Unified CallManager server.

For information about how to add, update, or delete a server address in the Cisco Unified CallManager database, see the [“Related Topics” section on page 2-4](#).

Finding a Server

Because you might have several servers in your network, Cisco Unified CallManager lets you locate specific servers on the basis of specific criteria. Use the following procedure to locate servers.



Note

During your work in a browser session, your find/list search preferences are stored in the cookies on the client machine. If you navigate to other menu items and return to this menu item, or if you close the browser and then reopen a new browser window, your Cisco Unified CallManager search preferences are retained until you modify your search.

Procedure

Step 1 Choose **System > Server**.

The Find and List Servers window displays. Use the two drop-down list boxes to search for a server.

Step 2 From the first Find Servers window drop-down list box, choose one of the following criteria:

- Host Name/IP Address
- Description

From the second Find Servers window drop-down list box, choose one of the following criteria:

- begins with
- contains

- is exactly
- ends with
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**.



Tip

To find all servers that are registered in the database, click **Find** without entering any search text.

A list of discovered servers displays by

- Host Name/IP Address
- Description

From the Find and List Servers window, you can also specify how many items per page to display.



Note

You can delete multiple servers from the Find and List Servers window by checking the check boxes next to the appropriate servers and clicking **Delete Selected**. You can delete all servers in the window by checking the check box in the Matching records title bar and clicking **Delete Selected**.

Step 4 From the list of records, click the Server name that matches your search criteria.

The window displays the server that you choose.

Additional Information

See the [“Related Topics” section on page 2-4](#).

Configuring a Server

This section describes how to add or update a server address to the Cisco Unified CallManager database.

Before You Begin

The following guideline applies to adding a server:

- Make sure that you only add each server once on the Server Configuration window. If you add a server using the host name and add the same server using the IP address, Cisco Unified CallManager cannot accurately determine component versions for the server after a Cisco Unified CallManager upgrade. If you have two entries in Cisco Unified CallManager Administration for the same server, delete one of the entries before you upgrade (see the [“Deleting a Server” section on page 2-3](#)).

Procedure

- Step 1** Perform one of the following tasks:
- To add a server, choose **System > Server** and click **Add New**.
 - To update a server, find the server by using the procedure in the [“Finding a Server” section on page 2-1](#).
- The Server Configuration window displays.
- Step 2** Enter the appropriate settings as described in [Table 2-1](#).
- Step 3** Click the **Save** icon that displays in the tool bar in the upper, left corner of the window (or click the **Save** button that displays at the bottom of the window) to save the data and to add the server to the database.
- Changes to the server configuration do not take effect until you restart Cisco Unified CallManager. For information about restarting the Cisco Unified CallManager service, refer to the *Cisco Unified CallManager Serviceability Administration Guide*.



Note

When you perform a fresh installation of Cisco Unified CallManager, you must define any subsequent servers (nodes) in the Cisco Unified CallManager Administration Server Configuration window before you can install the Cisco Unified CallManager software on each subsequent server. To define a subsequent node, click **Add New**, as described in [Step 1](#) above, and configure the server. After you add the subsequent server, you can then install the Cisco Unified CallManager software on that server.

Additional Information

See the [“Related Topics” section on page 2-4](#).

Deleting a Server

This section describes how to delete a server from the Cisco Unified CallManager database.

Before You Begin

If the dependency records feature is not enabled for the system, the dependency records summary window displays a message showing the action you can take to enable the dependency records; the message also displays information about high CPU consumption related to the dependency records feature. For more information about dependency records, refer to the [“Accessing Dependency Records” section on page A-2](#).

Procedure

- Step 1** Find the server by using the procedure in the [“Finding a Server” section on page 2-1](#).
- Step 2** From list of matching records, choose the server that you want to delete.
- Step 3** Click the **Delete Selected Item** icon that displays in the tool bar in the upper, left corner of the window (or click the **Delete Selected** button that displays at the bottom of the window) to delete the server.
- If the server is not in use, Cisco Unified CallManager deletes it. If it is in use, an error message displays.

Changes to the server configuration do not take effect until you restart Cisco Unified CallManager. For information about restarting the Cisco CallManager service, refer to the *Cisco Unified CallManager Serviceability Administration Guide*.

Additional Information

See the [“Related Topics”](#) section on page 2-4.

Server Configuration Settings

[Table 2-1](#) describes the server configuration settings. For related procedures, see the [“Related Topics”](#) section on page 2-4.

Table 2-1 **Server Configuration Settings**

Server Information Field	Description
Host Name/ IP Address	If your network uses DNS services, you can enter the host name of the Cisco Unified CallManager server. Otherwise, you must enter the full IP address of the server. Note You must update the DNS server with the appropriate Cisco Unified CallManager name and address information before using that information here.
MAC Address	This entry is optional. Enter the media access control (MAC) address of the network interface card (NIC) in the Cisco Unified CallManager server. The MAC address specifies the permanent hardware address of the NIC. Tip If you plan to move the server periodically to different locations on the network, you must enter the MAC address, so other devices on the network can always identify the server. If you do not plan to relocate the server, entry of the MAC address is optional.
Description	This entry is optional. Enter a description of the server.

Related Topics

- [Finding a Server, page 2-1](#)
- [Configuring a Server, page 2-2](#)
- [Deleting a Server, page 2-3](#)
- [Server Configuration Settings, page 2-4](#)
- [Cisco Unified CallManager Configuration, page 3-1](#)



Cisco Unified CallManager Configuration

Use Cisco Unified CallManager configuration to specify the ports and other properties for each Cisco Unified CallManager that is installed in the same cluster. A cluster comprises a set of Cisco Unified CallManagers that enables redundancy.

For the first node in a Cisco Unified CallManager cluster, the server gets automatically added as part of the installation. To add additional Cisco Unified CallManagers to a cluster, the administrator must configure a server (by using Server Configuration) and then add the Cisco Unified CallManager (by using Cisco Unified CallManager Configuration). This procedure is repeated for each Cisco Unified CallManager that is in the cluster.

Use the following topics to find and update a Cisco Unified CallManager configuration or to view system component version information:

- [Finding a Cisco Unified CallManager, page 3-1](#)
- [Updating a Cisco Unified CallManager, page 3-2](#)
- [Cisco Unified CallManager Configuration Settings, page 3-3](#)
- [Cisco CallManager Service Activation/Deactivation, page 3-6](#)
- [Related Topics, page 3-7](#)

Finding a Cisco Unified CallManager

Because you may have several Cisco Unified CallManagers in your network, Cisco Unified CallManager Administration lets you locate specific Cisco Unified CallManagers on the basis of specific criteria. Use the following procedure to locate Cisco Unified CallManagers.



Note

During your work in a browser session, your find/list search preferences are stored in the cookies on the client machine. If you navigate to other menu items and return to this menu item, or if you close the browser and then reopen a new browser window, the system retains your Cisco Unified CallManager search preferences until you modify your search.

Procedure

Step 1 Choose **System** > Cisco Unified CallManager.

The Find and List Cisco Unified CallManagers window displays. Use the two drop-down list boxes to search for a Cisco Unified CallManager.

Step 2 From the first Find Cisco Unified CallManagers window drop-down list box, choose one of the following criteria:

- Name
- Description

From the second Find Cisco Unified CallManagers window drop-down list box, choose one of the following criteria:

- begins with
- contains
- is exactly
- ends with
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**.



Tip To find all Cisco Unified CallManagers that are registered in the database, click **Find** without entering any search text.

A list of discovered Cisco Unified CallManagers displays by

- Cisco Unified CallManager name
- Description

From the Find and List Cisco Unified CallManagers window, you can also specify how many rows per page to display.

Step 4 From the list of records, click the Cisco Unified CallManager name that matches your search criteria. The window displays the Cisco Unified CallManager that you chose.

Additional Information

See the [“Related Topics” section on page 3-7](#).

Updating a Cisco Unified CallManager

This section describes how to update a Cisco Unified CallManager.

Procedure

Step 1 Choose **System** > Cisco Unified CallManager.

The Find and List Cisco Unified CallManagers window displays.

Step 2 To update a Cisco Unified CallManager, locate the appropriate Cisco Unified CallManager as described in [Finding a Cisco Unified CallManager, page 3-1](#). Click the Cisco Unified CallManager that you want to update and continue with [Step 3](#).

- Step 3** Enter the appropriate settings as described in [Table 3-1](#).
- Step 4** Click **Save**.

Additional Information

See the [“Related Topics”](#) section on page 3-7.

Cisco Unified CallManager Configuration Settings

[Table 3-1](#) describes the Cisco Unified CallManager configuration settings. For related procedures, see the [“Related Topics”](#) section on page 3-7.

Table 3-1 *Cisco Unified CallManager Configuration Settings*

Field	Description
Server Information	
Cisco Unified CallManager Server	This read-only field displays the server where this Cisco Unified CallManager is installed.
Cisco Unified CallManager Name	Enter the name that you want to assign to this Cisco Unified CallManager.
Description	Enter a description of the Cisco Unified CallManager.
Auto-registration Information	
Starting Directory Number	Enter the first directory number to use for autoregistration of devices.
Ending Directory Number	Enter the last directory number to use for autoregistration of devices. Note Specifying a valid range of directory numbers in the Starting Directory Number and Ending Directory Number fields automatically enables autoregistration. Setting the starting and ending directory numbers to the same value disables autoregistration.

Table 3-1 Cisco Unified CallManager Configuration Settings (continued)

Field	Description
Partition	If you are not using partitions, choose <None>. If you are using partitions, choose the partition to which autoregistered directory numbers belong from the drop-down list box. Tip You must choose a range for autoregistration before you can choose a partition, external phone number mask or voice messaging box mask. If more than 250 partitions exist, the ellipsis (...) button displays next to the drop-down list box. 1. To display the Select Partition window, click the (...) button. 2. In the List items where Name contains field, enter a partial partition name. 3. In the list of partitions that displays in the Select item to use box, click the desired partition name. 4. Click OK.
External Phone Number Mask	Specify the mask that is used to format caller ID information for external (outbound) calls that are made from the autoregistered devices. • The mask can contain up to 50 characters. • Enter the literal digits that you want to appear in the caller ID information and use Xs to represent the directory number of the autoregistered device. See the following examples: • If you specify a mask of 972813XXXX, an external call from extension 1234 displays a caller ID number of 9728131234 if the Use External Phone Number Mask option is checked on the route pattern that is used to make the external call. • If you specify a mask of all literal digits, such as 9728135000 to represent a main attendant number, that literal number (9728135000) displays as the caller ID for an external call from any autoregistered device.

Table 3-1 Cisco Unified CallManager Configuration Settings (continued)

Field	Description
Auto-registration Disabled on this Cisco Unified CallManager	Cisco Unified CallManager disables the autoregistration by default to prevent unauthorized connections to the network. You can choose to enable or disable autoregistration by one of the following options: - To enable autoregistration for this Cisco Unified CallManager, uncheck the Auto-registration Disabled check box. - To disable autoregistration for this Cisco Unified CallManager, check the Auto-registration Disabled check box. - When autoregistration is disabled, you must configure the directory numbers manually whenever you add new devices to your network. - Setting the Starting Directory Number and Ending Directory Number to the same value also disables autoregistration. - If starting and ending directory numbers are currently specified when you disable autoregistration by checking this option, Cisco Unified CallManager sets the starting and ending directory numbers to the same value. Cisco Unified CallManager resets the partition and external phone mask information when autoregistration is disabled.
Cisco Unified CallManager TCP Port Settings for This Server	
Ethernet Phone Port	Cisco Unified CallManager uses this TCP port to communicate with the Cisco Unified IP Phones (SCCP only) on the network. - Accept the default port value of 2000 unless this port is already in use on your system. Choosing 2000 identifies this port as non-secure. - Ensure all port entries are unique. - Valid port numbers range from 1024 to 49151. - Refer to the <i>Cisco Unified CallManager Security Guide</i> for information about security configurations.
MGCP Listen Port	Cisco Unified CallManager uses this TCP port to detect messages from its associated MGCP gateway. - Accept the default port of 2427 unless this port is already in use on your system. - Ensure all port entries are unique. - Valid port numbers range from 1024 to 49151.
MGCP Keep-alive Port	Cisco Unified CallManager uses this TCP port to exchange keepalive messages with its associated MGCP gateway. - Accept the default port of 2428 unless this port is already in use on your system. - Ensure all port entries are unique. - Valid port numbers range from 1024 to 49151.

Table 3-1 Cisco Unified CallManager Configuration Settings (continued)

Field	Description
SIP Phone Port	This field specifies the port number that Cisco Unified CallManager uses to listen for SIP line registrations over TCP and UDP.
SIP Phone Secure Port	This field specifies the port number that Cisco Unified CallManager uses to listen for SIP line registrations over TLS. Refer to the <i>Cisco Unified CallManager Security Guide</i> for information about security configurations.

Cisco CallManager Service Activation/Deactivation

The following requirements apply to Cisco CallManager service activation and deactivation:

- [Cisco CallManager Service Activation, page 3-6](#)
- [Cisco CallManager Service Deactivation, page 3-6](#)

Additional Information

See the “[Related Topics](#)” section on page 3-7.

Cisco CallManager Service Activation

When you perform a new Cisco Unified CallManager installation, you must follow these steps in sequence:

1. Add the Server. Cisco Unified CallManagers automatically get added when a server gets configured.
2. Activate the Cisco CallManager service, as described in the *Cisco Unified CallManager Serviceability Administration Guide*.

A message displays if you do not follow this sequence.

Additional Information

See the “[Related Topics](#)” section on page 3-7.

Cisco CallManager Service Deactivation

You can deactivate the Cisco CallManager service in Cisco Unified CallManager Serviceability. When you deactivate the Cisco CallManager service, the Cisco Unified CallManager where you deactivated the service becomes inactive for use.



Note

From Cisco Unified CallManager Serviceability, you can view the status of the Cisco Unified CallManager by accessing **Tools > Service Activation**.

When the Cisco CallManager service is deactivated, no one can make calls on that Cisco Unified CallManager.

You may still be able to perform configuration operations on a deactivated Cisco Unified CallManager if the Cisco CallManager Administration web service is active and the database is up and running.

When you reactivate the Cisco CallManager service on the Cisco Unified CallManager, the database automatically re-creates the Cisco Unified CallManager by retaining the original configuration (server name or IP address). This Cisco Unified CallManager then becomes active; you can verify that the Cisco CallManager service is running by accessing **Tools > Control Center - Feature Services** in Cisco Unified CallManager Serviceability.

For more information about Service Activation, refer to the *Cisco Unified CallManager Serviceability System Guide* and the *Cisco Unified CallManager Serviceability Administration Guide*.

Additional Information

See the [“Related Topics” section on page 3-7](#).

Related Topics

- [Finding a Cisco Unified CallManager, page 3-1](#)
- [Updating a Cisco Unified CallManager, page 3-2](#)
- [Cisco Unified CallManager Configuration Settings, page 3-3](#)
- [Cisco CallManager Service Activation/Deactivation, page 3-6](#)
- [Server Configuration, page 2-1](#)
- *Cisco Unified CallManager Security Guide*



Cisco Unified CallManager Group Configuration

A Cisco Unified CallManager Group specifies a prioritized list of up to three Cisco Unified CallManagers. The first Cisco Unified CallManager in the list serves as the primary Cisco Unified CallManager for that group, and the other members of the group serve as secondary and tertiary (backup) Cisco Unified CallManagers.

Each device pool has one Cisco Unified CallManager Group assigned to it. When a device registers, it attempts to connect to the primary (first) Cisco Unified CallManager in the group that is assigned to its device pool. If the primary Cisco Unified CallManager is not available, the device tries to connect to the next Cisco Unified CallManager that is listed in the group, and so on.

Cisco Unified CallManager Groups provide important features for your system:

- Redundancy—This feature enables you to designate a primary and backup Cisco Unified CallManagers for each group.
- Call processing load balancing—This feature enables you to distribute the control of devices across multiple Cisco Unified CallManagers.

For most systems, you need to have multiple groups, and you need to assign a single Cisco Unified CallManager to multiple groups to achieve better load distribution and redundancy.

Use the following topics to add, update, or delete a Cisco Unified CallManager group:

- [Finding a Cisco Unified CallManager Group, page 4-1](#)
- [Configuring a Cisco Unified CallManager Group, page 4-3](#)
- [Cisco Unified CallManager Group Configuration Settings, page 4-3](#)
- [Deleting a Cisco Unified CallManager Group, page 4-4](#)
- [Related Topics, page 4-5](#)

Finding a Cisco Unified CallManager Group

Because you might have several Cisco Unified CallManager groups in your network, Cisco Unified CallManager Administration lets you locate specific Cisco Unified CallManager groups on the basis of specific criteria. Use the following procedure to locate Cisco Unified CallManager groups.

**Note**

During your work in a browser session, your find/list search preferences are stored in the cookies on the client machine. If you navigate to other menu items and return to this menu item, or if you close the browser and then reopen a new browser window, your Cisco Unified CallManager search preferences are retained until you modify your search.

Procedure

Step 1 Choose **System > Cisco Unified CallManager Group**.

The Find and List Cisco Unified CallManager Groups window displays. Use the drop-down list box to search for a Cisco Unified CallManager Group.

Step 2 From the Find Cisco Unified CallManager Groups window drop-down list box, choose one of the following criteria:

- begins with
- contains
- is exactly
- ends with
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**.

**Tip**

To find all Cisco Unified CallManager groups that are registered in the database, click **Find** without entering any search text.

A list of discovered Cisco Unified CallManager groups displays by

- Cisco Unified CallManager Group name
- Auto-registration Cisco Unified CallManager Group

From the Find and List Cisco Unified CallManager Groups window, you can also specify how many items per page to display.

**Note**

You can delete multiple Cisco Unified CallManager groups from the Find and List Cisco Unified CallManager Groups window by checking the check boxes next to the appropriate Cisco Unified CallManager groups and clicking **Delete Selected**. You can delete all Cisco Unified CallManager groups in the window by checking the check box in the Matching records title bar and clicking **Delete Selected**.

Step 4 From the list of records, click the Cisco Unified CallManager Group name that matches your search criteria.

The window displays the Cisco Unified CallManager group that you chose.

Additional Information

See the [“Related Topics” section on page 4-5](#).

Configuring a Cisco Unified CallManager Group

This section describes how to add, copy, or update a Cisco Unified CallManager group.

Before You Begin

Before configuring a Cisco Unified CallManager group, you must configure the Cisco Unified CallManagers that you want to assign as members of that group. See the [“Updating a Cisco Unified CallManager” section on page 3-2](#) for more information.

Procedure

Step 1 Choose **System > Cisco Unified CallManager Group**.

The Find and List Cisco Unified CallManager Groups displays.

Step 2 Perform one of the following tasks:

- To copy an existing Cisco Unified CallManager Group, locate the appropriate Cisco Unified CallManager Group as described in the [“Finding a Cisco Unified CallManager Group” section on page 4-1](#), choose the Cisco Unified CallManager Group that you want to copy, click **Copy**, and continue with [Step 3](#).
- To add a new Cisco Unified CallManager Group, click Add New button, and continue with [Step 3](#).
- To update an existing Cisco Unified CallManager Group, locate the appropriate Cisco Unified CallManager Group as described in the [“Finding a Cisco Unified CallManager Group” section on page 4-1](#), and continue with [Step 3](#).

Step 3 Enter the appropriate settings as described in [Table 4-1](#).

Step 4 Click the **Save** icon that displays in the tool bar in the upper, left corner of the window (or click the **Save** button that displays at the bottom of the window) to save the Cisco Unified CallManager Group configuration in the database.

After you have configured the Cisco Unified CallManager Group, you can use it to configure device pools. Devices obtain their Cisco Unified CallManager Group list setting from the device pool to which they are assigned.

Additional Information

See the [“Related Topics” section on page 4-5](#).

Cisco Unified CallManager Group Configuration Settings

[Table 4-1](#) describes the configuration settings for Cisco Unified CallManager groups. For related procedures, see the [“Related Topics” section on page 4-5](#).

Table 4-1 Cisco Unified CallManager Group Configuration Settings

Field	Description
Cisco Unified CallManager Group Settings	
Name	Enter the name of the new group.

Table 4-1 Cisco Unified CallManager Group Configuration Settings (continued)

Field	Description
Auto-registration Cisco Unified CallManager Group	Check the Auto-registration Cisco Unified CallManager Group check box if you want this Cisco Unified CallManager group to be the default Cisco Unified CallManager group when auto-registration is enabled. Leave this check box unchecked if you do not want devices to auto-register with this Cisco Unified CallManager group. Note Each Cisco Unified CallManager cluster can have only one default auto-registration group. If you choose a different Cisco Unified CallManager group as the default auto-registration group, the previously chosen auto-registration group no longer serves as the default for the cluster.
Cisco Unified CallManager Group Members	
Available Cisco Unified CallManagers	This field displays the list of available Cisco Unified CallManager that are not a part of the Cisco Unified CallManager group. Choose the Cisco Unified CallManager names and use the up and down arrows to move Cisco Unified CallManagers between the <i>Selected</i> list and the <i>Available</i> list.
Selected Cisco Unified CallManagers	This field displays the Cisco Unified CallManagers that are in the Cisco Unified CallManager group. The <i>Selected</i> list, which can contain up to three Cisco Unified CallManagers, lists the Cisco Unified CallManagers in order by highest priority. Cisco Unified CallManagers in the <i>Selected</i> list become members of the group when you click Save. Choose the Cisco Unified CallManager names and use the up and down arrows to move Cisco Unified CallManagers between the <i>Selected</i> list and the <i>Available</i> list. Within the <i>Selected</i> list, use the up and down arrows to arrange the groups in the <i>Selected</i> list in the order that you want.

Deleting a Cisco Unified CallManager Group

This section describes how to delete a Cisco Unified CallManager Group from the database.

Before You Begin



Note

You cannot delete a Cisco Unified CallManager group if it is assigned to any device pools or MGCP gateways or if it is the current Auto-registration Cisco Unified CallManager Group for the cluster.

To find out which devices are using the Cisco Unified CallManager group, choose **Dependency Records** from the Related Links drop-down list box on the Cisco Unified CallManager Group Configuration window and click **Go**.

If the dependency records feature is not enabled for the system, the dependency records summary window displays a message that shows the action that you can take to enable the dependency records; the message also displays information about high CPU consumption that is related to the dependency records feature. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#).

If you attempt to delete a Cisco Unified CallManager group that is in use, an error message displays. Before deleting a Cisco Unified CallManager group that is currently in use, you must perform some or all of the following tasks:

- Assign a different Cisco Unified CallManager group to the device pools or MGCP gateways that currently use this Cisco Unified CallManager group. See the [“Configuring a Device Pool” section on page 9-3](#).
- Create or choose a different Cisco Unified CallManager group to be the Auto-registration Cisco Unified CallManager Group.

Procedure

-
Step 1	Find the Cisco Unified CallManager group by using the procedure in the “Finding a Cisco Unified CallManager Group” section on page 4-1 .
Step 2	From the list of matching records, choose the group that you want to delete.
Step 3	Click the Delete Selected Item icon that displays in the tool bar in the upper, left corner of the window (or click the Delete Selected button that displays at the bottom of the window) to delete the Cisco Unified CallManager group.
Step 4	When asked to confirm the delete operation, click either OK to delete or Cancel to cancel the delete operation.
-

Additional Information

See the [“Related Topics” section on page 4-5](#).

Related Topics

- [Cisco Unified CallManager Group Configuration, page 4-1](#)
- [Finding a Cisco Unified CallManager Group, page 4-1](#)
- [Configuring a Cisco Unified CallManager Group, page 4-3](#)
- [Deleting a Cisco Unified CallManager Group, page 4-4](#)



Presence Group Configuration

When you configure Presence in Cisco Unified CallManager Administration, an interested party, known as a watcher, can monitor the real-time status of a directory number or SIP URI, a presence entity, from the device of the watcher.

Cisco Unified CallManager controls which destinations a watcher can monitor with presence groups. A presence group contains watchers and the destinations that can be monitored by the watchers in the group. To allow watchers in one group to monitor directory numbers in other groups, you specify permission settings to allow or block (disallow) the presence request. Presence authorization works with the presence groups that are configured to ensure that a watcher has permission to monitor the status of a destination.

After you configure the presence groups, you apply a presence group to the following items in Cisco Unified CallManager Administration:

- Directory number—Presence entity for which you want status
- SIP trunk—Watcher
- SIP phone—Watcher
- SCCP phone—Watcher
- Application user—Watcher
- End user—Watcher
- Autogenerated device profile (for phones with extension mobility support only)—Watcher

For information about configuring presence groups, refer to the “[Presence](#)” chapter in the *Cisco Unified CallManager Features and Services Guide*.



Date/Time Group Configuration

Use Date/Time Groups to define time zones for the various devices that are connected to Cisco Unified CallManager. Each device exists as a member of only one device pool, and each device pool has only one assigned Date/Time Group.

Installing Cisco Unified CallManager automatically configures a default Date/Time Group that is called CMLocal. CMLocal synchronizes to the active date and time of the operating system on the server where Cisco Unified CallManager is installed. After installing Cisco Unified CallManager, you can change the settings for CMLocal as desired. Normally, adjust server date/time to the local time zone date and time.



Note

CMLocal resets to the operating system date and time whenever you restart Cisco Unified CallManager or upgrade the Cisco Unified CallManager software to a new release. Do not change the name of CMLocal.



Tip

For a worldwide distribution of Cisco Unified IP Phones, create one named Date/Time Group for each of the 24 time zones.

Use the following topics to add, update, or delete Date/Time Groups:

- [Finding a Date/Time Group, page 6-1](#)
- [Configuring a Date/Time Group, page 6-3](#)
- [Date/Time Group Configuration Settings, page 6-4](#)
- [Deleting a Date/Time Group, page 6-5](#)

Finding a Date/Time Group

Because you might have several date/time groups in your network, Cisco Unified CallManager Administration lets you locate specific date/time groups on the basis of specific criteria. Use the following procedure to locate date/time groups.



Note

During your work in a browser session, your find/list search preferences are stored in the cookies on the client machine. If you navigate to other menu items and return to this menu item, or if you close the browser and then reopen a new browser window, your Cisco Unified CallManager search preferences are retained until you modify your search.

Procedure

Step 1 Choose **System > Date/Time Group**.

The Find and List Date/Time Groups window displays. Use the two drop-down list boxes to search for a date/time group.

Step 2 From the first Find Date/Time Groups window drop-down list box, choose one of the following criteria:

- Group Name
- Time Zone

From the second Find Date/Time Groups window drop-down list box, choose one of the following criteria:

- begins with
- contains
- is exactly
- ends with
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**.



Tip To find all Date/Time Groups that are registered in the database, click **Find** without entering any search text.

A list of discovered Date/Time Groups displays by

- Name
- Time Zone

From the Find and List Date/Time Groups window, you can also specify how many items per page to display.



Note You can delete multiple date/time groups from the Find and List Date/Time Groups window by checking the check boxes next to the appropriate date/time groups and clicking **Delete Selected**. You can delete all date/time groups in the window by checking the check box in the Matching records title bar and clicking **Delete Selected**.

Step 4 From the list of records, click the Date/Time Group name that matches your search criteria.

The window displays the date/time group that you chose.

Additional Information

See the [“Related Topics” section on page 6-6](#).

Configuring a Date/Time Group

This section describes how to add, copy, or update a date/time group to the Cisco Unified CallManager database.

Procedure

Step 1 Choose **System > Date/Time Group**.

The Find and List Date/Time Groups window displays.

Step 2 Perform one of the following tasks:

- To copy an existing date/time group, locate the appropriate date/time group as described in the [“Finding a Date/Time Group” section on page 6-1](#), click the **Copy** button next to the date/time group that you want to copy, and continue with [Step 3](#).
- To add a new date/time group, locate the appropriate date/time group as described in the [“Finding a Date/Time Group” section on page 6-1](#), click the **Add New** button, and continue with [Step 3](#).
- To update an existing date/time group, locate the appropriate date/time group as described in the [“Finding a Date/Time Group” section on page 6-1](#) and continue with [Step 3](#).

Step 3 Enter the appropriate settings as described in [Table 6-1](#).

Step 4 To get its date and time, a SIP phone can use NTP server(s) that exist in Cisco Unified CallManager Administration, as described in the [“Phone NTP Reference Configuration” section on page 8-1](#). To add a phone NTP reference to a date/time group for a SIP phone, perform the following tasks:

- a. Click the **Add Phone NTP References** button.
- b. Find the phone NTP reference(s) that you want to add, as described in the [“Finding the Phone NTP References” section on page 8-1](#).

Only phone NTP references that exist in the Cisco Unified CallManager database display. For information on adding a phone NTP reference to Cisco Unified CallManager Administration, see the [“Configuring the Phone NTP References” section on page 8-2](#).

- c. After the search results display, check the check boxes for any phone NTP references that you want to add to the date/time group or click **Select All**.
- d. Click **Add Selected**.



Tip

After you add the phone NTP reference(s) to the date/time group, you can prioritize them, starting with the first server that you want the SIP phone to contact. For example, to move a server to the top of the list, highlight the entry in the pane and click the Up arrow. To move a server to the bottom of the list, highlight the entry in the pane and click the Down arrow.

Step 5 To remove a phone NTP reference from the date/time group, highlight the reference in the pane and click **Remove Phone NTP References**.

Removing the phone NTP reference from the date/time group does not remove the phone NTP reference from the Cisco Unified CallManager database.

- Step 6** To save the new date/time group in the database, click the Save icon that displays in the tool bar in the upper, left corner of the window (or click the Save button that displays at the bottom of the window).
- Step 7** To reset the devices that use the date/time group, click Reset.

Next Steps

After adding a new date/time group to the database, you can assign it to a device pool to configure the date and time information for that device pool. For more information, refer to the [“Configuring a Device Pool”](#) section on page 9-3.

Additional Information

See the [“Related Topics”](#) section on page 6-6.

Date/Time Group Configuration Settings

Table 6-1 describes the date/time group configuration settings. For related procedures, see the [“Related Topics”](#) section on page 6-6.

Table 6-1 *Date/Time Group Configuration Settings*

Field	Description
Group Name	Enter the name that you want to assign to the new date/time group.
Time Zone	From the drop-down list box, choose the time zone for the group that you are adding. The default setting for new Cisco Unified CallManager installations equals (GMT) Monrovia, Casablanca. If you upgrade from a compatible Cisco Unified CallManager release and you use “local time zone of CallManager” in the configuration, the Cisco Unified CallManager database determines the appropriate time zone for the database server and then displays that time zone as replacement for the CallManager time zone.
Separator	Choose the separator character to use between the date fields.
Date Format	Choose the date format for the date that displays on the Cisco Unified IP Phones.

Table 6-1 **Date/Time Group Configuration Settings (continued)**

Field	Description
Time Format	Choose a 12-hour or 24-hour time format.
Selected Phone NTP References (ordered by highest priority)	To ensure that a SIP phone gets its date and time configuration from an NTP server, add the phone NTP reference(s) to the date/time group. To add a phone NTP reference to the date/time group, perform the following tasks: 1. Click the Add Phone NTP References button. 2. Find the phone NTP reference(s) that you want to add, as described in the “Finding the Phone NTP References” section on page 8-1. Only phone NTP references that exist in the Cisco Unified CallManager database display. For information on adding a phone NTP reference to Cisco Unified CallManager Administration, see the “Configuring the Phone NTP References” section on page 8-2. 3. After the search results display, check the check boxes for the phone NTP references or click Select All. 4. Click Add Selected. After you add the phone NTP reference(s) to the date/time group, you can prioritize them, starting with the first reference that you want the phone to contact. For example, to move a reference to the top of the list, highlight the entry in the pane and click the Up arrow. To move a reference to the bottom of the list, highlight the entry in the pane and click the Down arrow. Tip To remove a phone NTP reference from the date/time group, highlight the server in the pane and click Remove Phone NTP References. Removing the phone NTP reference from the date/time group does not remove the phone NTP reference from the Cisco Unified CallManager database.

Deleting a Date/Time Group

This section describes how to delete a date/time group from the Cisco Unified CallManager database.

Before You Begin



Note

You cannot delete a date/time group that any device pool uses.

To find out which device pools use the date/time group, choose **Dependency Records** from the Related Links drop-down list box on the Date/Time Group Configuration window and click **Go**.

If the dependency records feature is not enabled for the system, the dependency records summary window displays a message that shows the action that you can take to enable the dependency records; the message also displays information about high CPU consumption that is related to the dependency records feature. For more information about dependency records, refer to the [“Accessing Dependency Records” section on page A-2](#).

If you attempt to delete a date/time group that is in use, Cisco Unified CallManager displays an error message. Before deleting a date/time group that is currently in use, you must perform either or both of the following tasks:

- Assign a different date/time group to any device pools that use the date/time group that you want to delete. Refer to the [“Configuring a Device Pool” section on page 9-3](#).
- Delete the device pools that use the date/time group that you want to delete. Refer to the [“Deleting a Device Pool” section on page 9-7](#).

Procedure

-
- Step 1** Find the date/time group by using the procedure in the [“Finding a Date/Time Group” section on page 6-1](#).
- Step 2** From the list of matching records, choose the date/time group that you want to delete.
- Step 3** Click the **Delete Selected Item** icon that displays in the tool bar in the upper, left corner of the window (or click the **Delete Selected** button that displays at the bottom of the window) to delete the date/time group.
- Step 4** When prompted to confirm the delete operation, click either **OK** to delete or **Cancel** to cancel the delete operation.
-

Additional Information

See the [“Related Topics” section on page 6-6](#).

Related Topics

- [Date/Time Group Configuration, page 6-1](#)
- [Finding a Date/Time Group, page 6-1](#)
- [Configuring a Date/Time Group, page 6-3](#)
- [Date/Time Group Configuration Settings, page 6-4](#)
- [Deleting a Date/Time Group, page 6-5](#)
- [Finding the Phone NTP References, page 8-1](#)
- [Configuring the Phone NTP References, page 8-2](#)



Region Configuration

Use regions to specify the bandwidth that is used for audio and video calls within a region and between existing regions.

- The audio codec determines the type of compression and the maximum amount of bandwidth that is used per audio call.
- The video call bandwidth comprises the sum of the audio bandwidth and video bandwidth but does not include overhead.



Note

The default audio codec for all calls through Cisco Unified CallManager specifies G.711. If you do not plan to use any other audio codec, you do not need to use regions. See the [“Related Topics” section on page 7-8](#) for more information.



Note

Cisco Unified CallManager allows addition of a maximum of 500 regions.

Use the following procedures to add, update, or delete regions:

- [Finding a Region, page 7-1](#)
- [Configuring a Region, page 7-2](#)
- [Related Topics, page 7-8](#)
- [Deleting a Region, page 7-7](#)

Refer to the [“Regions”](#) section in the *Cisco Unified CallManager System Guide* for more information about configuring regions and selecting audio codecs.

Finding a Region

Because you may have several regions in your network, Cisco Unified CallManager Administration lets you locate specific regions on the basis of specific criteria. Use the following procedure to locate regions.



Note

During your work in a browser session, your find/list search preferences are stored in the cookies on the client machine. If you navigate to other menu items and return to this menu item, or if you close the browser and then reopen a new browser window, your Cisco Unified CallManager search preferences are retained until you modify your search.

Procedure

Step 1 Choose **System > Region**.

The Find and List Regions window displays. Use the drop-down list box to search for a region by Name.

Step 2 From the Find Regions window drop-down list box, choose one of the following criteria:

- begins with
- contains
- is exactly
- ends with
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**.**Tip**

To find all regions that are registered in the database, click **Find** without entering any search text.

A list of discovered regions displays by Name.

From the Find and List Regions window, you can also specify how many items per page to display.

**Note**

You can delete multiple regions from the Find and List Regions window by checking the check boxes next to the appropriate regions and clicking **Delete Selected**. You can delete all regions in the window by checking the check box in the Matching records title bar and clicking **Delete Selected**.

Step 4 From the list of records, click the region name that matches your search criteria.

The window displays the region that you chose.

Additional Information

See the [“Related Topics”](#) section on page 7-8.

Configuring a Region

Use the following procedure to add or update a Region.

Before You Begin

For every region, an association exists with that region in other regions; therefore, the addition of regions occurs in a matrixlike fashion. For example, if you add regions A, B, and C, a matrix with region A, region B, and region C as both columns and rows results, as shown in the following matrix:

	Region A	Region B	Region C
Region A			
Region B			
Region C			

If you assign 20 regions, the database adds 400 entries (20 x 20). Some performance limitations exist when large numbers of regions are assigned.

**Note**

Cisco Unified CallManager allows addition of a maximum of 500 regions.

Configuring Default Values

Region entries contain two values—audio codec and video call bandwidth.

- **Audio Codec**—You define audio codec values to be used within the same region, and you also define audio codec values to be used between regions.
- **Video Call Bandwidth**—You define video call bandwidth values to be used within the same region, and you also define video call bandwidth values to be used between regions.

**Tip**

If you set both the audio codec values and the video call bandwidth values to use the default, the system optimizes its performance by making more efficient use of resources.

**Note**

Regions have default values for use within a region (the recommended default value specifies G.711) and regions have default values for use between regions (the recommended default value specifies G.729).

You configure the default values for regions in the Cisco Unified CallManager Administration Service Parameters Configuration window (**System > Service Parameters**).

1. Choose **System > Service Parameters**.
2. From the drop-down Server list box, choose the Cisco Unified CallManager server that you want to configure.
3. From the drop-down Service list box, choose **Cisco CallManager (Active)** as the service.
4. The Cisco CallManager Service Parameters Configuration window displays.
5. Scroll down to **Clusterwide Parameters (System - Location and Region)** and configure the parameters in this section.
6. Click the **Save** icon that displays in the tool bar in the upper, left corner of the window (or click the **Save** button that displays at the bottom of the window).

Use the following procedure to add or update a region.

Procedure**Step 1** Choose **System > Region**.

The Region Configuration window displays.

Step 2 Perform one of the following tasks:

- To add a new region, click the **Add New** button and continue with [Step 3](#).
- To update an existing region, locate the appropriate region as described in the “[Finding a Region](#)” section on page 7-1 and continue with [Step 3](#).



Note Cisco Unified CallManager recommends that you reset devices after changing a region name.

Step 3 In the Region Name field, enter the name that you want to assign to the region.

Step 4 To save the new region in the database, click the **Save** icon that displays in the tool bar in the upper, left corner of the window (or click the **Save** button that displays at the bottom of the window).

Step 5 To configure the default codecs to use within this region, click the region name to highlight it in the Regions window pane.

- a. From the Audio Codec drop-down list box, choose a default audio codec value to use within this region.

The audio codec determines the type of compression and the maximum amount of bandwidth that is allocated for these calls. See [Table 7-2](#) for a summary of the available codec types and bandwidth usage.

- b. In the Video Call Bandwidth column, click the appropriate radio button to configure the default value to specify the video bandwidth to use for video calls within this region.

If you specify *None*, the system does not allow video calls.



Note For enhanced scalability, Cisco recommends that you properly set the default values in the Cisco Unified CallManager Administration Service Parameters Configuration window for both the audio codec and the video call bandwidth values and then choose the Default settings in the Cisco Unified CallManager Administration Region Configuration window.

Step 6 To configure the default codecs to use between this region and other regions, click another region name (other than this region) to highlight it in the Regions window pane.

- a. From the Audio Codec drop-down list box, choose a default audio codec value to use between this region and the region that you highlighted.

The audio codec determines the type of compression and the maximum amount of bandwidth that is allocated for these calls. See [Table 7-2](#) for a summary of the available codec types and bandwidth usage.

- b. In the Video Call Bandwidth column, click the appropriate radio button to configure the default value to specify the video bandwidth to use for video calls between this region and the region that you highlighted.

If you specify *None*, the system does not allow video calls between this region and the specified region.



Note For enhanced scalability, Cisco recommends that you properly set the default values in the Cisco Unified CallManager Administration Service Parameters Configuration window for both the audio codec and the video call bandwidth values and then choose the Default settings in the Cisco Unified CallManager Administration Region Configuration window.

Step 7 To save the new region in the database, click the **Save** icon that displays in the tool bar in the upper, left corner of the window (or click the **Save** button that displays at the bottom of the window).



Tip The Region Configuration window displays an Items per page drop-down list box that allows you to list 25, 50, 100, 150, 200, or 250 configured regions. If you choose to display 100 or more regions, Cisco Unified CallManager may experience performance degradation.

Next Step
After adding a new region to the database, you can use it to configure device pools. Devices acquire a region setting from the device pool to which they are assigned. See the [“Configuring a Device Pool” section on page 9-3](#) for information on configuring device pools.

Additional Information
See the [“Related Topics” section on page 7-8](#).

Region Configuration Settings

[Table 7-1](#) summarizes the audio codec and video call bandwidth settings that can be specified for regions. For related procedures, see the [“Related Topics” section on page 7-8](#).

Table 7-1 Region Configuration Settings

Field	Description
Region Information	
Name	Enter a unique name for this region. This name can comprise up to 30 characters. Valid characters include letters, numbers, dashes, dots (periods), blanks, and underscores.
	 Note Cisco Unified CallManager recommends that you reset devices after changing a region name.
Region Relationships	
Modify Relationship to Other Regions	
Regions	The entries in this column specify all existing regions, including the Default region, the region that you are configuring, and all other regions.

Table 7-1 *Region Configuration Settings (continued)*

Field	Description
Audio Codec	For each region that is specified in the Regions window pane, choose the corresponding value from the drop-down list box in this column to set the audio codec to use for calls within this region and between this region and the specified region. To choose the default setting, click the Defaults radio button. • Cisco recommends that you choose the Default settings that you configured in the Cisco Unified CallManager Administration Service Parameters Configuration window. See the “Configuring Default Values” section on page 7-3. • Because of bandwidth constraints at most remote-site deployments, use G.729 as the recommended default codec setting between a new region and existing regions.
Video Call Bandwidth	For each region that is specified in the Regions window pane, click one radio button in this column as specified: • Use System Default—Click this button to use the default value. The default value normally specifies 384 kbps, unless the default value has been set to a different value in the Service Parameters Configuration window. • None—Click this radio button if no video call bandwidth is allotted between this region and the specified region. • kbps—Click this button to allot video call bandwidth between this region and the specified region. Enter the bandwidth that is available for each video call between these two regions. Valid values range from 1 to 8128.

The total bandwidth that is used per call stream depends on the audio codec type as well as factors such as data packet size and overhead (packet header size). The bandwidth figures shown in [Table 7-2](#) apply for 30-ms data packets and include IP headers. Each call comprises two call streams.

**Note**

The codecs specified in [Table 7-2](#) correlate to an approximate bandwidth usage per call. For information on bandwidth usage for each codec, refer to *Cisco Unified Communications Solution Reference Network Design (SRND)* for the current release of Cisco Unified CallManager.

Table 7-2 *Bandwidth That Audio Codecs Use*

Audio Codec	Bandwidth Used Per Call (Including IP Headers) With 30-ms Data Packets	Description
G.711	80 kbps	This codec represents the default codec for all Cisco Unified CallManager calls.
G.722	80 kbps	Video endpoints typically prefer this codec.
G.723	24 kbps	The system supports this low-bit-rate codec for use with older Cisco IP Phone model 12 SP Series and Cisco IP Phone model 30 VIP.

Table 7-2 *Bandwidth That Audio Codecs Use (continued)*

Audio Codec	Bandwidth Used Per Call (Including IP Headers) With 30-ms Data Packets	Description
G.728	16 kbps	Video endpoints support this low-bit-rate codec.
G.729	24 kbps	The system supports this low bit-rate codec for Cisco Unified IP Phone 7900 models.
Wideband	272 kbps	The system supports this high-quality, high-bandwidth audio codec for IP-phone to IP-phone calls that the Cisco Unified IP Phone 7900 models support.
GSM	29 kbps	The Global System for Mobile Communications (GSM) codec enables the MNET system for GSM wireless handsets to interoperate with Cisco Unified CallManager.

Deleting a Region

This section describes how to delete a region from the Cisco Unified CallManager database.

Before You Begin

**Note**

You cannot delete a region that any device pools are using.

To find out which device pools use the region, choose **Dependency Records** from the Related Links drop-down list box on the Region Configuration window and click **Go**.

If the dependency records feature is not enabled for the system, the dependency records summary window displays a message that shows the action that you can take to enable the dependency records; the message also displays information about high CPU consumption that is related to the dependency records feature. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#).

If you attempt to delete a region that is in use, Cisco Unified CallManager displays an error message. Before deleting a region that is currently in use, you must perform either or both of the following tasks:

- Update the device pools to use a different region. See the [“Configuring a Device Pool” section on page 9-3](#).
- Delete the device pools that use the region that you want to delete. See the [“Deleting a Device Pool” section on page 9-7](#).

Procedure

-
- Step 1** Find the region by using the procedure in the [“Finding a Region” section on page 7-1](#).
- Step 2** From the list of matching records, choose the region that you want to delete.
- Step 3** Click the **Delete Selected Item** icon that displays in the tool bar in the upper, left corner of the window (or click the **Delete Selected** button that displays at the bottom of the window) to delete the region.
-

**Tip**

The Region Configuration window displays an Items per page drop-down list box that allows you to list 25, 50, 100, 150, 200, or 250 configured regions. If you choose to display 100 or more regions, Cisco Unified CallManager may experience performance degradation.

Additional Information

See the [“Related Topics” section on page 7-8](#).

Related Topics

- [Region Configuration, page 7-1](#)
- [Finding a Region, page 7-1](#)
- [Configuring a Region, page 7-2](#)
- [Region Configuration Settings, page 7-5](#)
- [Deleting a Region, page 7-7](#)



Phone NTP Reference Configuration

If you want to do so, you can configure phone Network Time Protocol (NTP) references in Cisco Unified CallManager Administration to ensure that a Cisco SIP IP Phone gets its date and time from the NTP server. If all NTP servers do not respond, the SIP phone uses the date header in the 200 OK response to the REGISTER message for the date and time.

After you add the phone NTP reference to Cisco Unified CallManager Administration, you must add it to a date/time group. In the date/time group, you prioritize the phone NTP references, starting with the first server that you want the phone to contact.

The date/time group configuration gets specified in the device pool, and the device pool gets specified on the phone page.

Use the following topics to configure phone NTP references:

- [Finding the Phone NTP References, page 8-1](#)
- [Configuring the Phone NTP References, page 8-2](#)
- [Phone NTP Reference Configuration Settings, page 8-3](#)
- [Deleting the Phone NTP Reference, page 8-4](#)

Finding the Phone NTP References

Because you can configure several phone NTP references in Cisco Unified CallManager Administration, Cisco Unified CallManager Administration allows you to locate specific phone NTP references. Use the following procedure to locate the phone NTP references that exist in Cisco Unified CallManager Administration.



Note

During your work in a browser session, the cookies on the client machine store your find/list preferences. If you navigate to other menu items and return to this menu item, or if you close the browser and then reopen a new browser window, the system retains your Cisco Unified CallManager search preferences until you modify your search.

Procedure

Step 1 Choose **System > Phone NTP Reference**.

The Find and List window displays.

**Tip**

To find all phone NTP references that exist in the database, click **Find** without specifying any search criteria.

Step 2 If you want to do so, choose search criteria from the Find drop-down list boxes; enter the appropriate search text, if applicable, and click **Find**.

From the Find and List window, you can also specify how many items per page to display.

Step 3 From the list of records, click the phone NTP reference name that matches your search criteria.

Additional Information

See the [“Related Topics” section on page 8-4](#).

Configuring the Phone NTP References

This section describes how to add a phone NTP reference to the Cisco Unified CallManager database or to update a phone NTP reference that exists in the database.

Procedure

Step 1 Choose **System > Phone NTP Reference**.

The Find and List window displays.

Step 2 Perform one of the following tasks:

- To add the phone NTP reference to the Cisco Unified CallManager database, click the **Add New** button and continue with [Step 3](#).
- To update an existing phone NTP reference, locate the existing phone NTP reference as described in the [“Finding the Phone NTP References” section on page 8-1](#) and continue with [Step 3](#).

Step 3 Enter the appropriate settings as described in [Table 8-1](#).

Step 4 To save the configuration in the database, click the **Save** icon that displays in the tool bar in the upper, left corner of the window (or click the **Save** button that displays at the bottom of the window).

Next Steps

After you add a new phone NTP reference to the Cisco Unified CallManager database, assign it to a date/time group. For more information, refer to the [“Configuring a Date/Time Group” section on page 6-3](#).

Additional Information

See the [“Related Topics” section on page 8-4](#).

Phone NTP Reference Configuration Settings

Table 8-1 describes the phone NTP reference configuration settings. For related procedures, see the “Related Topics” section on page 8-4.

Table 8-1 Phone NTP Reference Configuration Settings

Field	Description
IP Address	Enter the IP address of the NTP server that you want the SIP phone to use to get its date and time.  Note Cisco Unified CallManager cannot be configured as Phone NTP References.
Description	Enter a description for the phone NTP reference. Cisco Unified CallManager Administration automatically propagates the information in the IP Address field to the Description field. If you want to do so, you can change the information.
Mode	From the drop-down list box, choose the mode for the phone NTP reference. The values from which you can choose follow: - Directed Broadcast—If you choose this default NTP mode, the phone accesses date/time information from any NTP server but gives the listed NTP servers (1st = primary, 2nd = secondary) priority. For example, if the phone configuration contains NTP servers where A = primary NTP server and B = secondary/backup NTP server, the phone uses the broadcast packets (derives the date/time) from NTP server A. If NTP server A is not broadcasting, the phone accesses date/time information from NTP server B. If neither NTP server is broadcasting, the phone accesses date/time information from any other NTP server. If no other NTP server is broadcasting, the phone will derive the date/time from the Cisco Unified CallManager 200 OK response to the REGISTER message. - Unicast—If you choose this mode, the phone will send an NTP query packet to that particular NTP server. If the phone gets no response, the phone will access date/time information from any other NTP server. If no other NTP servers respond, the phone will derive the date/time from the Cisco Unified CallManager 200 OK response to the REGISTER message.  Note Cisco Unified CallManager currently does not support the Multicast and Anycast modes. If you choose either of these modes, Cisco Unified CallManager will default to the Directed Broadcast mode.

Deleting the Phone NTP Reference

This section describes how to delete a phone NTP reference from the Cisco Unified CallManager database.

Before You Begin

Before you can delete the phone NTP reference from Cisco Unified CallManager Administration, you must delete the phone NTP reference from the date/time group. To find which date/time groups use the phone NTP reference, choose **Dependency Records** from the Related Links drop-down list box in the Phone NTP Reference Configuration window and click **Go**. When you know which date/time groups use the phone NTP reference, you can then remove that phone NTP reference from that group.

If the dependency records feature is not enabled for the system, the dependency records summary window displays a message that shows the action that you can take to enable the dependency records; the message also displays information about high CPU consumption that is related to the dependency records feature. For more information about dependency records, refer to the [“Accessing Dependency Records” section on page A-2](#).

Procedure

-
- Step 1** By using the procedure in the [“Finding the Phone NTP References” section on page 8-1](#), find the phone NTP reference.
- Step 2** To delete multiple phone NTP references, check the check boxes next to the appropriate phone NTP references in the Find and List window; then, click the **Delete Selected** icon or the **Delete Selected** button.
- Step 3** To delete a single phone NTP reference, perform one of the following tasks:
- In the Find and List window, check the check box next to the appropriate phone NTP reference; then, click the **Delete Selected** icon or the **Delete Selected** button.
 - In the Find and List window, click the Name link for the phone NTP reference. After the Phone NTP Reference Configuration window for that specific phone NTP reference displays, click the **Delete Selected** icon or the **Delete Selected** button.
- Step 4** When prompted to confirm the delete operation, click **OK** to delete or **Cancel** to cancel the delete operation.
-

Additional Information

See the [“Related Topics” section on page 8-4](#).

Related Topics

- [Phone NTP Reference Configuration, page 8-1](#)
- [Finding the Phone NTP References, page 8-1](#)
- [Configuring the Phone NTP References, page 8-2](#)

- [Phone NTP Reference Configuration Settings, page 8-3](#)
- [Deleting the Phone NTP Reference, page 8-4](#)
- [Finding a Date/Time Group, page 6-1](#)
- [Configuring a Date/Time Group, page 6-3](#)
- [Date/Time Group Configuration Settings, page 6-4](#)
- [Deleting a Date/Time Group, page 6-5](#)



Device Pool Configuration

Use device pools to define sets of common characteristics for devices. You can specify the following device characteristics for a device pool:

- Cisco Unified CallManager group
- Date/time group
- Region
- Softkey template
- SRST reference
- Calling search space for auto-registration
- Media resource group list
- Music On Hold (MOH) audio sources
- User and network locales
- Connection monitor duration timer for communication between SRST and Cisco Unified CallManager
- MLPP settings

Use the following topics to add, update, or delete a device pool:

- [Finding a Device Pool, page 9-1](#)
- [Configuring a Device Pool, page 9-3](#)
- [Device Pool Configuration Settings, page 9-4](#)
- [Deleting a Device Pool, page 9-7](#)
- [Related Topics, page 9-8](#)

Refer to the “[System-Level Configuration Settings](#)” section in the *Cisco Unified CallManager System Guide* for more information about device pools and the device settings that are assigned through device pools.

Finding a Device Pool

Because you might have several device pools in your network, Cisco Unified CallManager Administration lets you locate specific device pools on the basis of specific criteria. Use the following procedure to locate device pools.

**Note**

During your work in a browser session, Cisco Unified CallManager Administration retains your device pool search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your device pool search preferences until you modify your search or close the browser.

Procedure**Step 1** Choose **System > Device Pool**.

The Find and List Device Pools window displays. Use the two drop-down list boxes to search for a device pool.

Step 2 From the first Find Device Pools where drop-down list box, choose one of the following criteria:

- Device Pool Name
- Cisco Unified CallManager Group
- Region

**Note**

The criterion that you choose in this drop-down list box specifies how the list of device pools that your search generates will be sorted. For example, if you choose Region, the Region column will display as the left column of the results list.

From the second Find Device Pools where drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is not empty
- is empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.**Tip**

To find all device pools that are registered in the database, click **Find** without entering any search text.

A list of discovered device pools displays by

- Device Pool icon
- Device Pool Name
- CallManager Group
- Region
- Date/Time Group

**Note**

You can delete multiple device pools from the Find and List Device Pools window by checking the check boxes next to the appropriate device pools and clicking **Delete Selected**. You can delete all device pools in the window by checking the check box in the Matching records title bar and clicking **Delete Selected**.

- Step 4** From the list of records, click the Device Pool icon or name, the CallManager Group, the Region, or the Date/Time Group that matches your search criteria.

The window displays the device pool that you choose.

Additional Information

See the [“Related Topics” section on page 9-8](#).

Configuring a Device Pool

This section describes how to add, copy, or update a device pool to the Cisco Unified CallManager database. After adding a new device pool to the database, you can use it to configure devices such as Cisco Unified IP Phones, gateways, conference bridges, transcoders, media termination points, voice-mail ports, CTI route points, and so on.

Before You Begin

Before configuring a device pool, you must configure the following items if you want to choose them for the device pool:

- Cisco Unified CallManager group (required). Refer to the [“Configuring a Cisco Unified CallManager Group” section on page 4-3](#).
- Date/time group (required). Refer to the [“Configuring a Date/Time Group” section on page 6-3](#).
- Region (required). Refer to the [“Configuring a Region” section on page 7-2](#).
- SRST reference (optional). Refer to the [“Configuring an SRST Reference” section on page 16-2](#).
- Media resource group list (optional). Refer to the [“Configuring a Media Resource Group List” section on page 61-2](#).
- MOH audio sources (optional). Refer to the [“Finding a Music On Hold Audio Source” section in the *Cisco Unified CallManager Features and Services Guide*](#).
- Calling search space for auto-registration (optional). Refer to the [“Configuring a Calling Search Space” section on page 43-2](#).
- Softkey templates if you are not using the standard softkey templates that are provided with Cisco Unified CallManager (optional). Refer to the [“Adding Nonstandard Softkey Templates” section on page 77-2](#).

Procedure

- Step 1** Choose **System > Device Pool**.

The Find and List Device Pools window displays.

- Step 2** Perform one of the following tasks:
- To copy an existing device pool, locate the appropriate device pool as described in the [“Finding a Device Pool” section on page 9-1](#), click the Copy button next to the device pool that you want to copy, and continue with [Step 3](#).
 - To add a new device pool, click the **Add New** button and continue with [Step 3](#).
 - To update an existing device pool, locate the appropriate device pool as described in the [“Finding a Device Pool” section on page 9-1](#) and continue with [Step 3](#).
- Step 3** Enter the appropriate fields as described in [Table 9-1](#).
- Step 4** Click **Save** to save the device pool information to the database.

Additional Information

See the [“Related Topics” section on page 9-8](#).

Device Pool Configuration Settings

[Table 9-1](#) lists and describes device pool configuration settings. For related procedures, see the [“Related Topics” section on page 9-8](#).

Table 9-1 *Device Pool Configuration Settings*

Field Name	Description
Device Pool Settings	
Device Pool Name	Enter the name of the new device pool that you are creating.
Cisco Unified CallManager Group	Choose the Cisco Unified CallManager group to assign to devices in this device pool. A Cisco Unified CallManager group specifies a prioritized list of up to three Cisco Unified CallManagers. The first Cisco Unified CallManager in the list serves as the primary Cisco Unified CallManager for that group, and the other members of the group serve as backup Cisco Unified CallManagers for redundancy.
Date/Time Group	Choose the date/time group to assign to devices in this device pool. The date/time group specifies the time zone and the display formats for date and time.
Region	Choose the Cisco Unified CallManager region to assign to devices in this device pool. The Cisco Unified CallManager region settings specify voice codec that can be used for calls within a region and between other regions.
Softkey Template	From the drop-down list box, choose the softkey template that is associated with the devices in the device pool.

Table 9-1 **Device Pool Configuration Settings (continued)**

Field Name	Description
SRST Reference	From the drop-down list box, choose a survivable remote site telephony (SRST) reference to assign to devices in this device pool. Choose from the following options: • Disable—If you choose this option, devices in this device pool will not have SRST reference gateways available to them. • Use Default Gateway—If you choose this option, devices in this device pool use the default gateway for SRST. • Existing SRST references—If you choose an SRST reference from the drop-down list, devices in this device pool will use this SRST reference gateway.
Calling Search Space for Auto-registration	Choose the calling search space to assign to devices in this device pool that auto-registers with Cisco Unified CallManager. The calling search space specifies partitions that devices can search when attempting to complete a call.
Media Resource Group List	From the drop-down list box, choose a media resource group list. A media resource group list specifies a prioritized list of media resource groups. An application selects the required media resource (for example, a music on hold server, transcoder, or conference bridge) from the available media resource groups according to the priority order that is defined in a media resource group list.
Network Hold MOH Audio Source	Choose the audio source to use for music on hold (MOH) when the network initiates a hold action.
User Hold MOH Audio Source	Choose the audio source to use for music on hold (MOH) when a user initiates a hold action.
Network Locale	From the drop-down list box, choose the locale that is associated with phones and gateways. The network locale contains a definition of the tones and cadences that the phones and gateways in the device pool in a specific geographic area use. Make sure that you select a network locale supported by all of the phones and gateways that use this device pool. Note If the user does not choose a network locale, the locale that is specified in the Cisco Unified CallManager clusterwide parameters as Default Network Locale applies. Note Choose only a network locale that is already installed and supported by the associated devices. The list contains all available network locales for this setting, but not all are necessarily installed. If a device is associated with a network locale that it does not support in the firmware, the device will fail to come up.

Table 9-1 **Device Pool Configuration Settings (continued)**

Field Name	Description
User Locale	From the drop-down list box, choose the locale that is associated with the phones and gateways in the device pool. The user locale identifies a set of detailed information to support users, including language and font. Note If the user does not choose a user locale, the locale that is specified in the Cisco Unified CallManager clusterwide parameters as Default User Locale applies.
Connection Monitor Duration	This setting defines the amount of time that the IP phone monitors its connection to Cisco Unified CallManager before it unregisters from SRST and re-registers to Cisco Unified CallManager. The default value, which specifies 120 seconds, resides in the Connection Monitor Duration enterprise parameter. Change this setting if you need to disable the connection monitor (by changing the value to zero) or if you want to extend the connection monitor time. Note When you change the value of the connection monitor duration, it applies only to the device pool that is being updated. All other device pools use the value in their own connection monitor duration fields or use the value that is configured in the enterprise parameter. For more information, refer to Survivable Remote Site Telephony References in the <i>Cisco Unified CallManager System Guide</i>.
Multilevel Precedence and Preemption (MLPP) Information	
MLPP Indication	This setting specifies whether devices in the device pool that are capable of playing precedence tones will use the capability when the devices place an MLPP precedence call. From the drop-down list box, choose a setting to assign to the devices in this device pool from the following options: • Default—This device pool inherits its MLPP Indication setting from the MLPP Indication Status enterprise parameter. • Off—Devices in this device pool do not handle nor process indication of an MLPP precedence call. • On—Devices in this device pool do handle and process indication of an MLPP precedence call. Note Do not configure a device pool with the following combination of settings: MLPP Indication is set to <i>Off</i> or <i>Default</i> (when default is <i>Off</i>) while MLPP Preemption is set to <i>Forceful</i>. Note Turning on MLPP Indication (at the enterprise parameter, device pool, or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device.

Table 9-1 **Device Pool Configuration Settings (continued)**

Field Name	Description
MLPP Preemption	This setting specifies whether devices in the device pool that are capable of preempting calls in progress will use the capability when the devices place an MLPP precedence call. From the drop-down list box, choose a setting to assign to the devices in this device pool from the following options: • Default—This device pool inherits its MLPP Preemption setting from the MLPP Preemption Setting enterprise parameter. • Disabled—Devices in this device pool do not allow preemption of lower-precedence calls to take place when necessary for completion of higher-precedence calls. • Forceful—Devices in this device pool allow preemption of lower-precedence calls to take place when necessary for completion of higher-precedence calls. Note Do not configure a device pool with the following combination of settings: MLPP Indication is set to <i>Off</i> or <i>Default</i> (when default is <i>Off</i>) while MLPP Preemption is set to <i>Forceful</i>.
MLPP Domain	Enter a hexadecimal value between 0 and FFFFFFFF for the MLPP domain that is associated with this device pool. If you leave this field blank, this device pool inherits its MLPP domain from the value set for the MLPP Domain Identifier enterprise parameter.

Deleting a Device Pool

This section describes how to delete a device pool from the Cisco Unified CallManager database.

Before You Begin

You cannot delete a device pool if it has any devices assigned to it, if it is used for Device Defaults configuration, or if it is the only device pool in the database. If you try to delete a device pool that is in use, an error message displays. Before deleting a device pool that is currently in use, you must perform either or both of the following tasks:

- Update the devices to assign them to a different device pool. Refer to the [“Deleting a Phone” section on page 70-5](#).
- Delete the devices that are assigned to the device pool that you want to delete. Refer to the [“Deleting a Phone” section on page 70-5](#).

Procedure

-
- Step 1** Find the device pool by using the procedure in the [“Finding a Device Pool” section on page 9-1](#).
- Step 2** From the list of matching records, choose the device pool that you want to delete.

Step 3 Click **Delete Selected**.

Step 4 When prompted to confirm the delete operation, click **OK** to delete or click **Cancel** to cancel the delete operation.

Additional Information

See the [“Related Topics”](#) section on page 9-8.

Related Topics

- [Device Pool Configuration, page 9-1](#)
- [Finding a Device Pool, page 9-1](#)
- [Configuring a Device Pool, page 9-3](#)
- [Deleting a Device Pool, page 9-7](#)



DHCP Server Configuration

Dynamic Host Configuration Protocol (DHCP) server enables Cisco Unified IP Phones, connected to either the customer's data or voice Ethernet network, to dynamically obtain their IP addresses and configuration information. DHCP uses Domain Name System (DNS) to resolve host names both within and outside the cluster.

This chapter contains the following topics:

- [Activating DHCP Monitor Service, page 10-1](#)
- [Starting DHCP Monitor Service, page 10-2](#)
- [Finding a DHCP Server, page 10-2](#)
- [Configuring a DHCP Server, page 10-4](#)
- [DHCP Server Configuration Settings, page 10-4](#)
- [Deleting a DHCP Server, page 10-5](#)

Activating DHCP Monitor Service

You can activate and deactivate DHCP monitor process by using the Serviceability window of Cisco Unified CallManager. Use the following procedure to activate the service.

Procedure

Step 1 From Cisco Unified CallManager Serviceability, choose **Tools > Service Activation**.

The Service Activation window displays.

Step 2 Select Cisco DHCP Monitor Service from the CM Services list and click **Save**.



Note If the service is already activated, the Activation Status will display as Activated.

Step 3 The service gets activated, and the Activation Status column displays the status as Activated.



Note The DHCP monitor service starts automatically after it is activated. See the [“Starting DHCP Monitor Service” section on page 10-2](#) to stop, start, or restart the service.

Additional Information

See the [“Related Topics”](#) section on page 10-6.

Starting DHCP Monitor Service

The DHCP Monitor Service starts automatically after it is activated by using Cisco Unified CallManager Serviceability. This section describes the procedures to stop or restart the DHCP service.

Procedure

-
- Step 1** In Cisco Unified CallManager Serviceability, choose **Tools > Control Center - Feature Services**.
The Control Center–Feature Services window displays.
- Step 2** Choose the Cisco Unified CallManager server from the Servers drop-down list box.
Cisco DHCP Monitor Service displays in the list under Service Name column, in CM Services.



Note If the Cisco DHCP Monitor Service was activated by using [“Activating DHCP Monitor Service”](#) section on page 10-1, the Status displays as Activated.

- Step 3** Check the check box corresponding to Cisco DHCP Monitor Service.
- Step 4** If you want to restart the Cisco DHCP Monitor Service, click **Restart**.
The service restarts, and the message, Service Successfully Restarted, displays.
- Step 5** If you want to stop the Cisco DHCP Monitor Service, click **Stop**.
The service stops, and the message, Service Successfully Stopped, displays.
- Step 6** If you want to start a stopped Cisco DHCP Monitor Service, click **Start**.
The service starts, and the message, Service Successfully Started, displays.
-

Additional Information

See the [“Related Topics”](#) section on page 10-6.

Finding a DHCP Server

Because you might have several servers in your network, Cisco Unified CallManager lets you locate specific DHCP servers on the basis of specific criteria. Use the following procedure to locate servers.



Note During your work in a browser session, the cookies on the client machine store your find/list search preferences. If you navigate to other menu items and return to this menu item, or if you close the browser and then reopen a new browser window, the system retains your Cisco Unified CallManager search preferences until you modify your search.

Procedure

Step 1 Choose **System > DHCP > DHCP Server**.

The Find and List DHCP Servers window displays. Use the two drop-down list boxes to search for a server.

Step 2 From the first Find DHCP Servers where window drop-down list box, choose one of the following criteria:

- Host Server
- Primary DNS
- Secondary DNS
- Domain Name

From the second Find Servers where drop-down list box, choose one of the following criteria:

- begins with
- contains
- is exactly
- ends with
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**.**Tip**

To find all DHCP servers that are registered in the database, click **Find** without entering any search text.

A list of discovered servers displays by

- Host Server
- Primary DNS
- Secondary DNS
- Domain Name

Step 4 From the list of records, click the DHCP Server name that matches your search criteria.

The window displays the server that you choose.

Additional Information

See the [“Related Topics”](#) section on page 10-6.

Configuring a DHCP Server

This section describes how to add, copy, and update a DHCP server address to the Cisco Unified CallManager database.

Procedure

- Step 1**
- Choose **System > DHCP > DHCP Server**
- Step 2**
- Perform one of the following tasks:
 - To add a DHCP server, click **Add New**.
 - To update a server, find the server by using the procedure in the [“Finding a DHCP Server” section on page 10-2](#).
 - To copy a server, find the server by using the procedure in the [“Finding a DHCP Server” section on page 10-2](#), select the DHCP server that you want by checking the check box next to the server name, and click the **Copy** icon.

The DHCP Server Configuration window displays.
- Step 3**
- Enter the appropriate settings as described in [Table 10-1](#).
- Step 4**
- Click the **Save** icon that displays in the tool bar in the upper, left corner of the window (or click the **Save** button that displays at the bottom of the window) to save the data and to add the server to the database.

Additional Information

See the [“Related Topics” section on page 10-6](#).

DHCP Server Configuration Settings

[Table 10-1](#) describes the server configuration settings. For related procedures, see the [“Related Topics” section on page 10-6](#).

Table 10-1 DHCP Server Configuration Settings

Server Information Field	Description
Host Name	Choose the host name of the Cisco Unified CallManager server that uses DNS services. Note You must update the DNS server with the appropriate Cisco Unified CallManager name and address information before using that information here.
Primary DNS IP Address	This field specifies primary DNS IP address.
Secondary DNS IP Server	This field specifies secondary DNS IP address name.
Primary TFTP Server IP Address (Option 150)	You can enable the IP phones to access the TFTP server using DHCP custom option 150. This is the method that Cisco recommends. This field specifies the IP address for primary Trivial File Transfer Protocol (TFTP) server.

Table 10-1 **DHCP Server Configuration Settings (continued)**

Server Information Field	Description
Secondary TFTP Server IP Address (Option 150)	This field specifies the IP address for secondary TFTP server.
Bootstrap Server IP Address	This field specifies the address of the server that is used in the next step of the bootstrap process. You can use as the IP address of the TFTP server or as the default value to DHCP server address if the server supplies the next bootstrap service.
Domain Name	The Domain Name specifies the domain name that you should use when resolving hostname via the Domain Name System.
TFTP Server Name (Option 66)	You can enable the IP phones to access the TFTP server using DHCP option 66. Use this field to identify a TFTP server. You can configure only one DNS name or a dotted decimal IP address in this parameter.
ARP Cache Timeout	This field specifies the timeout in seconds for ARP cache entries. Specify the time as a 32-bit unsigned integer.
IP Address Lease Time	The DHCP server uses the information in this field to specify the lease time that it is willing to offer. Specify the time in units of seconds and as a 32-bit unsigned integer.
Renewal Time	This field specifies the time interval from address assignment until the client transitions to the RENEWING state.
Rebinding Time (T1)	This field specifies the time interval from address assignment until the client transitions to the REBINDING state. Specify the value in units of seconds and as a 32-bit unsigned integer.

Deleting a DHCP Server

This section describes how to delete a DHCP server from the Cisco Unified CallManager database.

Procedure

- Step 1** Find the DHCP server by using the procedure in the [“Finding a DHCP Server”](#) section on page 10-2.
- Step 2** From list of matching records, choose the DHCP server that you want to delete.
- Step 3** Click the **Delete Selected Item** icon that displays in the tool bar in the upper, left corner of the window (or click the **Delete Selected** button that displays at the bottom of the window) to delete the server.
If the server is not in use, Cisco Unified CallManager deletes it. If it is in use, an error message displays.



Note You can delete multiple host servers from the Find and List Servers window by checking the check boxes next to the appropriate servers and clicking **Delete Selected**. You can delete all servers in the window by clicking **Select All** and then clicking **Delete Selected**.

Additional Information

See the [“Related Topics”](#) section on page 10-6.

Related Topics

- [Activating DHCP Monitor Service, page 10-1](#)
- [Starting DHCP Monitor Service, page 10-2](#)
- [Finding a DHCP Server, page 10-2](#)
- [Configuring a DHCP Server, page 10-4](#)
- [Deleting a DHCP Server, page 10-5](#)
- [DHCP Server Configuration Settings, page 10-4](#)
- [DHCP Subnet Configuration](#)

Additional Information

- [Dynamic Host Configuration Protocol](#), *Cisco Unified CallManager System Guide*



DHCP Subnet Configuration

This chapter describes the procedures for adding subnets to DHCP servers.

Use the following procedures to find and add subnets to DHCP servers.

- [Finding a DHCP Subnet, page 11-1](#)
- [Configuring a DHCP Subnet, page 11-2](#)
- [Deleting a DHCP Subnet, page 11-4](#)
- [DHCP Subnet Configuration Settings, page 11-3](#)

Finding a DHCP Subnet

Use the following procedure to locate DHCP subnets.



Note

During your work in a browser session, the cookies on the client machine store your find/list search preferences. If you navigate to other menu items and return to this menu item, or if you close the browser and then reopen a new browser window, the system retains your Cisco Unified CallManager search preferences retained until you modify your search.

Procedure

Step 1 Choose **System > DHCP > DHCP Subnet**.

The Find and List DHCP Subnets window displays. Use the two drop-down list boxes to search for a server.

Step 2 From the first Find DHCP Subnets where window drop-down list box, choose one of the following criteria:

- DHCP Server
- Subnet IP Address
- Primary Start IP Address
- Primary End IP Address
- Secondary Start IP Address
- Secondary End IP Address

From the second Find DHCP Subnet where drop-down list box, choose one of the following criteria:

- begins with
- contains
- is exactly
- ends with
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**.



Tip

To find all DHCP subnets that are registered in the database, click **Find** without entering any search text.

A list of discovered subnets displays by

- DHCP Server
- Subnet IP Address
- Primary Start IP Address
- Primary End IP Address
- Secondary Start IP Address
- Secondary End IP Address

Step 4 From the list of records, click the DHCP subnet name that matches your search criteria. The window displays the subnet that you choose.

Additional Information

See the [“Related Topics” section on page 11-5](#).

Configuring a DHCP Subnet

This section describes how to add, update, or copy a DHCP subnet address to the Cisco Unified CallManager database.

Procedure

Step 1 Choose **System > DHCP > DHCP Subnet**

Step 2 Perform one of the following tasks:

- To add a DHCP subnet, click **Add New**.
- To update a subnet, find the subnet by using the procedure in the [“Finding a DHCP Subnet” section on page 11-1](#).

- To copy a subnet, find the subnet by using the procedure in the [“Finding a DHCP Subnet” section on page 11-1](#); select the DHCP server that you want by checking the check box next to the server name and click **Copy**.

The DHCP Subnet Configuration window displays.

Step 3 Enter the appropriate settings as described in [Table 11-1](#).

Step 4 Click the **Save** icon that displays in the tool bar in the upper, left corner of the window (or click the **Save** button that displays at the bottom of the window) to save the data and to add the subnet to the database.

Changes to the server configuration do not take effect until you restart Cisco Unified CallManager. For information about restarting the Cisco CallManager service, refer to the *Cisco Unified CallManager Serviceability Administration Guide*.

Additional Information

See the [“Related Topics” section on page 11-5](#).

DHCP Subnet Configuration Settings

[Table 11-1](#) describes the server configuration settings. For related procedures, see the [“Related Topics” section on page 11-5](#).

Table 11-1 DHCP Subnet Configuration Settings

Server Information Field	Description
DHCP Server	Choose the DHCP server name from the drop-down list box.
Subnet IP Address	Enter the Subnet IP address.
Primary Start IP Address	Enter the start IP address of the first range of IP addresses to be assigned.
Primary End IP Address	Enter the end IP address of the first range of IP addresses to be assigned.
Secondary Start IP Address	Enter the start IP address of the second range of IP addresses to be assigned.
Secondary End IP Address	Enter the end IP address of the second range of IP addresses to be assigned.
Primary Router IP Address	Enter the IP address of the primary router on your subnet.
Secondary Router IP Address	Enter the IP address of the secondary router on your subnet.
Subnet Mask	Enter the subnet mask.
Domain Name	This field specifies the name that you should use when resolving hostname via the Domain Name System.
Primary DNS IP Address	This field specifies primary DNS IP server name.
Secondary DNS IP Address	This field specifies secondary DNS IP server name.
TFTP Server Name (Option 66)	Use this field to identify a TFTP server. You can configure only one DNS name or a dotted decimal IP address in this parameter.

Table 11-1 DHCP Subnet Configuration Settings (continued)

Server Information Field	Description
Primary TFTP Server IP Address (Option 150)	This field specifies the IP addresses for primary Trivial File Transfer Protocol (TFTP) server.
Secondary TFTP Server IP Address (Option 150)	This field specifies the IP addresses for secondary TFTP server.
Bootstrap Server IP Address	This field specifies the address of the server that is used in the next step of the bootstrap process. You can use this as the IP address of the TFTP server or as the default value to DHCP server address if the server is to supply the next bootstrap service.
ARP Cache Timeout (sec)	This field specifies the timeout in seconds for ARP cache entries. Specify the time as a 32-bit unsigned integer.
IP Address Lease Time (sec)	The DHCP server uses the information in this field to specify the lease time that it is willing to offer. Specify the time in units of seconds and as a 32-bit unsigned integer.
Renewal (T1) Time (sec)	This field specifies the time interval from address assignment until the client transitions to the RENEWING state.
Rebinding (T2)Time (sec)	This field specifies the time interval from address assignment until the client transitions to the REBINDING state. Specify the value in units of seconds and as a 32-bit unsigned integer.

Deleting a DHCP Subnet

This section describes how to delete a DHCP server from the Cisco Unified CallManager database.

Procedure

- Step 1** Find the DHCP subnet by using the procedure in the [“Finding a DHCP Subnet”](#) section on page 11-1.
- Step 2** From list of matching records, choose the DHCP subnet that you want to delete.
- Step 3** Click the **Delete Selected Item** icon that displays in the tool bar in the upper, left corner of the window (or click the **Delete Selected** button that displays at the bottom of the window) to delete the subnet.

If the subnet is not in use, Cisco Unified CallManager deletes it. If it is in use, a message displays.



Note You can delete multiple DHCP servers from the Find and List Servers window by checking the check boxes next to the appropriate servers and clicking **Delete Selected**. You can delete all servers in the window by clicking **Select All** and then clicking **Delete Selected**.

Additional Information

See the [“Related Topics”](#) section on page 11-5.

Related Topics

- [Finding a DHCP Subnet, page 11-1](#)
- [Configuring a DHCP Subnet, page 11-2](#)
- [Deleting a DHCP Subnet, page 11-4](#)
- [DHCP Subnet Configuration Settings, page 11-3](#)
- [DHCP Server Configuration, page 10-1](#)
- [Dynamic Host Configuration Protocol, *Cisco Unified CallManager System Guide*](#)



LDAP System Configuration

In Cisco Unified CallManager Release 5.0 and above, directory configuration takes place in three related windows:

- LDAP System
- LDAP Directory
- LDAP Authentication

Changes to LDAP Directory information and LDAP Authentication settings are possible only if synchronization from the customer's LDAP directory is enabled in the Cisco Unified CallManager Administration LDAP System window.

Administrators use this window to enable LDAP synchronization and to set up the LDAP server type and the LDAP attribute name for the user ID.



Note

After an LDAP Directory configuration for the DirSync service gets created or the LDAP user authentication is enabled, the settings in the LDAP System window become read-only.

Use the following topics to configure LDAP system information:

- [Updating LDAP System Information, page 12-1](#)
- [LDAP System Configuration Settings, page 12-2](#)

Additional Information

See the [“Related Topics” section on page 12-3](#).

Updating LDAP System Information

Use the following procedure to update LDAP system information.

Before You Begin

The setting of the Enable Synchronizing from LDAP Server check box in this window affects the administrator's ability to modify end users. LDAP synchronization applies only to end users; LDAP synchronization does not affect application users. Refer to the [“Understanding the Directory” section on page 20-1](#) for more information about LDAP synchronization.

For end user data, administrators cannot use the End User Configuration window to update the attributes that get synchronized from the corporate directory. These attributes can be updated only in the corporate directory itself, after which a resynchronization should be performed.

**Note**

If end users exist in the Cisco Unified CallManager database before synchronization with a corporate directory occurs, these end users will be deleted. If Cisco Unified CallManager was already synchronized with a different type of server, existing users will be marked with a *Delete Pending* status. A garbage collector program that runs nightly will delete these users from the database.

Procedure

- Step 1** Choose **System > LDAP > LDAP System**.
- Step 2** Enter the appropriate configuration settings as described in [Table 12-1](#).
- Step 3** To save your changes, click **Save**.

Additional Information

See the “[Related Topics](#)” section on page 12-3.

LDAP System Configuration Settings

[Table 12-1](#) describes the LDAP system configuration settings. For related procedures, see the “[Related Topics](#)” section on page 12-3.

Table 12-1 LDAP System Configuration Settings

Field	Description
LDAP System Information	
Enable Synchronizing from LDAP Server	To enable synchronization of data from the customer’s LDAP server, check this check box. If synchronization with the LDAP server is enabled, the following circumstances occur: - The administrator cannot modify end user data, except for the fields (attributes) that are not synchronized from the corporate directory. Example: user PIN. (The administrator can always modify application user data.) - The administrator can modify the LDAP Directory information. - The administrator can modify LDAP Authentication information. If synchronization with the LDAP server is not enabled (is disabled), the following circumstances occur: - The administrator cannot modify LDAP Directory information. - The administrator cannot modify LDAP Authentication information.

Table 12-1 LDAP System Configuration Settings (continued)

Field	Description
LDAP Server Type	If synchronization with the LDAP server is currently enabled, you can choose one of the selections in this drop-down list box. Choose the value that corresponds to the customer's LDAP server type: • Microsoft Active Directory • Netscape LDAP Server
LDAP Attribute for User ID	If synchronization with the LDAP server is enabled, you can choose an LDAP attribute value for the user ID. Choose one of the following values from the drop-down list box: • for Microsoft Active Directory: – sAMAccountName – mail – employeeNumber • for Netscape LDAP Server: – uid – mail – employeeNumber

Related Topics

- [LDAP System Configuration, page 12-1](#)
- [Updating LDAP System Information, page 12-1](#)
- [LDAP System Configuration Settings, page 12-2](#)
- [Understanding the Directory, Cisco Unified CallManager System Guide](#)
- [LDAP Directory Configuration, page 13-1](#)
- [LDAP Authentication Configuration, page 14-1](#)
- [Application User Configuration, page 86-1](#)
- [End User Configuration, page 87-1](#)
- [Application Users and End Users, Cisco Unified CallManager System Guide](#)



LDAP Directory Configuration

Directory configuration takes place in three related windows:

- LDAP System
- LDAP Directory
- LDAP Authentication

Changes to LDAP Directory information and LDAP Authentication settings are possible only if synchronization from the customer's LDAP directory is enabled in the Cisco Unified CallManager Administration LDAP System window.

Use the following topics to configure LDAP directory information:

- [Finding an LDAP Directory, page 13-1](#)
- [Configuring an LDAP Directory, page 13-2](#)
- [Related Topics, page 13-6](#)
- [Deleting an LDAP Directory, page 13-5](#)

For more information, see the “[Related Topics](#)” section on [page 13-6](#).

Finding an LDAP Directory

Use the following procedure to locate LDAP directory configurations.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your LDAP directory search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your LDAP directory search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **System > LDAP > LDAP Directory**.

The Find and List LDAP Directories window displays. Use the two drop-down list boxes to search for a LDAP directory.

Step 2 From the first Find LDAP Directory where drop-down list box, choose one of the following criteria:

- LDAP Configuration Name
- LDAP Manager Distinguished Name
- LDAP User Search Base

From the second Find LDAP Directory where drop-down list box, choose one of the following criteria:

- begins with
- contains
- is exactly
- ends with
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Tip To find all LDAP directories that are registered in the database, click **Find** without entering any search text.

A list of discovered LDAP directories displays by

- LDAP Configuration Name
- LDAP Manager Distinguished Name
- LDAP User Search Base

Step 4 From the list of records, click the LDAP directory name that matches your search criteria.

The window displays the LDAP directory that you choose.

Additional Information

See the [“Related Topics” section on page 13-6](#).

Configuring an LDAP Directory

This section describes how to add or update information about an LDAP directory that is used to synchronize user data with the Cisco Unified CallManager Administration database.

Procedure

Step 1 Choose **System > LDAP > LDAP Directory**.

The Find and List LDAP Directories window displays.

Step 2 Perform one of the following tasks:

- To add new information about an LDAP directory, locate the appropriate directory as described in the [“Finding an LDAP Directory” section on page 13-1](#), click the **Add New** button, and continue with [Step 3](#).

- To update existing information about an LDAP directory, locate the appropriate directory as described in the [“Finding an LDAP Directory” section on page 13-1](#) and continue with [Step 3](#).

Step 3 Enter the appropriate settings as described in [Table 13-1](#).

Step 4 Click **Save**.

The new LDAP directory gets added or updated to the Cisco Unified CallManager database.

Additional Information

See the [“Related Topics” section on page 13-6](#).

LDAP Directory Configuration Settings

[Table 13-1](#) describes the LDAP directory configuration settings. For related procedures, see the [“Related Topics” section on page 13-6](#).

Table 13-1 **LDAP Directory Configuration Settings**

Field	Description
LDAP Directory Information	
LDAP Configuration Name	Enter a unique name (up to 40 characters) for the LDAP directory.
LDAP Manager Distinguished Name	Enter the user ID (up to 128 characters) of the LDAP Manager, who is an administrative user that has access rights to the LDAP directory in question.
LDAP Password	Enter a password (up to 128 characters) for the LDAP Manager.
Confirm Password	Re-enter the password that you provided in the LDAP Password field.
LDAP User Search Base	Enter the location (up to 256 characters) where all LDAP users exist. This location is a container or a directory. This information varies depending on customer setup.
LDAP Directory Synchronization Schedule	
Perform Sync Just Once	If you want to perform synchronization of the data in this LDAP directory with the data in the Cisco Unified CallManager database only once, check this check box.
Perform a Re-sync Every	If you want to perform synchronization of the data in this LDAP directory with the data in the Cisco Unified CallManager database at a regular interval, use these fields. In the left field, enter a number. In the drop-down list box, choose a value: • hours • days • weeks • months Note This field is active only if you do not check the Perform Sync Just Once check box.

Table 13-1 LDAP Directory Configuration Settings (continued)

Field		Description
Next Re-sync Time (YYYY-MM-DD hh:mm)		Specify a time to perform the next synchronization of Cisco Unified CallManager directory data with this LDAP directory. Use a 24-hour clock to specify the time of day. For example, 1:00 pm is 13:00.
User Fields To Be Synchronized		
Cisco Unified CallManager User Fields	LDAP User Fields	
User ID	sAMAccountName	For these fields, the Cisco Unified CallManager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.
Middle Name	(drop-down list box)	For these fields, the Cisco Unified CallManager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right. For the LDAP User field, choose one of the following values: - middleName - initials
Manager ID	manager	For these fields, the Cisco Unified CallManager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.
Phone Number	(drop-down list box)	For these fields, the Cisco Unified CallManager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right. For the LDAP User field, choose one of the following values: - telephoneNumber - ipPhone
First Name	givenName	For these fields, the Cisco Unified CallManager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.
Last Name	sn	For these fields, the Cisco Unified CallManager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.
Department	department	For these fields, the Cisco Unified CallManager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.
Mail ID	(drop-down list box)	For these fields, the Cisco Unified CallManager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right. For the LDAP User field, choose one of the following values: - mail - sAMAccountName

Table 13-1 LDAP Directory Configuration Settings (continued)

Field	Description
LDAP Server Information	
Host Name or IP Address for Server	Enter the host name or IP address of the server where the data for this LDAP directory resides.
LDAP Port	Enter the port number on which the corporate directory receives the LDAP requests. Default LDAP port for Microsoft Active Directory and for Netscape Directory specifies 389. Default LDAP port for Secured Sockets Layer (SSL) specifies 636. Note You can only access this field if LDAP authentication for end users is enabled.
Use SSL	Check this check box to use Secured Sockets Layer (SSL) encryption for security purposes. Note You can only access this field if LDAP authentication for end users is enabled.
Add Another Redundant LDAP Server	Click this button to add another row for entry of information about an additional server.

Deleting an LDAP Directory

This section describes how to delete an LDAP directory in Cisco Unified CallManager Administration.

Before You Begin

When you delete an LDAP directory, Cisco Unified CallManager removes information about that directory from the database.

**Note**

You can delete multiple LDAP directories from the Find and List LDAP directories window by checking the check boxes next to the appropriate LDAP directories and clicking **Delete Selected**. You can delete all LDAP directories in the window by clicking **Select All** and then clicking **Delete Selected**.

Procedure

- Step 1** Find the LDAP directory that you want to delete by using the procedure in the [“Finding an LDAP Directory”](#) section on page 13-1.
- Step 2** Click the name of the LDAP directory that you want to delete.
The LDAP directory that you chose displays.
- Step 3** Click **Delete**.
You receive a message that asks you to confirm the deletion.
- Step 4** Click **OK**.
The window refreshes, and the LDAP directory gets deleted from the database.

Additional Information

See the “Related Topics” section on page 13-6.

Related Topics

- [LDAP Directory Configuration, page 13-1](#)
- [Finding an LDAP Directory, page 13-1](#)
- [Configuring an LDAP Directory, page 13-2](#)
- [Deleting an LDAP Directory, page 13-5](#)
- [Understanding the Directory, *Cisco Unified CallManager System Guide*](#)
- [LDAP System Configuration, page 12-1](#)
- [LDAP Authentication Configuration, page 14-1](#)
- [Application Users and End Users, *Cisco Unified CallManager System Guide*](#)
- [Application User Configuration, page 86-1](#)
- [End User Configuration, page 87-1](#)



LDAP Authentication Configuration

In Cisco Unified CallManager Release 5.0 and above, directory configuration takes place in three related windows:

- LDAP System
- LDAP Directory
- LDAP Authentication

Changes to LDAP directory information and LDAP authentication settings are possible only if synchronization with the customer's LDAP directory is enabled in the Cisco Unified CallManager Administration LDAP System window.

Use the following topics to configure LDAP authentication information:

- [Updating LDAP Authentication Information, page 14-1](#)
- [LDAP Authentication Configuration Settings, page 14-2](#)

Updating LDAP Authentication Information

Use the following procedure to update LDAP authentication information.

Before You Begin

The setting of the Enable Synchronizing from LDAP Server check box in the LDAP System Configuration window affects the administrator's ability to modify LDAP authentication settings. If synchronization with the LDAP server is enabled, administrators cannot modify LDAP directory information and LDAP authorization settings. Refer to the [“Understanding the Directory” section on page 20-1](#) for more information about LDAP synchronization.

Conversely, if you want to enable administrators to modify LDAP directory information and LDAP authorization settings, you must disable synchronization with the LDAP server.

Procedure

-
Step 1	Choose System > LDAP > LDAP Authentication .
Step 2	Enter the appropriate configuration settings as described in Table 14-1 .
Step 3	To save your changes, click Save .
-

Additional Information

See the [“Related Topics”](#) section on page 14-3.

LDAP Authentication Configuration Settings

Table 14-1 describes the LDAP authentication configuration settings. For related procedures, see the [“Related Topics”](#) section on page 14-3.

Table 14-1 LDAP Authentication Configuration Settings

Field	Description
LDAP Authentication for End Users	
Use LDAP Authentication for End Users	Click this check box to require authentication of end users from the LDAP directory. If the check box is left unchecked, authentication gets performed against the database. Note You can only access this field if LDAP synchronization is enabled in the LDAP System Configuration window.
LDAP Manager Distinguished Name	Enter the user ID of the LDAP Manager, who is an administrative user that has access rights to the LDAP directory in question. Note You can only access this field if LDAP authentication for end users is enabled.
LDAP Password	Enter a password for the LDAP Manager. Note You can only access this field if LDAP authentication for end users is enabled.
Confirm Password	Re-enter the password that you provided in the LDAP Password field. Note You can only access this field if LDAP authentication for end users is enabled.
LDAP User Search Base	Enter the user search base. Cisco Unified CallManager searches for users under this base. Note You can only access this field if LDAP authentication for end users is enabled.
LDAP Server Information	
Host Name or IP Address for Server	Enter the host name or IP address where you installed the corporate directory. Note You can only access this field if LDAP authentication for end users is enabled.
LDAP Port	Enter the port number on which the corporate directory receives the LDAP requests. Default LDAP port for Microsoft Active Directory and for Netscape Directory specifies 389. Default LDAP port for Secured Sockets Layer (SSL) specifies 636. Note You can only access this field if LDAP authentication for end users is enabled.

Table 14-1 LDAP Authentication Configuration Settings (continued)

Field	Description
Use SSL	Check this check box to use SSL encryption for security purposes. Note You can only access this field if LDAP authentication for end users is enabled.
Add Another Redundant LDAP Server	Click this button to add another row for entry of information about an additional server. Note You can only access this button if LDAP authentication for end users is enabled.

Related Topics

- [LDAP Authentication Configuration, page 14-1](#)
- [Updating LDAP Authentication Information, page 14-1](#)
- [LDAP Authentication Configuration Settings, page 14-2](#)
- [Understanding the Directory, Cisco Unified CallManager System Guide](#)
- [LDAP System Configuration, page 12-1](#)
- [LDAP Directory Configuration, page 13-1](#)
- [Application Users and End Users, Cisco Unified CallManager System Guide](#)
- [Application User Configuration, page 86-1](#)
- [End User Configuration, page 87-1](#)



Location Configuration

Use locations to implement call admission control in a centralized call-processing system. Call admission control enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between the locations. For more information, refer to the [“Call Admission Control”](#) section in the *Cisco Unified CallManager System Guide*.



Note

If you do not use call admission control to limit the audio and video bandwidth on an IP WAN link, an unlimited number of calls can be active on that link at the same time. This situation can cause the audio quality of each audio call and the video quality of each video call to degrade as the link becomes oversubscribed.

In a centralized call-processing system, a single Cisco Unified CallManager cluster provides call processing for all locations on the IP telephony network. The Cisco Unified CallManager cluster usually resides at the main (or central) location, along with other devices such as phones and gateways. The remote locations contain additional devices, but no Cisco Unified CallManager. IP WAN links connect the remote locations to the main location.

The following topics explain locations in more detail:

- [Finding a Location, page 15-1](#)
- [Configuring a Location, page 15-3](#)
- [Location Configuration Settings, page 15-4](#)
- [Deleting a Location, page 15-5](#)
- [Resynchronizing a Location Bandwidth, page 15-6](#)
- [Related Topics, page 15-7](#)

Finding a Location

Because you might have several locations in your network, Cisco Unified CallManager Administration lets you locate specific locations on the basis of specific criteria. Use the following procedure to find locations.

**Note**

During your work in a browser session, Cisco Unified CallManager Administration retains your location search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your location search preferences until you modify your search or close the browser.

Procedure**Step 1** Choose **System > Location**.

The Find and List Locations window displays. Use the two drop-down list boxes to search for a location.

Step 2 From the first Find locations where drop-down list box, choose one of the following criteria:

- Location
- Audio Bandwidth

**Note**

The criterion that you choose in this drop-down list box specifies how the list of location that your search generates will be sorted. For example, if you choose Bandwidth, the Bandwidth column will display as the left column of the results list.

From the second Find locations where drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.**Tip**

To find all locations that are registered in the database, click **Find** without entering any search text.

A list of discovered locations displays by

- Location icon
- Location Name
- Bandwidth

**Note**

You can delete multiple locations from the Find and List Locations window by checking the check boxes next to the appropriate locations and clicking **Delete Selected**. You can delete all locations in the window by checking the check box in the Matching records title bar and clicking **Delete Selected**.

Step 4 From the list of records, click the Location name that matches your search criteria.

The window displays information on the location that you choose.

Additional Information

See the [“Related Topics” section on page 15-7](#).

Configuring a Location

This section describes how to add, copy, or update a location to the Cisco Unified CallManager database.

Before You Begin

Before configuring a location, you must configure the Cisco Unified CallManagers that form the cluster. For details, see the [“Updating a Cisco Unified CallManager” section on page 3-2](#)

Procedure

Step 1 Choose **System > Location**.

The Find and List Locations window displays.

Step 2 Perform one of the following tasks:

- To copy an existing location, locate the appropriate location as described in the [“Finding a Location” section on page 15-1](#), click the **Copy** button next to the location that you want to copy, and continue with [Step 3](#).
- To add a new location, click the **Add New** button and continue with [Step 3](#).
- To update an existing location, locate the appropriate location as described in the [“Finding a Location” section on page 15-1](#) and continue with [Step 3](#).

Step 3 Enter the appropriate settings as described in [Table 15-1](#).

Step 4 To save the location information in the database, click **Save**.

Next Steps

After adding a new location to the database, you can assign devices to that location; for example, see:

- [Gateway Configuration, page 69-1](#)
- [Cisco Unified IP Phone Configuration, page 70-1](#)
- [CTI Route Point Configuration, page 67-1](#)

Additional Information

See the [“Related Topics” section on page 15-7](#).

Location Configuration Settings

Table 15-1 describes the location configuration settings. For related procedures, see the “[Related Topics](#)” section on page 15-7.

Table 15-1 **Location Configuration Settings**

Field	Description
Location Information	
Name	Enter the name of the new location that you are creating.
Audio Calls Information	
Audio Bandwidth	Enter the maximum amount of audio bandwidth (in kbps) that is available for all audio calls on the link between this location and other locations. For audio calls, the audio bandwidth includes overhead. Choose between the following options: - Unlimited bandwidth—Click the Unlimited radio button. - Specified bandwidth—Specify a bandwidth by clicking the radio button next to the kbps box and entering a specified bandwidth. Valid values are 1 to 2147483647. For purposes of location bandwidth calculations only, assume that each call stream consumes the following amount of bandwidth: - G.711 call uses 80 kbps. - G.722 call uses 80 kbps. - G.723 call uses 24 kbps. - G.728 call uses 16 kbps. - G.729 call uses 24 kbps. - GSM call uses 29 kbps. - Wideband call uses 272 kbps. Note Each call comprises two call streams. To improve audio quality, lower the bandwidth setting, so fewer active calls are allowed on the link to this location.
Video Calls Information	
Video Bandwidth	Enter the maximum amount of video bandwidth (in kbps) that is available for all video calls on the link between this location and other locations. For video calls, the video bandwidth does not include overhead. Choose between the following options: - None—Video calls are not allowed between this location and other locations. Video calls can, however, take place within this location. - Unlimited bandwidth—Click the Unlimited radio button. - Specified bandwidth—Specify a video bandwidth by clicking the radio button next to the kbps box and entering a specified video bandwidth. The default value is 384 kbps.

Table 15-1 **Location Configuration Settings (continued)**

Field	Description
Locations RSVP Settings	
Location	This display-only field displays locations for which the interlocation RSVP setting has been changed from the system default RSVP policy.
RSVP Setting	This display-only field displays the RSVP policy setting between the selected location and the location listed in the Location column to the left.
Modify Setting(s) to Other Locations	
Location	To change the RSVP policy setting between the current location and a location that displays in this pane, choose a location in this pane.
RSVP Setting	To choose an RSVP policy setting between the current location and the location chosen in the Location pane at left, choose an RSVP setting from the drop-down list box. The following settings are available: • Use System Default—The RSVP policy for the location pair matches the clusterwide RSVP policy. See the “Clusterwide Default RSVP Policy” section of the <i>Cisco Unified CallManager System Guide</i> for details. • No Reservation—No RSVP reservations are made between any two locations. • Optional (Video Desired)—A call can proceed as a best-effort audio-only call if failure to obtain reservations for both audio and video streams occurs. RSVP Agent continues to attempt RSVP reservation and informs Cisco Unified CallManager if reservation succeeds. • Mandatory—Cisco Unified CallManager does not ring the terminating device until RSVP reservation succeeds for the audio stream and, if the call is a video call, for the video stream as well. • Mandatory (Video Desired)—A video call can proceed as an audio-only call if a reservation for the video stream cannot be reserved.

Deleting a Location

This section describes how to delete a location from the Cisco Unified CallManager database.

Before You Begin

You cannot delete a location to which devices are assigned. To find out which devices are using the location, click **Dependency Records** from **Related Links** in the Location Configuration window, then click **Go**. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the “[Accessing](#)

[Dependency Records](#)” section on page A-2. If you try to delete a location that is in use, Cisco Unified CallManager displays an error message. Before deleting a location that is currently in use, you must perform either or both of the following tasks:

- Update the devices to assign them to a different location.
- Delete the devices that are assigned to the location that you want to delete.

**Note**

Deleting a location allocates infinite bandwidth for the links that are connected to that location and allows an unlimited number of calls on those links. Deleting a location can cause audio quality on the links to degrade.

Procedure

-
- Step 1** Find the location by using the procedure in the [“Finding a Location”](#) section on page 15-1.
- Step 2** From the list of matching records, choose the location that you want to delete.
- Step 3** Click **Delete Selected**.
- Step 4** When prompted to confirm the delete operation, click either **OK** to confirm deletion or **Cancel** to cancel the delete operation.
-

Additional Information

See the [“Related Topics”](#) section on page 15-7.

Resynchronizing a Location Bandwidth

This section describes how to resynchronize the bandwidth for a location. When calls are blocked from using the link for a location, bandwidth leakage may have occurred that may reduce the allotted bandwidth for the location. You can resynchronize the location bandwidth to the maximum amount that is assigned to this location without resetting the Cisco Unified CallManager server. For more information, refer to the [“Bandwidth Calculations”](#) section in the Call Admission Control chapter of the *Cisco Unified CallManager System Guide*.

Procedure

-
- Step 1** Find the location by using the procedure in the [“Finding a Location”](#) section on page 15-1.
- Step 2** From the list of matching records, choose the location that you want to resynchronize.
The Location Configuration window displays.
- Step 3** To resynchronize the bandwidth for the chosen location click **Resync Bandwidth**.
This warning message appears: “If calls are using the bandwidth for this location when the bandwidth is resynchronized, the bandwidth might be oversubscribed until all calls that are using the bandwidth for this location disconnect.”
- Step 4** To continue click **OK** or click **Cancel**.
-

Additional Information

See the [“Related Topics”](#) section on page 15-7.

Related Topics

- [Location Configuration, page 15-1](#)
- [Finding a Location, page 15-1](#)
- [Configuring a Location, page 15-3](#)
- [Location Configuration Settings, page 15-4](#)
- [Deleting a Location, page 15-5](#)
- [Resynchronizing a Location Bandwidth, page 15-6](#)



Survivable Remote Site Telephony Configuration

A survivable remote site telephony (SRST) reference comprises the gateway that can provide limited Cisco Unified CallManager functionality when all other Cisco Unified CallManager servers for a device are unreachable. Typically assigned to device pools, SRST references determine the gateways where calling devices search when they attempt to complete a call if Cisco Unified CallManager is unavailable. For more detailed information on SRST references, refer to the [“Survivable Remote Site Telephony References”](#) section in the *Cisco Unified CallManager System Guide*.

Use the following topics to add, update, copy, or delete a SRST reference:

- [Finding an SRST Reference, page 16-1](#)
- [Configuring an SRST Reference, page 16-2](#)
- [Deleting an SRST Reference, page 16-3](#)
- [SRST Reference Configuration Settings, page 16-4](#)

Finding an SRST Reference

Because you might have several SRST references in your network, Cisco Unified CallManager lets you locate specific SRST references based on specific criteria. Use the following procedure to locate SRST references that are defined by a particular user.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your SRST reference search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your SRST reference search preferences until you modify your search or close the browser.

Procedure

- Step 1** Choose **System > SRST**.
- The Find and List SRST References window displays.
- Step 2** From the drop-down list box, choose one of the following criteria:
- begins with
 - contains

- ends with
- is exactly

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Note To find all user-defined SRST references that are registered in the database, click **Find** without entering any search text.

A list of discovered SRST references displays by

- SRST Reference Name
- IP Address
- Port



Note You can delete multiple SRST references from the Find and List SRST References window by checking the check boxes next to the appropriate SRST references and clicking **Delete Selected**. You can choose all the SRST references in the window by checking the check box in the matching records title bar and clicking **Delete Selected**.

Step 4 From the list of records, click the SRST reference that matches your search criteria.
The window displays the SRST reference that you chose.

Additional Information

See the [“Related Topics” section on page 16-5](#).

Configuring an SRST Reference

The following procedure describes how to add, update or copy an SRST reference.

Procedure

Step 1 Choose **System > SRST**.

Step 2 Perform one of the following tasks:

- To add a new SRST reference, click the **Add New** button and continue with [Step 3](#).
- To update an existing SRST reference, locate the appropriate SRST reference as described in the [“Finding an SRST Reference” section on page 16-1](#) and continue with [Step 3](#).
- To copy an existing SRST reference, locate the appropriate SRST reference as described in the [“Finding an SRST Reference” section on page 16-1](#), click the **Copy** button next to the SRST reference that you want to copy, and continue with [Step 3](#).

Step 3 Enter or update the appropriate settings as described in [Table 16-1](#).

Step 4 Click **Save**.



Note If devices are associated with this SRST reference, a message displays to tell you that devices need to be reset for the update to take effect. Cisco Unified CallManager may drop calls in progress on an affected gateway may be dropped when the gateway is reset.

To reset the affected devices, click the **Reset Devices** button when the update is complete. If you do not want to reset the devices at this time, you can return to this item at any time and click the **Reset Devices** button to initiate the required device resets.

Additional Information

See the [“Related Topics” section on page 16-5](#).

Deleting an SRST Reference

The following procedure describes how to delete an SRST reference.

Before You Begin

You cannot delete SRST references that device pools or other items are using. To find out which device pools are using the SRST reference, click the **Dependency Records** link from the SRST Reference Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#). If you try to delete an SRST reference that is in use, Cisco Unified CallManager displays an error message. Before deleting an SRST reference that is currently in use, you must perform either or both of the following tasks:

- Assign a different SRST reference to any device pools that are using the SRST reference that you want to delete. Refer to the [“Configuring a Device Pool” section on page 9-3](#).
- Delete the device pools that are using the SRST reference that you want to delete. See the [“Deleting a Device Pool” section on page 9-7](#).

Procedure

-
- Step 1** In the menu bar, choose **System > SRST**.
- Step 2** Locate the SRST reference that you want to delete. See the [“Finding an SRST Reference” section on page 16-1](#).
- Step 3** Check the check box of the SRST reference that you want to delete and click **Delete Selected**.
A message displays, that tells you that you cannot undo this action.
- Step 4** To delete the SRST reference, click **OK** or to cancel the deletion, click **Cancel**.



Caution Before initiating this action, check carefully to ensure that you are deleting the correct SRST reference. You cannot retrieve deleted SRST references. If an SRST reference is accidentally deleted, you must rebuild it.

**Tip**

You can also delete an SRST reference by locating and displaying the SRST reference that you want to delete and clicking **Delete**.

Additional Information

See the [“Related Topics” section on page 16-5](#).

SRST Reference Configuration Settings

Table 16-1 describes the SRST reference configuration settings. For related procedures, see the [“Related Topics” section on page 16-5](#).

Table 16-1 *SRST Reference Configuration Settings*

Field	Description
SRST Reference Name	Enter a name in the SRST Reference Name field. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each SRST reference name is unique. Note Use concise and descriptive names for your SRST references.
IP Address	Enter the IP address of the gateway for devices in a device pool to use as an SRST reference.
Port	Enter the port number for this SRST reference. Default value specifies 2000. Note Change this value only if it does not match the gateway port setting. This value and the gateway port setting must match.
SIP Network/IP Address	Enter the IP address of the server that the SIP phones will use when in SRST mode.
SIP Port	Enter the SIP port of the SRST gateway. Default value specifies 5060.
Is SRST Secure?	After you verify that the SRST-enabled gateway contains a self-signed certificate, check this check box. After you configure the SRST and reset the gateway and dependent phones, the Cisco CTL Provider service authenticates to the Certificate Provider service on the SRST-enabled gateway. The Cisco CTL client retrieves the certificate from the SRST-enabled gateway and stores the certificate in the Cisco Unified CallManager database. Tip To remove the SRST certificate from the database and phone, uncheck this check box, click Save , and reset the dependent phones.

Table 16-1 SRST Reference Configuration Settings (continued)

Field	Description
SRST Certificate Provider Port	This port monitors requests for the Certificate Provider service on the SRST-enabled gateway. Cisco Unified CallManager uses this port to retrieve the certificate from the SRST-enabled gateway. The Cisco SRST Certificate Provider default port equals 2445. After you configure this port on the SRST-enabled gateway, enter the port number in this field. Tip You may need to configure a different port number if the port is currently used or if you use a firewall and you cannot use the port within the firewall.
Update Certificate	 Tip This button displays only after you check the Is SRST Secure? check box and click Save. After you click this button, the Cisco CTL client replaces the existing SRST-enabled gateway certificate that is stored in the Cisco Unified CallManager database, if a certificate exists in the database. After you reset the dependent phones, the TFTP server sends the cnf.xml file (with the new SRST-enabled gateway certificate) to the phones.

Related Topics

- [Finding an SRST Reference, page 16-1](#)
- [Configuring an SRST Reference, page 16-2](#)
- [Deleting an SRST Reference, page 16-3](#)
- [SRST Reference Configuration Settings, page 16-4](#)
- [Survivable Remote Site Telephony References](#), *Cisco Unified CallManager System Guide*.



MLPP Domain Configuration

An MLPP domain specifies the collection of devices and resources that are associated with an MLPP subscriber. When an MLPP subscriber that belongs to a particular domain places a precedence call to another MLPP subscriber that belongs to the same domain, MLPP service can preempt the existing call that the called MLPP subscriber is on for a higher precedence call. MLPP service availability does not go across different domains.

Use the following topics to add, update, or delete MLPP domains:

- [Finding an MLPP Domain, page 17-1](#)
- [Configuring an MLPP Domain, page 17-2](#)
- [MLPP Domain Configuration Settings, page 17-3](#)
- [Deleting an MLPP Domain, page 17-3](#)

Finding an MLPP Domain

Because you might have several MLPP domains in your network, Cisco Unified CallManager Administration lets you locate specific MLPP domains on the basis of specific criteria. Use the following procedure to locate MLPP domains.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your MLPP domain search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your MLPP domain search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **System > MLPP Domain**.

The Find and List MLPP Domains window displays. Use the two drop-down list boxes to search for an MLPP Domain.

Step 2 From the first Find MLPP Domains where drop-down list box, choose the following criterion:

- Name

From the second Find MLPP Domains where drop-down list box, choose one of the following criteria:

- begins with
- contains
- is exactly
- ends with
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Tip

To find all MLPP domains that are registered in the database, click **Find** without entering any search text.

A list of discovered MLPP domains displays by name.



Note

You can delete multiple MLPP domains from the Find and List MLPP Domains window by checking the check boxes next to the appropriate MLPP domains and clicking **Delete Selected**. You can delete all MLPP domains in the window, other than the Default MLPP domain, by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records, click the MLPP domain name that matches your search criteria. The MLPP Domain Configuration window displays the MLPP domain that you choose.

Additional Information

See the [“Related Topics” section on page 17-4](#).

Configuring an MLPP Domain

This section describes how to configure an MLPP domain in the Cisco Unified CallManager database.

Procedure

Step 1 Choose **System > MLPP Domain**.

The Find and List MLPP Domains window displays.

Step 2 Perform one of the following tasks:

- To copy an existing MLPP domain, locate the appropriate MLPP domain as described in the [“Finding an MLPP Domain” section on page 17-1](#), click the **Copy** button next to the MLPP domain that you want to copy, and continue with [Step 3](#).
- To add a new MLPP domain, click the **Add New** button, and continue with [Step 3](#).
- To update an existing MLPP domain, locate the appropriate MLPP domain as described in the [“Finding an MLPP Domain” section on page 17-1](#), and continue with [Step 3](#).

- Step 3** In the MLPP Domain Configuration window that displays, enter or edit the appropriate settings as described in [Table 17-1](#).
- Step 4** Click **Save** to save the new or updated MLPP domain in the database.

Additional Information

See the [“Related Topics”](#) section on page 17-4.

MLPP Domain Configuration Settings

[Table 17-1](#) describes the MLPP domain configuration settings.

Table 17-1 MLPP Domain Configuration Settings

Field	Description
MLPP Domain Information	
Domain Name	Enter the name that you want to assign to the new MLPP domain. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each MLPP domain name is unique. Note The name of the default MLPP domain specifies <i>Default</i>. The <i>Default</i> domain cannot be changed nor deleted.
Domain ID (e. g., “0000FF”)	Enter a unique six-character hexadecimal MLPP domain ID. Valid values are numeric characters 0 through 9 and alphabetic characters A through F. Ensure that each MLPP domain ID is unique. Domain IDs must fall in the range between 000001 and FFFFFFFF. (000000 is reserved for the default MLPP domain ID.) Note Use leading zeroes for values lower than 100000.

Additional Information

See the [“Related Topics”](#) section on page 17-4.

Deleting an MLPP Domain

This section describes how to delete an MLPP domain from the Cisco Unified CallManager database.

Before You Begin

You cannot delete an MLPP Domain that any device is using. To find out which devices are using the MLPP domain, from the MLPP Domain Configuration window, choose **Dependency Records** from the Related Links drop-down list box and click **Go**. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency

records, refer to the [“Accessing Dependency Records” section on page A-2](#). If you try to delete an MLPP Domain that is in use, Cisco Unified CallManager displays an error message. Before deleting an MLPP Domain that is currently in use, you must perform either or both of the following tasks:

- Assign a different MLPP domain to any devices that are using the MLPP domain that you want to delete.
- Delete the devices that are using the MLPP domain that you want to delete.

Procedure

-
Step 1	Find the MLPP domain by using the procedure in the “Finding an MLPP Domain” section on page 17-1 .
Step 2	From the list of matching records, choose the MLPP domain that you want to delete.
Step 3	Click Delete .
Step 4	When prompted to confirm the delete operation, click either OK to delete or Cancel to cancel the delete operation.
-

Additional Information

See the [“Related Topics” section on page 17-4](#).

Related Topics

- [Finding an MLPP Domain, page 17-1](#)
- [Configuring an MLPP Domain, page 17-2](#)
- [MLPP Domain Configuration Settings, page 17-3](#)
- [Deleting an MLPP Domain, page 17-3](#)
- [Multilevel Precedence and Preemption](#), *Cisco Unified CallManager Features and Services Guide*



Enterprise Parameters Configuration

Enterprise parameters provide default settings that apply to all devices and services in the same cluster. (A cluster comprises a set of Cisco Unified CallManagers that share the same database.) When you install a new Cisco Unified CallManager, it uses the enterprise parameters to set the initial values of its device defaults. For more information on device defaults, refer to the [“Device Defaults Configuration” section on page 72-1](#) and refer to the [“System-Level Configuration Settings”](#) section of the *Cisco Unified CallManager System Guide*.

You cannot add or delete enterprise parameters, but you can use the following procedure to update existing enterprise parameters.



Note

Many of the enterprise parameters rarely require change. Do not change an enterprise parameter unless you fully understand the feature that you are changing or unless the Cisco Technical Assistance Center (TAC) specifies the change.

Procedure

Step 1 Choose **System > Enterprise Parameters**.

Step 2 Update the appropriate parameter settings.

To view the description of a particular enterprise parameter, click the parameter name. To view the descriptions of all the enterprise parameters, click the ? button.

Step 3 Click **Save** to save the changes in the database.



Service Parameters Configuration

Service parameters for Cisco Unified CallManager allow you to configure different services on selected servers. You can view a list of parameters and their descriptions by clicking the question mark button in the Service Parameters Configuration window. You can view the list with a particular parameter at the top by clicking that parameter.

If you deactivate a service by using Cisco Unified CallManager Serviceability, Cisco Unified CallManager retains any updated service parameter values. If you start the service again, Cisco Unified CallManager sets the service parameters to the changed values.



Note

For information about what happens to service parameter values during an upgrade, refer to *Upgrading Cisco Unified CallManager*.

For more information about Cisco Unified CallManager services, refer to the *Cisco Unified CallManager Serviceability System Guide* and the *Cisco Unified CallManager Serviceability Administration Guide*.

Before You Begin

Ensure the following prerequisites are met before proceeding with the steps:

- Make sure that servers are configured. Refer to the [“Server Configuration” section on page 2-1](#) for more information.
- Make sure that the service is available on the servers. The Service Parameter Configuration window displays all the available services (active or not active). Refer to the *Cisco Unified CallManager Serviceability Administration Guide* for more information.



Caution

Some changes to service parameters may cause system failure. Cisco recommends that you do not make any changes to service parameters unless you fully understand the feature that you are changing or unless the Cisco Technical Assistance Center (TAC) specifies the changes.

Use the following topics to configure or display service parameters:

- [Configuring Service Parameters for a Service on a Server, page 19-2](#)
- [Displaying Parameters for a Service, page 19-3](#)

Configuring Service Parameters for a Service on a Server

Use the following procedure to configure the service parameters for a particular service on a particular server.

Procedure

- Step 1** Choose **System > Service Parameters**.
- Step 2** From the Server drop-down list box, choose a server.
- Step 3** From the Service drop-down list box, choose the service that contains the parameter that you want to update.



Note The Service Parameter Configuration window displays all services (active or not active).

The Service Parameters Configuration window displays.

- Step 4** Update the appropriate parameter value. To set all service parameters for this instance of the service to the default values, click the **Set to Default** button.

To view a list of parameters and their descriptions, click the question mark button as shown in [Figure 19-1](#). To view the list with a particular parameter at the top, click that parameter in the Service Parameters Configuration window.

Figure 19-1 Service Parameter Configuration Window

NavigationCisco Unified CallManager

Cisco Unified CallManager AdministrationFor Cisco IP Telecommunication SolutionsLogged in as

SystemCall RoutingMedia ResourcesVoice MailDeviceApplicationUser ManagementBulk AdministrationHelp

Service Parameter ConfigurationRelated Links: Parameters f

Status

Status: Ready

Select Server and Service

Server *nw095a-149 (Active)

Service *Cisco IP Manager Assistant (Inactive)

All parameters apply only to the current server except parameters that are in the Clusterwide group(s).

Cisco IP Manager Assistant (Inactive) Parameters on server nw095a-149 (Active)

Parameter Name	Parameter Value	Suggested Value
CTIManager (Primary) IP Address *		
CTIManager (Backup) IP Address		
Route Point Device Name for Proxy Mode	< None >	
CAPF Profile Instance ID for Secure Connection to CTIManager	< None >	

Clusterwide Parameters (Parameters that apply to all servers)

[Cisco IPMA Server \(Primary\) IP Address *](#)

[Cisco IPMA Server \(Backup\) IP Address](#)

141829

**Note**

Some services contain service parameters that should rarely be changed. Cisco Unified CallManager Administration does not automatically display these parameters when you access the Service Parameters Configuration window. To view all parameters, click **Advanced**. After all parameters display, you can redisplay the basic parameters by clicking **Condensed**. If the **Advanced** button is disabled, all parameters for that service display by default.

Step 5 Click **Save**.

The window refreshes, and Cisco Unified CallManager updates the service parameter with your changes.

Additional Information

See the [“Related Topics” section on page 19-4](#).

Displaying Parameters for a Service

You may need to compare all service parameters that belong to a particular service on all servers in a cluster. You may also need to display only out-of-sync parameters (that is, service parameters for which values differ from one server to another) or parameters that have been modified from the suggested value.

Use the following procedure to display the service parameters for a particular service on all servers in a cluster.

Procedure

Step 1 Choose **System > Service Parameters**.

Step 2 From the Server drop-down list box, choose a server.

Step 3 From the Service drop-down list box, choose the service for which you want to display the service parameters on all servers in a cluster.

**Note**

The Service Parameter Configuration window displays all services (active or not active).

Step 4 In the Service Parameters Configuration window that displays, choose Parameters for All Servers in the Related Links drop-down list box, then click **Go**.

The Parameters for All Servers window displays. For the current service, the list shows all parameters in alphabetical order. For each parameter, the suggested value displays next to the parameter name. Under each parameter name, a list of servers that contain this parameter displays. Next to each server name, the current value for this parameter on this server displays.

For a given parameter, click on the server name or on the current parameter value to link to the corresponding service parameter window to change the value. Click **Previous** and **Next** to navigate between Parameters for All Servers windows.

Step 5 If you need to display out-of-sync service parameters, choose Out of Sync Parameters for All Servers in the Related Links drop-down list box, then click **Go**.

The Out of Sync Parameters for All Servers window displays. For the current service, service parameters that have different values on different servers display in alphabetical order. For each parameter, the suggested value displays next to the parameter name. Under each parameter name, a list of servers that contain this parameter displays. Next to each server name, the current value for this parameter on this server displays.

For a given parameter, click on the server name or on the current parameter value to link to the corresponding service parameter window to change the value. Click **Previous** and **Next** to navigate between Out of Sync Parameters for All Servers windows.

Step 6 If you need to display service parameters that have been modified from the suggested value, choose Modified Parameters for All Servers in the Related Links drop-down list box, then click **Go**.

The Modified Parameters for All Servers window displays. For the current service, service parameters that have values different from the suggested values display in alphabetical order. For each parameter, the suggested value displays next to the parameter name. Under each parameter name, a list of servers that have different values from the suggested values displays. Next to each server name, the current value for this parameter on this server displays.

For a given parameter, click on the server name or on the current parameter value to link to the corresponding service parameter window to change the value. Click **Previous** and **Next** to navigate between Modified Parameters for All Servers windows.

Additional Information

See the [“Related Topics”](#) section on page 19-4.

Related Topics

- [Displaying Parameters for a Service, page 19-3](#)
- [Configuring Service Parameters for a Service on a Server, page 19-2](#)
- *Cisco Unified CallManager Serviceability System Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*



SIP Phone Security Profile Configuration

Cisco Unified CallManager Administration groups security-related settings in the SIP phone security profile, which works like a template; that is, you configure the settings in the profile and then apply the profile to the SIP phone. After you apply the profile to the phone, it uses the settings that you configured in the SIP Phone Security Profile window. If you want to do so, you can use the same profile for many SIP phones, which eliminates having to configure the same fields multiple times.

The SIP Phone Security Profile window includes security-related settings such as Device Security Mode, Authentication Mode (for CAPF), Key Size (for CAPF), Enable Digest Authentication, Nonce Validity Time, Transport Type, and SIP Phone Port.



Tip

All SIP phones require that you apply a security profile.

For information on configuring and applying a SIP phone security profile, refer to the *Cisco Unified CallManager Security Guide*.



SIP Trunk Security Profile Configuration

Cisco Unified CallManager Administration groups security-related settings in the SIP trunk security profile, which works like a template; that is, you configure the settings in the profile and then apply the profile to the SIP trunk. After you apply the profile to the trunk, it uses the settings that you configured in the SIP Trunk Security Profile window. If you want to do so, you can use the same profile for many SIP trunks, which eliminates having to configure the same fields multiple times.

The SIP Trunk Security Profile window includes security-related settings such as Incoming Transport Type, Outgoing Transport Type, Device Security Mode, Enable Digest Authentication, Nonce Validity Time, X.509 Subject Name, Incoming Port, Enable Application Level Authorization, Accept Presence Subscription, Accept Out-of-Dialog REFER, Accept Unsolicited Notification, and Accept Header Replacement.



Tip

All SIP trunks require that you apply a security profile.

For information on configuring and applying a SIP trunk security profile, refer to the *Cisco Unified CallManager Security Guide*.



SCCP Phone Security Profile Configuration

Cisco Unified CallManager Administration groups security-related settings in the SCCP phone security profile, which works like a template; that is, you configure the settings in the profile and then apply the profile to the SCCP phone. After you apply the profile to the phone, it uses the settings that you configured in the SCCP Phone Security Profile window. If you want to do so, you can use the same profile for many SCCP phones, which eliminates having to configure the same fields multiple times.

The SCCP Phone Security Profile window includes security-related settings such as Device Security Mode, Authentication Mode (for CAPF), and Key Size (for CAPF).



Tip

All SCCP phones require that you apply a security profile.

For information on configuring and applying a SCCP phone security profile, refer to the *Cisco Unified CallManager Security Guide*.



Application Server Configuration

You can use the Application Server windows in Cisco Unified CallManager Administration to maintain associations between the Cisco Unified CallManager and off-cluster, external applications, such as Cisco Unity and Cisco Unity Connection, and to synchronize Cisco Unified CallManager systems and other applications.

The following topics provide information about working with and configuring application servers in Cisco Unified CallManager Administration:

- [Configuring Application Servers, page 23-1](#)
- [Deleting an Application Server, page 23-2](#)
- [Finding an Application Server, page 23-3](#)
- [Application Server Configuration Settings, page 23-3](#)

Additional Information

See the “[Related Topics](#)” section on [page 23-4](#).

Configuring Application Servers

The following procedure describes how to configure application servers in Cisco Unified CallManager Administration.

Before You Begin

You can configure the application servers in Cisco Unified CallManager Administration after both the Cisco Unified CallManager servers and any other application servers are set up and fully operational and are running with a valid configuration.



Note

For Cisco Unity and Cisco Unity Connection, make sure that AXL is running on the Cisco Unified CallManager server that was configured to communicate with the Cisco Unity and Cisco Unity Connection server.

Procedure

- Step 1** Choose **System > Application Server**.

The Find and List Application Servers window displays.

- Step 2** Perform one of the followings tasks:
- To copy an existing application server, locate the server that you want to copy as described in [Finding an Application Server, page 23-3](#); click the server name. The Application Server Configuration window displays. Click the **Copy** button and continue with [Step 4](#).
 - To add a new application server, click the **Add New** button, and continue with [Step 3](#).
 - To update an existing application server, locate the appropriate server as described in [Finding an Application Server, page 23-3](#), and continue with [Step 4](#).
- Step 3** From the Application Server Type drop-down list box, choose the appropriate server type and click **Next**. After you choose an application server type, you cannot modify it.
- Step 4** Enter the appropriate settings as described in [Table 23-1](#).
- Step 5** Click **Save**.
-

Additional Information

See the [“Related Topics” section on page 23-4](#).

Deleting an Application Server

To delete an application server by using Cisco Unified CallManager Administration, perform the following procedure.

Procedure

-
- Step 1** Choose **System > Application Server**.
- The Find and List Application Servers window displays.
- Step 2** To locate a specific application server, enter search criteria and click **Find**.
- A list of application servers that match the search criteria displays.
- Step 3** Perform one of the following actions:
- Check the check boxes next to the application servers that you want to delete and click **Delete Selected**.
 - Delete all the application servers in the window by clicking **Select All** and then **Delete Selected**.
 - Choose the name of the application server that you want to delete from the list to display its current settings and click **Delete**.
- A confirmation dialog displays.
- Step 4** Click **OK**.
-

Additional Information

See the [“Related Topics” section on page 23-4](#).

Application Server Configuration Settings

Table 23-1 describes the available settings in the Application Server window. For related procedures, see the “Related Topics” section on page 23-4.

Table 23-1 Application Server Configuration Settings

Field	Description
Device Information	
Name	Enter a name to identify the application server that you are configuring.
IP Address	Enter the IP address of the server that you are configuring. Note Ensure the IP address is numeric with a number pattern between 1-255 (10.255.172.57).  Tip For Cisco Unity and Cisco Unity Connection, you must use the same Administrator user name and password that you defined in Cisco Unity and Cisco Unity Connection Administration. This user ID provides authentication between Cisco Unity or Cisco Unity Connection and Cisco Unified CallManager Administration.
Application User	From the drop-down list box, enter the type of application user that you want for this server (for example, CCMAAdministrator, CCMSysUser, and so on).

Additional Information

See the “Related Topics” section on page 23-4.

Finding an Application Server

The following procedure describes how to find and list application servers.

Procedure

- Step 1** Choose **System > Application Server**.
The Find and List Application Servers window displays.
- Step 2** Choose the field that you want to specify to locate an application server.


Note To find all application servers, click **Find**.
- Step 3** Choose the appropriate search pattern for your text search.
- Step 4** In the Find field, enter your search text, if any.

Step 5 Click **Find**.

A list of application servers that match the criteria displays. The field that you chose in [Step 2](#) determines how the servers in the list are sorted.

This window also lists the total number of servers in this window.

Step 6 To view the next set of discovered application servers, click **Next**.**Note**

You can delete multiple application servers from the Find and List Application Servers window by checking the check boxes next to the appropriate servers and clicking **Delete Selected** to delete the servers, or you can click **Select All** to select the servers and then **Delete Selected**. You can choose all the phones in the window by checking the check box in the matching records title bar.

Additional Information

See the “[Related Topics](#)” section on page 23-4.

Related Topics

- [Cisco Unity Messaging Integration](#), *Cisco Unified CallManager System Guide*
- [Application User Configuration](#), page 86-1



License Unit Report

Use license unit report to display the total license capacity and the number of licenses in use. This tool generates a report that lists the total number of available licenses.



Note

To know more about requesting licenses, refer to the *Cisco Unified CallManager System Guide*.

Generating a License Unit Report

A unit license refers to a fixed number of license units that correspond to each phone type. For example, Cisco 7920 phones requires four license units and Cisco 7970 phones require five units. If you are provisioning four Cisco 7920 phones and four Cisco 7970 phones, then you require 36 phone license units.

The number of licensed units in the license file corresponds to number of unit licenses for all the phone types that are purchased.



Note

To determine the number of license unit that are required for each device, choose **System > Licensing > License Unit Calculator**. This window lists the number of license units that are required for each type of device.

Use the following procedure to generate a report for the number of licenses that are available.

Procedure

-
- Step 1** Choose **System > Licensing > License Unit Report**.
- Step 2** The License Unit Report window displays. This window displays the number of phone licenses and number of node licenses that are available by:
- Units Available
 - Units Used
 - Units Remaining
-

Additional Information

See the [“Related Topics” section on page 24-2](#).

Related Topics

- [License Unit Report, page 24-1](#)
- [Generating a License Unit Report, page 24-1](#)
- [License Unit Calculator, page 25-1](#)
- [License File Upload, page 26-1](#)



License Unit Calculator

Use this window to calculate the number of phone unit licenses that are required for a specific configuration of type of phones and number of phones of each type. A unit license refers to a fixed number of license units that correspond to each phone type. Cisco 7920 phones requires four license units and Cisco 7970 phones require five units. If you are provisioning four Cisco 7920 phones and four Cisco 7970 phones, then you require 36 phone license units.

Calculating License Units

Use the following procedure to calculate the number of phone licenses that are required when the number of phone types and the total number of phones per phone type is entered.

Procedure

- Step 1** Choose **System > License > License Unit Calculator**.
- The License Unit Calculator window displays. The number of license units that are consumed per device displays corresponding to the node or device.
- Step 2** In the Number of Devices column, update the number of needed devices corresponding to each node or phone.
- Step 3** Click **Calculate**.
- The total number of Cisco Unified CallManager node license units and phone license units displays.
-

Additional Information

See the [“Related Topics” section on page 25-1](#).

Related Topics

- [License Unit Calculator, page 25-1](#)
- [Calculating License Units, page 25-1](#)
- [License Unit Report, page 24-1](#)
- [License File Upload, page 26-1](#)

- [Licensing](#), *Cisco Unified CallManager System Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*



License File Upload

License file contains the information that is needed to enforce licenses for Cisco Unified CallManager application. This chapter contains the following topics:

- [Obtaining a License File, page 26-1](#)
- [License File Contents, page 26-2](#)
- [Uploading a License file, page 26-3](#)
- [Related Topics, page 26-4](#)

Obtaining a License File

Use the following steps to obtain a license file for a new installation of Cisco Unified CallManager 5.0 phones nodes and for updating the licenses when new phones are added.

-
- Step 1** When you place an order for Cisco devices, Cisco provides a Product Authorization Key (PAK).
- Step 2** Register the PAK with Cisco Unified CallManager using the License Registration web tool that is provided on CCO.
- Step 3** You must enter the MAC address of the Cisco Unified CallManager server that you are requesting the licenses for, and a valid E-mail Id. You must enter the number of nodes and phone units that you want licenses for.



Note You can determine the number of phone unit licenses that you will require for each phone type using License Calculator in Cisco Unified CallManager Administration. See the [“Calculating License Units” section on page 25-1](#).

- Step 4** CCO generates a license file with the number of unit licenses that you requested and sends it you via E-mail using the E-mail ID that you provided in step [Step 2](#)
- Step 5** You must upload the license file to the server with the matching MAC address that you provided in [Step 3](#) See the [“Uploading a License file” section on page 26-3](#). This server then takes on the functionality of the license manager.
-

**Note**

For updating the licenses when you buy new phones, go to the License Registration web tool that is provided on CCO and follow the steps 3 through 5.

**Note**

The license file is uploaded into the database, only if the version specified in the license file is greater than or equal to the Cisco Unified CallManager version that is running in the cluster. If the version check fails, an alarm gets generated, and you should get a new license file with the correct version. The system bases the version check only on major releases.

**Note**

The licenses specified in the license file can be used only within the cluster on which the license file is uploaded.

Additional Information

See the [“Related Topics”](#) section on page 26-4.

License File Contents

The license file contains the following information:

- Number of Cisco Unified CallManager nodes that are licensed: This indicates number of Cisco Unified CallManager servers in a cluster that are licensed to the customer.
- Versions of the Cisco Unified CallManager that are supported.
- Number of phone units licensed: Instead of creating a separate license for each phone type, a concept of unit license is used. Each phone type corresponds to a fixed number of license units.

**Note**

To determine the number of license unit that are required for each device, choose **System > Licensing > License Unit Calculator**. This window lists the number of license units required for each type of device. See the [“Calculating License Units”](#) section on page 25-1.

- MAC address of the server, where the license file can be installed.

To upload a license file to the license server, see the [“Uploading a License file”](#) section on page 26-3.

Sample License Files

The following examples describe license files for permanent IP phone licenses and permanent Cisco Unified CallManager node licenses:

Example 26-1 Permanent IP Phone Licenses

```
INCREMENT PHONE_UNIT cisco 5.0 permanent uncounted \

VENDOR_STRING=<Count>1000</Count><OrigMacId>000BCD4EE59D</OrigMacId><LicFileVersion>1.0</LicFileVersion> \
HOSTID=000bcd4ee59d OVERDRAFT=50 \
NOTICE="<LicFileID>20050826140539162</LicFileID><LicLineID>2</LicLineID> \
<PAK></PAK>" SIGN="112D 17E4 A755 5EDC F616 0F2B B820 AA9C \
```

```
0313 A36F B317 F359 1E08 5E15 E524 1915 66EA BC9F A82B CBC8 \
4CAF 2930 017F D594 3E44 EBA3 04CD 01BF 38BA BF1B"
```

The preceding license file includes following information:

- No expiration date for this license exists as indicated by the keyword permanent.
- This license file provides 1000 PHONE_UNIT licenses.
- OVERDRAFT=50 indicates (5% of 1000) allowed overdraft. Cisco determines the overdraft value.
- The Cisco specific fieldLicFileID, identifies this license file.
- You can add multiple increment lines for same feature (phone unit license or node license) in a license file to increase the license count. None of the INCREMENT lines should be identical and each of them should be signed independently.

Example 26-2 Permanent CCM_Node licenses

```
# Optional usage agreement, legal language, tracking information
# Some other comments
INCREMENT CCM_NODE cisco 5.0 permanent uncounted \
VENDOR_STRING=<Count>3</Count><OrigMacId>000BCD4EE59D</OrigMacId><LicFileVersion>1.0</LicF
ileVersion> \
HOSTID=000bcd4ee59d \
NOTICE="<LicFileID>20050826140539162</LicFileID><LicLineID>1</LicLineID> \
<PAK></PAK>" SIGN="19B3 4C6C 25AC 6D22 4D75 DE6A 656B 08C5 \
30E4 16DB 771B 1393 9DC1 DBC4 C5AA 15CC 6E6C B7B8 895A DCBA \
B40F C551 2625 1C97 F20D 9977 6CFF 3603 081E 6FF2"
```

The preceding license file includes the following information:

- No expiration date for this license exists as indicated by the keyword permanent.
- This license file provides three licenses for the version 5.0 of the feature CCM_NODES.
- The Cisco specific fieldLicFileID, identifies this license file.
- You can add multiple increment lines for same feature in a license file to increase the license count. None of the INCREMENT lines should be identical and each of them should be signed independently.

Additional Information

See the [“Related Topics”](#) section on page 26-4.

Uploading a License file

Use the following procedure to upload a license file to the Cisco Unified CallManager server with the matching MAC address that is provided when requesting for a license file. For information about obtaining a license file see the [“Obtaining a License File”](#) section on page 26-1. The Cisco Unified CallManager server where the license file is loaded takes on the functionality of the license manager.



Note

Upload the license file only on the first node of Cisco Unified CallManager cluster.

Procedure

Step 1 Choose **System > License > Upload License File**.

The License File Upload window displays.

Step 2 The Existing License Files drop-down list box displays the license files that are already uploaded to the server.



Note Click **View File** to view the file content of any existing files.

Step 3 To choose a new license file to upload, click **Upload License File**.

The Upload File pop-up window displays.

Step 4 Browse and choose a license file to upload to the server.

Step 5 Click **Upload License File**.

After the upload process is complete, the Upload Result file displays.

Step 6 Click **Close**.

Step 7 In the License File Upload window, the status of the uploaded file displays.

Additional Information

See the [“Related Topics”](#) section on page 26-4.

Related Topics

- [Obtaining a License File, page 26-1](#)
- [License File Contents, page 26-2](#)
- [Uploading a License file, page 26-3](#)
- [Calculating License Units, page 25-1](#)
- [Generating a License Unit Report, page 24-1](#)
- [Licensing, Cisco Unified CallManager System Guide](#)
- [Cisco Unified CallManager Features and Services Guide](#)



Autoregistration Configuration

Use autoregistration if you want Cisco Unified CallManager to assign directory numbers automatically to new phones as they connect to the IP telephony network.



Note

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

After a phone has auto-registered, you can move it to a new location and assign it to a different device pool without affecting its directory number.

This section covers the following topics:

- [Enabling Autoregistration, page 27-1](#)
- [Disabling Autoregistration, page 27-2](#)
- [Autoregistration Configuration Settings, page 27-3](#)
- [Reusing Autoregistration Numbers, page 27-4](#)

Enabling Autoregistration

This section describes how to enable autoregistration for new devices.



Caution

Cisco Unified CallManager disables autoregistration by default. Enabling autoregistration carries a security risk in that “rogue” phones can automatically register with Cisco Unified CallManager. You should enable autoregistration only for brief periods when you want to perform bulk phone adds.

Configuring mixed mode clusterwide security through the Cisco CTL Client automatically disables autoregistration. If you want to use autoregistration and you have configured security, you must change the clusterwide security mode to non-secure through the Cisco CTL Client.

Procedure

- Step 1** Choose **System** > Cisco Unified CallManager.
- Step 2** From the list of Cisco Unified CallManagers, choose the Cisco Unified CallManager that you want to enable for autoregistration.
- Step 3** Enter the appropriate Autoregistration Information, as described in [Table 27-1](#).

- Step 4** Click **Save** to save the changes in the database.
- Step 5** Repeat [Step 2](#) through [Step 4](#) for each Cisco Unified CallManager that you want to enable for autoregistration. You can designate only one primary Cisco Unified CallManager for autoregistration, but you can designate other Cisco Unified CallManagers as backups for purposes of autoregistration. See the [“Redundancy”](#) section in the *Cisco Unified CallManager System Guide*.
- Step 6** Choose **System > Cisco Unified CallManager Group**.
- Step 7** From the list of Cisco Unified CallManager groups, choose the group that is enabled for autoregistration. (In most systems, the name of this group is Default.) This group serves as the default Cisco Unified CallManager group for devices that auto-register. Make sure that the Selected list for this group contains the Cisco Unified CallManagers that you configured for autoregistration in [Step 2](#). The Cisco Unified CallManagers get selected in the order that they are listed in the Cisco Unified CallManager group.
- Step 8** If you made any changes to the group configuration, click **Save** to save the changes in the database.
- Step 9** Choose **System > Device Pool**.
- Step 10** From the list of device pools, choose one of the default device pools that are assigned in the Device Defaults (refer to the [“Device Defaults Configuration”](#) section on page 72-1). Cisco Unified CallManager assigns each auto-registered device to a default device pool based on the device type.
- Step 11** From the drop-down list box for Cisco Unified CallManager Group, choose the Cisco Unified CallManager group that you configured for autoregistration in [Step 7](#). This step assigns the default device pool to the default Cisco Unified CallManager group for autoregistration.
- Step 12** From the drop-down list box for Calling Search Space for Auto-Registration, choose the calling search space to assign to the devices in this device pool that auto-register with Cisco Unified CallManager. The calling search space specifies the route partitions that are used by the devices in the pool.
- Step 13** Click **Save** to save the device pool changes in the database.
- Step 14** Repeat [Step 10](#) through [Step 13](#) for each device pool that is listed in the Device Defaults.

Additional Information

See the [“Related Topics”](#) section on page 27-5.

Disabling Autoregistration

This section describes how to disable autoregistration.

Procedure

-
- Step 1** Choose **System > Cisco Unified CallManager**.
 - Step 2** From the Cisco Unified CallManager list, choose the Cisco Unified CallManager where you want to disable autoregistration.
 - Step 3** Click the Auto-registration Disabled option to disable autoregistration for this Cisco Unified CallManager (when this box is checked, autoregistration is disabled).

**Note**

You can also disable autoregistration by setting the Starting Directory Number and Ending Directory Number to the same value.

Step 4 Click **Save** to save the changes in the database.

Step 5 Repeat [Step 2](#) through [Step 4](#) for each Cisco Unified CallManager where you want to disable autoregistration.

Additional Information

See the [“Related Topics” section on page 27-5](#).

Autoregistration Configuration Settings

[Table 27-1](#) describes the autoregistration configuration settings. For more information about related procedures, see the [“Related Topics” section on page 27-5](#).

Table 27-1 **Autoregistration Configuration Settings**

Field Name	Description
Starting Directory Number	Enter the first directory number to use for autoregistration of devices. Specifying a range of directory numbers in the Starting Directory Number and Ending Directory Number fields automatically enables autoregistration. Setting the starting and ending directory numbers to the same value disables autoregistration.
Ending Directory Number	Enter the last directory number to use for autoregistration of devices. Specifying a range of directory numbers in the Starting Directory Number and Ending Directory Number fields automatically enables autoregistration. Setting the starting and ending directory numbers to the same value disables autoregistration.
Partition	Choose the partition to which auto-registered directory numbers belong. If you are not using partitions, choose <None>. You must choose a valid directory number range for autoregistration before you can choose a partition and external phone number mask. The partition field resets if you disable autoregistration. If a large number of partitions exist, the ellipsis (...) button displays next to the drop-down list box. Click the ... button to display the Select Partition window. Enter a partial partition name in the List items where Name contains field. Click the desired partition name in the list of partitions that displays in the Select item to use box, and click OK.

Table 27-1 **Autoregistration Configuration Settings (continued)**

Field Name	Description
External Phone Number Mask	Specify the mask that is used to format caller ID information for external (outbound) calls that are made from the auto-registered devices. The mask can contain up to 50 characters. Enter the literal digits that you want to appear in the caller ID information and use Xs to represent the directory number of the auto-registered device. For example, if you specify a mask of 972813XXXX and enable the Use External Phone Number Mask option on the route pattern that is used to make the external call, an external call from extension 1234 displays a caller ID number of 9728131234. If you specify a mask of all literal digits (such as 9728135000) to represent a main attendant number, that literal number becomes the caller ID that displays for an external call from any auto-registered device.
Auto-registration Disabled on this Cisco Unified CallManager	Cisco Unified CallManager disables autoregistration by default to prevent unauthorized connections to the network. When autoregistration is disabled, you must configure the directory numbers manually whenever you add new devices to your network. • Uncheck the Auto-registration Disabled option to enable autoregistration for this Cisco Unified CallManager. • Check the Auto-registration Disabled option to disable autoregistration for this Cisco Unified CallManager. You can disable autoregistration by setting the Starting Directory Number and Ending Directory Number to the same value. If starting and ending directory numbers are specified when you disable autoregistration by checking this option, Cisco Unified CallManager sets the starting and ending directory numbers to the same value. The partition and external phone mask information fields also reset when you disable autoregistration.

Reusing Autoregistration Numbers

When you connect a new device to the network, Cisco Unified CallManager assigns the next available (unused) autoregistration directory number to that device. If you manually change the directory number of an auto-registered device, or if you delete that device from the database, Cisco Unified CallManager can reuse the autoregistration directory number of that device.

When a device attempts to auto-register, Cisco Unified CallManager searches the range of autoregistration numbers that you specified and tries to find the next available directory number to assign to the device. It begins the search with the next directory number in sequence after the last one that was assigned. If it reaches the ending directory number in the range, Cisco Unified CallManager continues to search from the starting directory number in the range.

You can use the following procedure to reset the range of autoregistration directory numbers and force Cisco Unified CallManager to search from the starting number in the range.

Procedure

-
- Step 1** Choose **System** > Cisco Unified CallManager.
- Step 2** Choose the Cisco Unified CallManager where you want to reset autoregistration.
- Step 3** Write down the current settings for Starting Directory Number and Ending Directory Number.
- Step 4** Click **Auto-registration Disabled on this** Cisco Unified CallManager.



Caution New phones cannot auto-register while autoregistration is disabled.

- Step 5** Click **Save**.
- Step 6** Set the Starting Directory Number and Ending Directory Number to their previous values (or to new values, if desired).
- Step 7** Click **Save**.
-

Additional Information

See the [“Related Topics” section on page 27-5](#).

Related Topics

- [Enabling Autoregistration, page 27-1](#)
- [Disabling Autoregistration, page 27-2](#)
- [Autoregistration Configuration Settings, page 27-3](#)
- [Reusing Autoregistration Numbers, page 27-4](#)



PART 3

Call Routing Configuration





Automated Alternate Routing Group Configuration

Automated alternate routing (AAR) provides a mechanism to reroute calls through the PSTN or other network by using an alternate number when Cisco Unified CallManager blocks a call due to insufficient location bandwidth. With automated alternate routing, the caller does not need to hang up and redial the called party. The AAR group represents the dialing area where the line/directory number (DN), the Cisco voice mail port, and the gateway are located.

For each AAR group, you enter the prefix digits that are used for automated alternate routing within the AAR group, as well as the prefix digits used for automated alternate routing between a given AAR group and other AAR groups. Devices, such as gateways, phones (by means of directory numbers), and trunks, associate with AAR groups. If automated alternate routing of calls takes place, you may also associate devices with an AAR calling search space.

Use the following topics to find, add, update, or delete AAR groups:

- [Finding an AAR Group, page 28-1](#)
- [Configuring an AAR Group, page 28-2](#)
- [AAR Group Configuration Settings, page 28-3](#)
- [Deleting an AAR Group, page 28-4](#)
- [AAR Group Configuration Settings, page 28-3](#)



Note

For AAR to function, you must configure AAR groups and also ensure that the Automated Alternate Routing Enable clusterwide service parameter is set to *True*. (The default value for this service parameter specifies *False*.)

Refer to the “[Understanding Route Plans](#)” section of the *Cisco Unified CallManager System Guide* for more information about automated alternate routing groups.

Finding an AAR Group

Because you might have several automated alternate routing (AAR) groups in your network, Cisco Unified CallManager lets you locate specific AAR groups based on specific criteria. Use the following procedure to locate AAR groups.

**Note**

During your work in a browser session, Cisco Unified CallManager Administration retains your AAR group search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your AAR group search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Call Routing > AAR Group**.

The Find and List Automated Alternate Routing Groups window displays.

Step 2 From the drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.

**Note**

To find all AAR groups that are registered in the database, click **Find** without entering any search text.

A list of discovered AAR groups displays by AAR group name.

Step 4 From the list of records, click the AAR group that matches your search criteria.

The window displays the AAR group that you choose.

Additional Information

See the [“Related Topics” section on page 28-5](#).

Configuring an AAR Group

The following procedure describes how to configure an AAR group.

Procedure

Step 1 Choose **Call Routing > AAR Group**.

The Find and List Automated Alternate Routing Groups window displays.

Step 2 Perform one of the followings tasks:

- To copy an existing AAR group, locate the appropriate AAR group as described in the “[Finding an AAR Group](#)” section on page 28-1, click the **Copy** button next to the AAR group that you want to copy, and continue with [Step 3](#).
- To add a new AAR group, click the **Add New** button, and continue with [Step 3](#).
- To update an existing AAR group, locate the appropriate AAR group as described in the “[Finding an AAR Group](#)” section on page 28-1, and continue with [Step 3](#).

Step 3 In the AAR Group Configuration window that displays, enter a name in the AAR Group Name field. The name can contain alphanumeric characters, any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure each AAR group name is unique. The current size for this field is 20 characters.



Timesaver

Use concise and descriptive names for your AAR groups. The CompanynameLocationGroup format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify an AAR group. For example, CiscoDallasAA1 identifies a Cisco Access Analog AAR group for the Cisco office in Dallas.

Step 4 Click **Save**.

Step 5 Choose the appropriate settings as described in [Table 28-1](#).

Step 6 To configure this AAR group, click **Save**.

Additional Information

See the “[Related Topics](#)” section on page 28-5.

AAR Group Configuration Settings

[Table 28-1](#) describes the AAR group configuration settings.

Table 28-1 AAR Group Configuration Settings

Field	Description
AAR Group Name	Enter the name that you want to assign to the new AAR group. The name can contain up to 20 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).
Prefix Digits Within This Group	
Prefix Digits	Enter the prefix digits to use for automated alternate routing within this AAR group. Valid entries include the following digits: [^ 0 1 2 3 4 5 6 7 8 9 -] + ? ! X * # . @

Table 28-1 AAR Group Configuration Settings (continued)

Field	Description
Prefix Digits Between This Group and Other AAR Groups	
Prefix Digits (From this group)	Enter the prefix digits to use for automated alternate routing when routing a call from this group to a device that belongs to another AAR group. Valid entries include the following digits: [^ 0 1 2 3 4 5 6 7 8 9 -] + ? ! X * # . @ Note Prefix digits that are entered in this field for the originating AAR group also get added in the Prefix Digits (To this group) field of the AAR destination group.
Prefix Digits (To this group)	Enter the prefix digits to use for automated alternate routing when you are routing a call to this group from a device that belongs to another AAR group. Valid entries include the following digits: [^ 0 1 2 3 4 5 6 7 8 9 -] + ? ! X * # . @ Note Prefix digits entered in this field for the destination AAR group also get added in the Prefix Digits (From this group) field of the AAR originating group.

Additional Information

See the [“Related Topics” section on page 28-5](#).

Deleting an AAR Group

The following procedure describes how to delete an AAR group.

Before You Begin

You cannot delete an AAR group that one or more devices references. To find out which devices are using the AAR group, click the **Dependency Records** link from the AAR Group Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#). You must remove the AAR group from all devices to which it belongs before deleting the AAR group.

Procedure

-
- Step 1** Choose **Call Routing > AAR Group** in the menu bar.
- Step 2** Locate the AAR group that you want to delete. See the [“Finding an AAR Group” section on page 28-1](#).
- Step 3** Check the check box next to the AAR group that you want to delete and click **Delete Selected**.
- A dialog box displays to warn you that you cannot undo deletion of AAR groups.

- Step 4** To delete the group, click **OK**, or to cancel the action, click **Cancel** . If you click **OK**, the Cisco Unified CallManager removes the AAR group from the AAR group list.

**Note**

You can delete multiple AAR groups from the Find and List AAR groups window by checking the check boxes next to the appropriate AAR groups and clicking **Delete Selected**. You can delete all the AAR groups in the window by clicking **Select All** and then clicking **Delete Selected**.

Additional Information

See the [“Related Topics”](#) section on page 28-5.

Related Topics

- [Finding an AAR Group, page 28-1](#)
- [Configuring an AAR Group, page 28-2](#)
- [AAR Group Configuration Settings, page 28-3](#)
- [Deleting an AAR Group, page 28-4](#)
- [Automated Alternate Routing, Cisco Unified CallManager System Guide](#)



Application Dial Rules Configuration

The administrator uses dial rules configuration to add and sort the priority of dialing rules. Dial rules for applications such as Cisco Unified CallManager Assistant automatically strip numbers from or add numbers to telephone numbers that a user dials. For example, the dial rules automatically add the digit 9 in front of a 7-digit telephone number to provide access to an outside line.

For example, in Cisco Unified CM Assistant, the assistant can perform a directory search from the assistant console. The assistant can drag and drop the directory entry to the My Calls panel on the assistant console, which invokes a call to the number that is listed in the entry. The dial rules apply to the number that is listed in the entry before the call gets made.

The following sections describe dial rules configuration:

- [Finding a Dial Rule, page 29-1](#)
- [Configuring Dial Rules, page 29-2](#)
- [Deleting a Dial Rule, page 29-4](#)
- [Reprioritizing a Dial Rule, page 29-4](#)

Finding a Dial Rule

Because you might have several dial rules in your network, Cisco Unified CallManager lets you locate specific dial rules based on specific criteria. Use the following procedure to locate dial rules.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your dial rule search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your dial search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Call Routing > Dial Rules > Application Dial Rules**.

The Find and List Application Dial Rules window displays.

- Step 2** From the first Find Application Dial Rule where drop-down list box, choose one of the following criteria:
- Name
 - Description
 - Number Begins With
- Step 3** From the second Find Application Dial Rule where drop-down list box, choose one of the following criteria:
- begins with
 - contains
 - ends with
 - is exactly
 - is empty
 - is not empty
- Step 4** Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Note To find all application dial rules that are registered in the database, click **Find** without entering any search text.

A list of discovered application dial rules displays.

- Step 5** From the list of records, click the dial rule that matches your search criteria.
The window displays the dial rule that you choose.

Additional Information

See the [“Related Topics” section on page 29-5](#).

Configuring Dial Rules

Perform the following procedure to add a new dial rule or update an existing dial rule. See [Application Dial Rules Configuration Error Checking](#) in the *Cisco Unified CallManager System Guide* for dial rule design and error checking.

Procedure

- Step 1** In the menu bar, choose **Call Routing > Dial Rules > Application Dial Rules**.
The Find and List Application Dial Rules window displays.
- Step 2** Perform one of the followings tasks:
- To add a new dial rule, click the **Add New** button, and continue with [Step 3](#).
 - To update an existing dial rule, locate the appropriate dial rule as described in [“Finding a Dial Rule” section on page 29-1](#), and continue with [Step 3](#).

Step 3 Enter the appropriate dial rule information settings as found in [Table 29-1](#).

Step 4 Click the **Save** button.



Note If more than one dial rule exists, you can change the priority of the dial rules. See the [“Reprioritizing a Dial Rule”](#) section on page 29-4.

Additional Information

See the [“Related Topics”](#) section on page 29-5.

Application Dial Rule Configuration Settings

[Table 29-1](#) describes the available settings in the Application Dial Rule Configuration window. For more information about related procedures, see the [“Related Topics”](#) section on page 29-5.

Table 29-1 *Dial Rule Configuration Settings*

Field	Description
Name	Enter a name in the Name field. The name can contain up to 20 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure each application dial rule name is unique.
Description	Enter a description of the application dial rule in the Description field or leave blank.
Number Begins With	Enter the initial digits of the directory numbers to which you want to apply this application dial rule. Valid values include numeric digits (0 through 9), plus (+), asterisk (*), and pound (#).
Number of Digits	Enter the length of the directory numbers to which you want to apply this application dial rule. Enter a digit between 1 and 100 or the characters +*#.
Total Digits to be Removed	Enter the number of digits that you want Cisco CallManager to remove from directory numbers that apply to this dial rule. Enter a digit between 0 and 100.
Prefix With Pattern	Enter the pattern to prepend to directory numbers that apply to this application dial rule. Valid values include digits (0 through 100), plus (+), asterisk (*), and pound (#).
Application Dial Rule Priority	Choose the dial rule priority as top, bottom, or middle.  Note This field displays when you enter the Prefix With Pattern information.

Additional Information

See the [“Related Topics” section on page 29-5](#).

Deleting a Dial Rule

Perform the following procedure to delete a dial rule.

Procedure

-
- Step 1** From Cisco Unified CallManager Administration, choose **Call Routing > Dial Rules > Application Dial Rules**.
- Step 2** Locate the application dial rule that you want to delete. See the [“Finding a Dial Rule” section on page 29-1](#).
- Step 3** Check the check box next to the application dial rule that you want to delete and click **Delete Selected**.
A dialog box appears to warn you that you cannot undo deletion of application dial rules.
- Step 4** To delete the group, click **OK**, or to cancel the action, click **Cancel**. If you click **OK**, the Cisco Unified CallManager removes the application dial rule from the application dial rules list.



Note You can delete multiple dial rules from the Find and List Application Dial Rules window by checking the check boxes next to the appropriate dial rules and clicking **Delete Selected**. You can delete all the AAR groups in the window by clicking **Select All** and then clicking **Delete Selected**.

Additional Information

See the [“Related Topics” section on page 29-5](#).

Reprioritizing a Dial Rule

Perform the following procedure to reprioritize a dial rule.

Procedure

-
- Step 1** From Cisco Unified CallManager Administration, choose **Call Routing > Dial Rules > Application Dial Rules**.



Note You can also change the priority starting from the Application Dial Rules Configuration window.

- Step 2** In the Find and List Application Dial Rules window, choose a dial rule and either click the check box next to it, or click the dial rule name. The Application Dial Rule Configuration window displays.

- Step 3** Use the up and down arrows to move the dial rule up or down the list.
- Step 4** When you complete prioritizing the order, click Save.
-

Additional Information

See the [“Related Topics”](#) section on page 29-5.

Related Topics

- [Finding a Dial Rule, page 29-1](#)
- [Configuring Dial Rules, page 29-2](#)
- [Deleting a Dial Rule, page 29-4](#)
- [Reprioritizing a Dial Rule, page 29-4](#)



Directory Lookup Dial Rules Configuration

Directory lookup rules transform caller identification numbers into numbers that can be looked up in the directory. Each rule specifies which numbers to transform based on the beginning digits and length of the number. For example, you can create a directory lookup rule that automatically removes the area code and 2 prefix digits from a 10-digit telephone, which would transform 4085551212 into 51212. If Cisco Unified CallManager Attendant Console can match the number with a user in the speed-dial entries of the attendant or in the directory, the attendant console displays the name in the Call Detail window.

This section contains the following topics:

- [Finding a Directory Lookup Dial Rule, page 30-1](#)
- [Configuring Directory Lookup Dial Rules, page 30-2](#)
- [Directory Lookup Dial Rule Configuration Settings, page 30-3](#)
- [Deleting a Directory Lookup Dial Rule, page 30-4](#)
- [Related Topics, page 30-4](#)

Finding a Directory Lookup Dial Rule

Use the following procedure to locate directory lookup dial rules.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your directory lookup dial rule search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your dial search preferences until you modify your search or close the browser.

Procedure

- Step 1** Choose **Call Routing > Dial Rules > Directory Lookup Dial Rules**.

The Directory Lookup Dial Rule Find and List window displays.

- Step 2** From the first Find Directory Lookup Dial Rule drop-down list box, choose the field you want to use to search for directory lookup dial rules; for example, Name, Description, or Number begins with.



Note To find all directory lookup dial rules in the database, do not enter any search text and click **Find**. A list of directory lookup dial rules that matches your search criteria displays.

- Step 3** From the second Find Directory Lookup Dial Rule drop-down list box, choose a search pattern for your text search; for example, begins with, contains, or ends with.

- Step 4** Specify the appropriate search text, if applicable, and click **Find**.

The records that match your search criteria display. You can change the number of items that display on each window by choosing a different value from the Rows Per Page drop-down list box.



Tip To search for directory lookup rules within the search results, click the **Extend Query** check box, enter your search criteria as described in this procedure, and click **Find**.



Note You can delete multiple dial rules by checking the check boxes next to the appropriate dial rules and clicking **Delete Selected**. You can delete all the directory lookup dial rules in the window by clicking **Select All** and then clicking **Delete Selected**.

- Step 5** From the list of records, click the name of the directory lookup dial rule that you want to view.
The Directory Lookup Dial Rule Configuration window displays with the dial rule that you choose.

Additional Information

See the [“Related Topics” section on page 30-4](#).

Configuring Directory Lookup Dial Rules

Perform the following procedure to add and update a directory lookup dial rule.

Procedure

- Step 1** Choose **Call Routing > Dial Rules > Directory Lookup Dial Rules**.

The Directory Lookup Dial Rule Find and List window displays.

- Step 2** Perform one of the following tasks:

- To add a new directory lookup dial rule, click **Add New**.
- To edit an existing directory lookup dial rule, display the appropriate dial as described in the [“Finding a Directory Lookup Dial Rule” section on page 30-1](#).

The Directory Lookup Dial Rule Configuration window displays.

Step 3 Enter the appropriate settings as described in [Table 30-1](#).

Step 4 Click **Save**.

Additional Information

See the [“Related Topics”](#) section on page 30-4.

Directory Lookup Dial Rule Configuration Settings

[Table 30-1](#) describes the available settings in the Phone Configuration window. For more information about related procedures, see the [“Related Topics”](#) section on page 30-4.

Table 30-1 **Directory Lookup Dial Rule Configuration Settings**

Field	Description
Name	Enter a name for the directory lookup dial rule. The name can contain up to 20 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).
Description	Enter a description of the directory lookup dial rule in the Description field or leave blank.
Number Begins With	Enter the initial digits of the directory numbers to which you want to apply this directory lookup dial rule. For example, if you enter 972, this dial rule applies to directory numbers that include 9725551212. Valid values include numeric digits (0 through 9), plus (+), asterisk (*), and pound (#).
Number of Digits	Enter the length of the directory numbers to which you want to apply this directory lookup dial rule. For example, if you enter 7, this dial rule applies to directory numbers including 8675309.
Total Digits to be Removed	Enter the number of digits that you want Cisco CallManager to remove from directory numbers that apply to this dial rule. For example, if you enter 3, Cisco Unified CallManager removes 408 from directory numbers that include 4085256666. Valid values for this field range from 0 to 100. The total digits to be removed cannot be more than the number of digits of the directory numbers that apply to this directory lookup dial rule.
Prefix With Pattern	Enter the pattern to prepend to directory numbers that apply to this directory lookup dial rule. Valid values include digits (0 through 9), plus (+), asterisk (*), and pound (#).

Deleting a Directory Lookup Dial Rule

Perform the following procedure to delete a directory lookup dial rule.

Procedure

-
- Step 1** Choose **Call Routing > Dial Rules > Directory Lookup Dial Rules**.
The Directory Lookup Dial Rule Find and List window displays.
- Step 2** To locate a specific directory lookup dial rule, enter search criteria and click **Find**.
A list of phones that match the search criteria displays.
- Step 3** Perform one of the following actions:
- Check the check boxes next to the directory lookup dial rules that you want to delete and click **Delete Selected**.
 - Delete all the directory lookup dial rules in the window by checking the check box in the matching records title bar and clicking **Delete Selected**.
 - Display the directory lookup dial rule that you want to delete by clicking the name of the directory lookup dial rule and clicking **Delete**.
- A confirmation dialog displays.
- Step 4** To delete the directory lookup dial rules, click **OK**; to cancel the action, click **Cancel**.
-

Additional Information

See the [“Related Topics”](#) section on page 30-4.

Related Topics

- [Finding a Directory Lookup Dial Rule](#), page 30-1
- [Configuring Directory Lookup Dial Rules](#), page 30-2
- [Directory Lookup Dial Rule Configuration Settings](#), page 30-3
- [Deleting a Directory Lookup Dial Rule](#), page 30-4

Application Dial Rules

- [Dial Rules Overview](#), *Cisco Unified CallManager System Guide*
- [Application Dial Rules Configuration](#), page 29-1
- [Configuring Dial Rules](#), page 29-2

Cisco Unified CallManager Attendant Console

- [Configuration Checklist for Cisco Unified CallManager Attendant Console](#), *Cisco Unified CallManager Features and Services Guide*
- [Cisco Unified CallManager Attendant Console](#), *Cisco Unified CallManager Features and Services Guide*



SIP Dial Rules Configuration

The administrator uses SIP dial rules configuration to configure SIP phone dial plans and associate them with the following SIP phones:

- Cisco SIP IP Phone model 7911, 7941, 7961, 7970, and 7971. These phones use the 7940_7960_OTHER dial rules patterns. These phones support Key Press Markup Language (KPML), which allows the digits to be sent to Cisco Unified CallManager without requiring the user to press the Dial softkey. To increase the performance of Cisco Unified CallManager (increasing the number of calls that get processed), Cisco recommends that administrators configure SIP dial rules.
- Cisco SIP IP Phone model 7940 and 7960. These phones use the 7940_7960_OTHER dial rules patterns and do not support KPML. If the administrator does not configure a SIP dial plan for these phones, the user must press the Dial softkey or wait a specified time before digits are sent to Cisco Unified CallManager for processing. This extra step for the user delays the actual call from being processed.
- Cisco SIP IP Phone model 7905 and 7912. These phones use the 7905_7912 dial rules patterns and do not support KPML. If the administrator does not configure a SIP dial plan for these phones, the user must press the Dial softkey or wait a specified time before digits are sent to Cisco Unified CallManager for processing. This extra step for the user delays the actual call from being processed.

If the administrator does not configure a SIP phone dial plan, the user must press the Dial softkey unless the phone supports KPML. If the administrator configures SIP dial plans, those dial plans must get associated with a SIP phone, so the dial plans get sent to the device.

The following sections describe SIP dial rules configuration:

- [Finding a SIP Dial Rule, page 31-1](#)
- [Configuring SIP Dial Rules, page 31-3](#)
- [SIP Dial Rule Configuration Settings, page 31-3](#)
- [Deleting a SIP Dial Rule, page 31-6](#)
- [Resetting a SIP Dial Rule, page 31-7](#)
- [Related Topics, page 31-7](#)

Finding a SIP Dial Rule

Because you may have several SIP dial rules in your network, Cisco Unified CallManager lets you locate specific SIP dial rules based on specific criteria. Use the following procedure to locate SIP dial rules.

**Note**

During your work in a browser session, Cisco Unified CallManager Administration retains your SIP dial rule search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your SIP dial rule search preferences until you modify your search or close the browser.

Procedure

-
- Step 1** Choose **Call Routing > Dial Rules > SIP Dial Rules**.
The Find and List SIP Dial Rules window displays.
- Step 2** From the first Find SIP Dial Rules where drop-down list box, choose one of the following criteria:
- Name
 - Dial Pattern
- Step 3** From the second drop-down list box, choose one of the following criteria:
- begins with
 - contains
 - ends with
 - is exactly
 - is empty
 - is not empty
- Step 4** Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per window to display.

**Note**

To find all SIP dial rules that are registered in the database, click **Find** without entering any search text.

A list of discovered SIP dial rules displays.

- Step 5** From the list of records, click the SIP dial rule that matches your search criteria.
The window displays the SIP Dial Rule Configuration window for the SIP dial rule that you chose.
-

Additional Information

See the [“Related Topics”](#) section on page 31-7.

Configuring SIP Dial Rules

Perform the following procedure to add or update a SIP dial rule.

Procedure

-
- Step 1** In the menu bar, choose **Call Routing > Dial Rules > SIP Dial Rules**.
The Find and List SIP Dial Rules window displays.
- Step 2** Perform one of the followings tasks:
- To add a new SIP dial rule, click the **Add New** button and continue with [Step 3](#).
 - To update an existing SIP dial rule, locate the appropriate SIP dial rule as described in “[Finding a SIP Dial Rule](#)” section on [page 31-1](#) and continue with [Step 9](#).
- Step 3** From the Dial Pattern drop-down list box, choose either 7905_7912 or 7940_7960_OTHER as the SIP dial rule type.
- Step 4** Click the **Next** button.
The SIP Dial Rule Configuration redisplay with updated information.
- Step 5** Enter a name and description of the Dial Rule that you are creating by using the information as described in [Table 31-1](#). Click **Save**.
The SIP Dial Rule Configuration redisplay with updated information.
- Step 6** Enter a name for the pattern description by using the information as described in [Table 31-1](#).
- Step 7** Depending on the type of dial pattern that you want to create, click **Add Pattern** or **Add PLAR**.
- 

Note The Add PLAR button only displays for 7940_7960_OTHER dial rules.
-
- The SIP Dial Rule Configuration redisplay with updated information and an area to configure the dial pattern parameters.
- Step 8** From the Dial Parameter drop-down list box, choose the type of parameter by using the information as described in [Table 31-1](#).
- Step 9** Enter the appropriate value, parameter, and description for the dial rule as described in [Table 31-1](#).
- Step 10** After completing a configuration, click the **Save** button.
-

Additional Information

See the “[Related Topics](#)” section on [page 31-7](#).

SIP Dial Rule Configuration Settings

[Table 31-1](#) describes the available settings in the SIP Dial Rules Configuration window. For more information about related procedures, see the “[Related Topics](#)” section on [page 31-7](#).

Table 31-1 *SIP Dial Rule Configuration Settings*

Field	Description
Dial Pattern	Choose the dial pattern that is applicable to the SIP phone type that you have; for example, dial pattern 7905_7912 applies for Cisco SIP IP Phone model 7905 and 7912, and dial pattern 7940_7960_OTHER applies for Cisco SIP IP Phone model 7911, 7940, 7941, 7960, 7961, 7970, and 7971. Note Cisco Unified IP Phone model 7905, 7912, 7940, and 7960 do not support KPML.
SIP Dial Rule Information	
Name	Enter a name for the SIP dial rule; for example, Long Distance. Enter up to 50 alphanumeric characters including spaces and special characters.
Description	Enter a brief description of the dial rule.
Pattern Information	
Pattern Description	Enter a name for the pattern description; for example, Emergency.
Delete Pattern	Check this check box to delete the dial pattern; then, click the Delete Selected button.
Dial Parameter	From this drop-down list box, choose the type of parameter for this pattern from the following choices: • Pattern—Use this parameter for 7905_7912 and 7940_7960_OTHER dial rules. See the “Pattern Formats” section on page 31-5 for specific pattern formats. • Button—This parameter specifies the dial pattern to which line button applies. If the user is initiating a call on line button 1, only the dial pattern that is specified for Button 1 applies. If this optional parameter is not configured, the dial pattern applies to all lines. It only applies to the Cisco SIP IP Phone model 7940, 7941, 7960, 7961, 7970, and 7971. The administrator must enter a button number as the value. The button number corresponds to the order of the buttons on the side of the screen that is on the phone, from top to bottom, with 1 being on top. The Cisco SIP IP Phone models 7940 and 7941 have two line buttons, the models 7960 and 7961 have six line buttons, and the models 970 and 7971 have eight line buttons. • Timeout—This parameter specifies the time, in seconds, before the system times out and dials the number as entered by the user. To have the number dial immediately, specify 0. Use this parameter only for 7940_7960_OTHER dial rules. • User—This parameter represents the tag that automatically gets added to the dialed number. Valid values include IP and Phone for this tag that is not case sensitive. Use this parameter only for 7940_7960_OTHER dial rules.
Value	For the dial parameters that this table describes, enter the value for that field here; for example, enter 1 for Button 1 of PLAR.
Delete Parameter	Check this check box to delete the dial pattern; then, click the Delete Selected button.

Table 31-1 *SIP Dial Rule Configuration Settings (continued)*

Field	Description
Edit Parameter	Click this button to update an existing parameter.
Add New Parameter	Click this button to add a new parameter to the pattern.
Delete Selected	Click this button to delete a parameter or a pattern.
Pattern Addition	
Pattern Description	Enter a name for a new pattern; for example, Longdistance; then, click the Add Pattern or Add PLAR button.
Add Pattern	Click this button to add the new pattern to the Pattern Information pane.
Add PLAR	Click this button to add the new PLAR pattern to the Pattern Information pane.

Pattern Formats

See the following formats for the 7905_7912 and 7940_7960_OTHER patterns.

Value for 7905_7912 Pattern

- Period (.) matches any digit.
- Hyphen (-) means more digits can be entered. If this character is needed, it must appear at the end of an individual rule. For example, 1408t5- is legal, but 1408t5-3... is illegal.
- Pound sign (#) acts as the terminating key, and termination can be applied only after matching hits >#. So >* means that the terminating character specifies the asterisk (*); that is, the terminating key must follow the greater-than sign (>).
- Characters “tn” set the timeout to *n* seconds.



Note *n* equals 0-9, and a-z, which ranges from 0 to 26.

- Characters “rn” repeat the last pattern *n* times.



Note The characters “>#” and “tn” specify modifiers, not patterns. *n* equals 0-9 and a-z, which ranges from 0 to 26. Use the repeat modifier to specify more rules in less space.

- Modifier “S” causes rule-matching to cease (that is, if a rule matches and the modifier “S” is seen, all other rules after that matching rule do not get used for matching).

Value for 7940_7960_OTHER Pattern

- Period (.) matches any character.
- Asterisk (*) matches one or more characters. The * gets processed as a wildcard character. You can override this by preceding the * with a backward slash (\) escape sequence, which results in the sequence *. The phone automatically strips the \, so it does not appear in the outgoing dial string. When * is received as a dial digit, it gets matched by the wildcard characters * and period (.).

- Comma (,) causes the phone to generate a secondary dial tone.

Example: 7.... will match any 4-digit DN that starts with 7. 8,..... will match 8, play secondary dial tone, then match any 5-digit DN.

SIP Dial Plan Rules Examples

Table 31-2 provides some example SIP dial plan rules for the 7905_7912 dial rules.

Table 31-2 SIP Dial Plan Rule Examples

Pattern String	Effect
.t7>#.....t4-	You must enter at least one digit. After that, the send occurs after 7 seconds. The terminating # character can also be applied after the first digit is entered. After 7 digits are entered, the timeout changes to 4 seconds. The * character means that more digits can be entered, as long as timeout or # does not terminate the string.
911	Send immediately.
1t7>#.....t1-	You must enter at least one digit. After that, the send occurs after 7 seconds. The terminating character # can also be applied after the first digit is entered. After 10 digits are entered, the timeout changes to 1 second. The * character means that more digits can be entered, as long as timeout or # does not terminate the string.
0t4>#.t7-"	After a 0, if no other digit is entered, the send occurs after 4 seconds. If another digit is entered, send occurs after 7 seconds. Again, # acts as the terminating digit.

Deleting a SIP Dial Rule

Perform the following procedure to delete a SIP dial rule.

Procedure

- Step 1** From Cisco Unified CallManager Administration, choose **Call Routing > Dial Rules > SIP Dial Rules**.
- Step 2** Locate the SIP dial rule that you want to delete. See the [“Finding a SIP Dial Rule”](#) section on page 31-1.
- Step 3** Check the check box next to the SIP dial rule that you want to delete and click **Delete Selected**.
A dialog box displays to warn you that you cannot undo deletion of SIP dial rules.
- Step 4** To delete the SIP dial rule, click **OK** or, to cancel the action, click **Cancel**. If you click **OK**, Cisco Unified CallManager removes the SIP dial rule from the SIP dial rules list.



Note

You can delete multiple dial rules from the Find and List SIP Dial Rules window by checking the check boxes next to the appropriate dial rules and clicking **Delete Selected**. You can delete all the SIP dial rules in the window by clicking **Select All** and then clicking **Delete Selected**.

Additional Information

See the [“Related Topics”](#) section on page 31-7.

Resetting a SIP Dial Rule

Perform the following procedure to reset or restart the SIP phone when the SIP dial rule gets updated, so the phone gets updated with the new SIP dial rule.

Procedure

-
Step 1	From Cisco Unified CallManager Administration, choose Call Routing > Dial Rules > SIP Dial Rules .
Step 2	Locate the SIP dial rule that you want to reset. See the “Finding a SIP Dial Rule” section on page 31-1.
Step 3	Click on the SIP dial rule that you want to reset. The SIP Dial Rule Configuration window displays.
Step 4	Click Reset . The Device Reset dialog displays.
Step 5	Click one of the following choices: • Restart—Restarts the chosen devices without shutting them down (reregisters the phones with Cisco Unified CallManager). • Reset—Shuts down, then restarts, the device. • Close—Closes the Reset Device dialog without performing any action.
-

Additional Information

See the [“Related Topics”](#) section on page 31-7.

Related Topics

- [Finding a SIP Dial Rule](#), page 31-1
- [Configuring SIP Dial Rules](#), page 31-3
- [SIP Dial Rule Configuration Settings](#), page 31-3
- [SIP Dial Plan Rules Examples](#), page 31-6
- [Deleting a SIP Dial Rule](#), page 31-6
- [Resetting a SIP Dial Rule](#), page 31-7
- [Dial Rules Overview](#), *Cisco Unified CallManager System Guide*



Route Filter Configuration

Route filters, along with route patterns/hunt pilots, use dialed-digit strings to determine how a call is handled. Route filters only apply when you configure a pattern that contains the at (@) wildcard. When the route pattern/hunt pilot contains the @ wildcard, Cisco Unified CallManager routes calls according to the numbering plan that is specified in the Numbering Plan drop-down list box. The route filter window that Cisco Unified CallManager displays varies according to the numbering plan that you select.

Route filters allow you to determine which route patterns/hunt pilots your users can dial; for example, whether your users can manually choose a long-distance carrier (by dialing 101 plus a carrier access code).

Refer to [“Understanding Route Plans”](#) in the *Cisco Unified CallManager System Guide* for more information.



Tip

Always add and define the route filter first and then add the route filter to the route pattern/hunt pilot.

Use the following topics to add, update, copy, or delete a route filter:

- [Finding a Route Filter, page 32-1](#)
- [Configuring a Route Filter, page 32-3](#)
- [Route Filter Configuration Settings, page 32-4](#)
- [Adding Route Filter Clauses, page 32-4](#)
- [Removing Route Filter Clauses, page 32-5](#)
- [Deleting a Route Filter, page 32-5](#)
- [Route Filter Tag Descriptions, page 32-6](#)

Finding a Route Filter

Because you might have several route filters in your network, Cisco Unified CallManager lets you locate specific route filters on the basis of specific criteria. Use the following procedure to locate route filters.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your route filter search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your route filter search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Call Routing > Route Filter**.

The Find and List Route Filters window displays.

Step 2 From the drop-down list box, choose one of the following criteria:

- begins with
- contains
- is exactly
- ends with
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Note To find all route filters that are registered in the database, click **Find** without entering any search text.

A list of discovered route filters displays by

- Name
- Numbering Plan
- Clause



Note You can delete multiple route filters from the Find and List Route Filters window by checking the check boxes next to the appropriate route filters and clicking **Delete Selected**. You can choose all the route filters in the window by clicking **Select All** and clicking **Delete Selected**.

Step 4 From the list of records, click the route filter that matches your search criteria.

The window displays the route filter that you choose.

Additional Information

See the [“Related Topics” section on page 32-9](#).

Configuring a Route Filter

The following procedure describes how to configure a route filter.

Procedure

-
- Step 1** From Cisco Unified CallManager Administration, choose **Call Routing > Route Filter**.
- Step 2** Perform one of the following tasks:
- To copy an existing route filter, locate the appropriate route filter as described in the [“Finding a Route Filter” section on page 32-1](#), click the **Copy** button next to the route filter that you want to copy, and continue with [Step 3](#).
 - To add a new route filter, click the **Add New** button and continue with [Step 3](#).
 - To update an existing route filter, locate the appropriate route filter as described in the [“Finding a Route Filter” section on page 32-1](#), and continue with [Step 3](#).
- Step 3** In the Route Filter Configuration window that displays, enter the appropriate settings as described in [Table 32-1](#).
- Step 4** Click **Next**.
- Step 5** Choose the route filter tags and operators and enter data, where appropriate, to create a clause for this route filter.
- 

Note For help with entering data for route filter tags and operators, see the [“Route Filter Tag Descriptions” section on page 32-6](#).
- Step 6** Click **Save** to add the route filter.
- Step 7** If you are updating a route filter, click **Reset Devices**. Resetting the devices that are associated with the route filter causes calls on affected gateways to drop.
-

Additional Information

See the [“Related Topics” section on page 32-9](#).

Route Filter Configuration Settings

Table 32-1 describes the route filter configuration settings.

Table 32-1 *Route Filter Configuration Settings*

Field	Description
Numbering Plan	From the drop-down list, choose a dial plan; for example, North American Numbering Plan.
Route Filter Name	Enter a name in the Route Filter Name field. The name can contain up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure each route filter name is unique to the route plan. Note Use concise and descriptive names for your route filters. The CompanynameLocationCalltype format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a route filter. For example, CiscoDallasMetro identifies a route filter for tollfree, inter-local access and transport area (LATA) calls from the Cisco office in Dallas.

Additional Information

See the [“Related Topics”](#) section on page 32-9.

Adding Route Filter Clauses

Adding route filter clauses allows you to expand upon an existing route filter by incorporating additional operators and entries for existing tags by using a logical OR. You can add route filter clauses either when initially adding a new route filter or when updating an existing route filter. This procedure describes adding a route filter clause to an existing route filter.

Procedure

- Step 1** From Cisco Unified CallManager Administration, choose **Call Routing > Route Filter**.
- Step 2** Locate the route filter to which you want to add route filter clauses. See the [“Finding a Route Filter”](#) section on page 32-1.
- Step 3** Click **Add Clause** to display a new Route Filter Clause Configuration data entry window. All the operator fields for this new clause display NOT-SELECTED.
- Step 4** Choose the route filter tags and operators and enter data, where appropriate, to create an additional clause for this route filter.



Note For help with entering data for route filter tags and operators for the North American Numbering Plan, see the [“Route Filter Tag Descriptions”](#) section on page 32-6.

- Step 5** To add the clause, click **Save and Close**.
- The new clause displays below the existing clauses in the window. (Scroll down, if necessary, to view the new information.)
- Step 6** Click **Save** to add the new route filter clauses to the route filter.
-

Additional Information

See the [“Related Topics”](#) section on page 32-9.

Removing Route Filter Clauses

You can remove route filter clauses either when setting up a new route filter or when updating an existing route filter. This procedure describes removing a route filter clause from an existing route filter.

Procedure

-
- Step 1** From Cisco Unified CallManager Administration, choose **Call Routing > Route Filter**.
- Step 2** Locate the route filter from which you want to remove route filter clauses.
- Step 3** Scroll down to the top of the clause that you want to remove and click **Remove Clause**.
- A dialog box appears that warns you that you cannot undo the removal of this route filter clause.

**Caution**

Each **Remove Clause** button applies to the clause immediately below the button. Check carefully to ensure that you are removing the correct clause before initiating this action. If you accidentally remove a clause, you cannot retrieve it, and you must rebuild it.

- Step 4** To remove the clause, click **OK** or to cancel the action, click **Cancel**. If you click **OK**, Cisco Unified CallManager removes the clause from the route filter.
-

Additional Information

See the [“Related Topics”](#) section on page 32-9.

Deleting a Route Filter

The following procedure describes how to delete a route filter.

Before You Begin

You cannot delete a route filter that route patterns/hunt pilots, translation patterns, or other items use. To find out which route patterns/hunt pilots, translation patterns, or other items are using the route filter, in the Route Filter Configuration window, choose **Dependency Records** from the Related Links drop-down list box and click **Go**. If the dependency records are not enabled for the system, the Dependency Records Summary window displays a message. For more information about dependency

records, see the [“Accessing Dependency Records” section on page A-2](#). If you try to delete a route filter that is in use, Cisco Unified CallManager displays an error message. Before deleting a route filter that is currently in use, you must perform either or both of the following tasks:

- Assign a different route filter to any route patterns/hunt pilots, translation patterns, or other items that are using the route filter that you want to delete. See the [“Configuring a Route Pattern” section on page 35-3](#) and the [“Configuring a Translation Pattern” section on page 46-3](#).
- Delete the route patterns/hunt pilots, translation patterns, or other items that are using the route filter that you want to delete. See the [“Deleting a Route Pattern” section on page 35-10](#) and the [“Deleting a Translation Pattern” section on page 46-9](#).

Procedure

- Step 1** From Cisco Unified CallManager Administration, choose **Call Routing > Route Filter**.
- Step 2** Locate the route filter that you want to delete. See the [“Finding a Route Filter” section on page 32-1](#).
- Step 3** Check the check box of the route filter that you want to delete and click **Delete Selected**.
A message displays that states that you cannot undo this action.



Caution

Check carefully to ensure that you are deleting the correct route filter before initiating this action. You cannot retrieve deleted route filters. If a route filter is accidentally deleted, you must rebuild it.

- Step 4** To delete the route filter, click **OK** or to cancel the deletion, click **Cancel**.



Tip

You can also delete a route filter by locating and displaying the route filter that you want to delete and clicking **Delete**.

Additional Information

See the [“Related Topics” section on page 32-9](#).

Route Filter Tag Descriptions

The tag serves as the core component of a route filter. A tag applies a name to a subset of the dialed-digit string. For example, the NANP number 972-555-1234 comprises LOCAL-AREA-CODE (972), OFFICE-CODE (555), and SUBSCRIBER (1234) route filter tags.

Route filter tags require operators and can require additional values to decide which calls are filtered.

The values for route filter tag fields can contain the wildcard characters X, *, #, [,], -, ^, and the numbers 0 through 9. (See [Table 17-3](#) in the [“Special Characters and Settings”](#) section of the *Cisco Unified CallManager System Guide* for definitions of wildcard characters.) The descriptions in [Table 32-2](#) use the notations [2-9] and XXXX to represent actual digits. In this notation, [2-9] represents any single digit in the range 2 through 9, and X represents any single digit in the range 0 through 9. Therefore, the description “The three-digit area code in the form [2-9]XX” means that you can enter the actual digits 200 through 999, or all wildcards, or any mixture of actual digits and wildcards that results in a pattern with that range.

Route filter tags vary depending on the numbering plan that you choose from the Numbering Plan drop-down list box on the Route Filter Configuration window. [Table 32-2](#) describes the route filter tags for the North American Numbering Plan.

Table 32-2 **Route Filter Tags**

Tag	Description
AREA-CODE	This three-digit area code in the form [2-9]XX identifies the area code for long-distance calls.
COUNTRY CODE	These one-, two-, or three-digit codes specify the destination country for international calls.
END-OF-DIALING	This single character identifies the end of the dialed-digit string. The # character serves as the end-of-dialing signal for international numbers that are dialed within the NANP.
INTERNATIONAL-ACCESS	This two-digit access code specifies international dialing. Calls that originate in the U.S. use 01 for this code.
INTERNATIONAL-DIRECT-DIAL	This one-digit code identifies a direct-dialed international call. Calls that originate in the U.S. use 1 for this code.
INTERNATIONAL-OPERATOR	This one-digit code identifies an operator-assisted international call. This code specifies 0 for calls that originate in the U.S.
LOCAL-AREA-CODE	This three-digit local area code in the form [2-9]XX identifies the local area code for 10-digit local calls.
LOCAL-DIRECT-DIAL	This one-digit code identifies a direct-dialed local call. NANP calls use 1 for this code.
LOCAL-OPERATOR	This one-digit code identifies an operator-assisted local call. NANP calls use 0 for this code.
LONG-DISTANCE-DIRECT-DIAL	This one-digit code identifies a direct-dialed, long-distance call. NANP calls use 1 for this code.
LONG-DISTANCE-OPERATOR	These one- or two-digit codes identify an operator-assisted, long-distance call within the NANP. Operator-assisted calls use 0 for this code, and operator access uses 00.
NATIONAL-NUMBER	This tag specifies the nation-specific part of the digit string for an international call.
OFFICE-CODE	This tag designates the first three digits of a seven-digit directory number in the form [2-9]XX.
SATELLITE-SERVICE	This one-digit code provides access to satellite connections for international calls.
SERVICE	This three-digit code designates services such as 911 for emergency, 611 for repair, and 411 for information.
SUBSCRIBER	This tag specifies the last four digits of a seven-digit directory number in the form XXXX.

Table 32-2 *Route Filter Tags (continued)*

Tag	Description
TRANSIT-NETWORK	This four-digit value identifies a long-distance carrier. Do not include the leading 101 carrier access code prefix in the TRANSIT-NETWORK value. Refer to TRANSIT-NETWORK-ESCAPE for more information.
TRANSIT-NETWORK-ESCAPE	This three-digit value precedes the long-distance carrier identifier. The value for this field specifies 101. Do not include the four-digit carrier identification code in the TRANSIT-NETWORK-ESCAPE value. Refer to TRANSIT-NETWORK for more information.

Route filter tag operators determine whether a call is filtered based on the existence, and sometimes the contents, of the dialed-digit string that is associated with that tag. The operators EXISTS and DOES-NOT-EXIST simply check for the existence of that part of the dialed-digit string. The operator == matches the actual dialed digits with the specified value or pattern. [Table 32-3](#) describes the operators that can be used with route filter tags.

Table 32-3 *Route Filter Operators*

Operator	Description
NOT-SELECTED	Specifies do not filter calls based on the dialed-digit string that is associated with this tag. Note The presence or absence of the tag with which the operator is associated does not prevent Cisco Unified CallManager from routing the call.
EXISTS	Specifies filter calls when the dialed-digit string that is associated with this tag is found. Note Cisco Unified CallManager routes or blocks the call only if the dialed-digit string contains a sequence of digits that are associated with the tag.
DOES-NOT-EXIST	Specifies filter calls when the dialed-digit string that is associated with this tag is not found. Note Cisco Unified CallManager routes or blocks the call only if the dialed-digit string does not contain a sequence of digits that are associated with the tag.
==	Specifies filter calls when the dialed-digit string that is associated with this tag matches the specified value. Note Cisco Unified CallManager routes or blocks the call only if the dialed-digit string contains a sequence of digits that are associated with the tag and within the numbering range that is specified in the attached field.

**Caution**

Do not enter route filter tag values for tags that are using the operators EXISTS, DOES-NOT-EXIST, or NOT-SELECTED.

Examples

Example 1: A route filter that uses AREA-CODE and the operator DOES-NOT-EXIST selects all dialed-digit strings that do not include an area code.

Example 2: A route filter that uses AREA-CODE, the operator ==, and the entry 515 selects all dialed-digit strings that include the 515 area code.

Example 3: A route filter that uses AREA-CODE, the operator ==, and the entry 5[2-9]X selects all dialed-digit strings that include area codes in the range of 520 through 599.

Example 4: A route filter that uses TRANSIT-NETWORK, the operator ==, and the entry 0288 selects all dialed-digit strings with the carrier access code 1010288.

Additional Information

See the [“Related Topics” section on page 32-9](#).

Related Topics

- [Finding a Route Filter, page 32-1](#)
- [Configuring a Route Filter, page 32-3](#)
- [Route Filter Configuration Settings, page 32-4](#)
- [Adding Route Filter Clauses, page 32-4](#)
- [Removing Route Filter Clauses, page 32-5](#)
- [Deleting a Route Filter, page 32-5](#)
- [Route Filter Tag Descriptions, page 32-6](#)
- [Understanding Route Plans, Cisco Unified CallManager System Guide](#)



Route Group Configuration

A route group allows you to designate the order in which gateways and trunks are selected. It allows you to prioritize a list of gateways and ports for outgoing trunk selection.

For example, if you use two long-distance carriers, you could add a route group, so long-distance calls to the less expensive carrier are given priority. Calls only route to the more expensive carrier if the first trunk is unavailable.

Use the following topics to add or delete a route group or to add devices to or to remove devices from a route group:

- [Finding a Route Group, page 33-1](#)
- [Configuring a Route Group, page 33-2](#)
- [Route Group Configuration Settings, page 33-3](#)
- [Adding Devices to a Route Group, page 33-5](#)
- [Removing Devices from a Route Group, page 33-6](#)
- [Deleting a Route Group, page 33-6](#)

Finding a Route Group

Because you might have several route groups in your network, Cisco Unified CallManager lets you locate specific route groups based on specific criteria. Use the following procedure to locate route groups.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your route group search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your route group search preferences until you modify your search or close the browser.

Procedure

- Step 1** Choose **Call Routing > Route/Hunt > Route Group**.
The Find and List Route Groups window displays.

Step 2 From the drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Note To find all route groups that are registered in the database, click **Find** without entering any search text.

A list of discovered route groups displays by route group name.



Tip To search for route groups within the search results, click the **Search Within Results** check box and enter your search criteria as described in this step.



Note You can delete multiple route groups from the Find and List Route Groups window by checking the check boxes next to the appropriate route groups and clicking **Delete Selected**. You can delete all the route groups in the window by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records, click the route group that matches your search criteria.
The window displays the route group that you choose.

Additional Information

See the [“Related Topics” section on page 33-7](#).

Configuring a Route Group

The following procedure describes how to configure a route group.

Procedure

Step 1 Choose **Call Routing > Route/Hunt > Route Group**.

Step 2 Perform one of the followings tasks:

- To copy an existing route group, locate the appropriate route group as described in the [“Finding a Route Group” section on page 33-1](#), click the **Copy** button next to the route group that you want to copy, and continue with [Step 3](#).

- To add a new route group, click the **Add New** button, and continue with [Step 3](#).
- To update an existing route group, locate the appropriate route group as described in the “[Finding a Route Group](#)” section on page 33-1, and continue with [Step 3](#).

Step 3 In the Route Group Configuration window that displays, enter a name in the Route Group Name field. The name can contain up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each route group name is unique to the route plan.

**Timesaver**

Use concise and descriptive names for your route groups. The CompanynameLocationGroup format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a route group. For example, CiscoDallasAA1 identifies a Cisco Access Analog route group for the Cisco office in Dallas.

Step 4 Choose the appropriate settings as described in [Table 33-1](#).

**Note**

You must choose at least one device for a new route group before adding the new route group.

Step 5 To add or update this route group, click **Save**.

Additional Information

See the “[Related Topics](#)” section on page 33-7.

Route Group Configuration Settings

[Table 33-1](#) describes the route group configuration settings.

Table 33-1 *Route Group Configuration Settings*

Field	Description
Route Group Information	
Route Group Name	Enter a name for this route group. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each route group name is unique to the route plan.

Table 33-1 **Route Group Configuration Settings (continued)**

Field	Description
Distribution Algorithm	Choose a distribution algorithm from the options in the drop-down list box: • Top Down—If you choose this distribution algorithm, Cisco Unified CallManager distributes a call to idle or available members starting from the first idle or available member of a route group to the last idle or available member. • Circular—If you choose this distribution algorithm, Cisco Unified CallManager distributes a call to idle or available members starting from the $(n+1)^{\text{th}}$ member of a route group, where the n^{th} member is the member to which Cisco Unified CallManager most recently extended a call. If the n^{th} member is the last member of a route group, Cisco Unified CallManager distributes a call starting from the top of the route group. The default value specifies <i>Circular</i>.
Route Group Member Information	
Find Devices to Add to Route Group	
Device Name contains	Enter the character(s) that are found in the device name that you are seeking and click the Find button. Device names that match the character(s) that you entered display in the Available Devices box. Note To find all available devices, leave the text box blank and click the Find button.
Available Devices (select device, then select port below)	Choose a device in the Available Devices list box and add it to the Selected Devices list box by clicking Add to Route Group. If the route group contains a gateway that uses the QSIG protocol, only gateways that use the QSIG protocol display in the list. If the route group contains a gateway that uses the non-QSIG protocol, gateways that use the controlled intercluster trunks, which are QSIG protocol do not display in the list. If you included the route group in a route list that contains QSIG gateways, the H.323 gateways do not display in the list.
Port(s)	If this device supports individually configurable ports, choose the port. (Devices that allow you to choose individual ports include Cisco Access Analog and Cisco MGCP Analog gateways and T1 CAS.) Otherwise, choose the default value (<i>All</i> or <i>None Available</i>, depending upon the device that is chosen). For a device that has no ports available (<i>None Available</i>), the device may be already added to the Route Group, or cannot be added to the route group.

Table 33-1 **Route Group Configuration Settings (continued)**

Field	Description
Current Route Group Members	
Selected Devices (ordered by highest priority)	To change the priority of a device, choose a device name in the Selected Devices list box. Move the device up or down in the list by clicking the arrows on the right side of the list box. To reverse the priority order of the devices in the Selected Devices list box, click Reverse Order of Selected Devices. For more information about the order of devices in a route group, see “Route Plan Overview” in the <i>Cisco Unified CallManager System Guide</i>.
Removed Devices (to be removed from Route Group when you click Update)	Choose a device in the Selected Devices list box and add it to the Removed Devices list box by clicking the down arrow button between the two list boxes. Note You must leave at least one device in a route group.

Additional Information

See the [“Related Topics”](#) section on page 33-7.

Adding Devices to a Route Group

You can add devices to a new route group or to an existing route group. You can add gateways to multiple route groups. Once you add a gateway to any route group, the gateway does not display in the Route Pattern configuration window. The following procedure describes adding a device to an existing route group.

Before You Begin

You must define one or more gateway and trunk devices before performing this procedure. A device can reside in only one route group.

Procedure

-
- Step 1** Choose **Call Routing > Route/Hunt > Route Group**.
- Step 2** Locate the route group to which you want to add a device. See the [“Finding a Route Group”](#) section on page 33-1.
- Step 3** In the Available Devices list box, choose a device to add and click **Add to Route Group** to move it to the Selected Devices list box. Repeat this step for each device that you want to add to this route group.
- Step 4** In the Selected Devices list box, choose the order in which the new device or devices are to be accessed in this route group. To change the order, click on a device and use the Up and Down arrows to the right of the list box to change the order of devices.
- Step 5** To add the new device(s) and to update the device order for this route group, click **Save**.
-

Additional Information

See the [“Related Topics”](#) section on page 33-7.

Removing Devices from a Route Group

You can remove devices from a new route group or from an existing route group. The following procedure describes removing a device from an existing route group.

Procedure

-
- Step 1** Choose **Call Routing > Route/Hunt > Route Group**.
- Step 2** Locate the route group from which you want to remove a device. See the [“Finding a Route Group”](#) section on page 33-1.
- Step 3** In the Selected Devices list box, choose a device to be removed and click the Down arrow below the Selected Devices list box to move the device to the Removed Devices list box. Repeat this step for each device that you want to remove from this route group.



Note You must leave at least one device in a route group.

- Step 4** To remove the devices, click **Save**.
-

Additional Information

See the [“Related Topics”](#) section on page 33-7.

Deleting a Route Group

The following procedure describes how to delete a route group.

Before You Begin

You cannot delete a route group that a route/hunt list references. To find out which route lists are using the route group, in the Route Group Configuration window, choose **Dependency Records** from the Related Links drop-down list box and click **Go**. If the dependency records are not enabled for the system, the Dependency Records Summary window displays a message. For more information about dependency records, refer to the [“Accessing Dependency Records”](#) section on page A-2. If you try to delete a route group that is in use, Cisco Unified CallManager displays an error message. Before deleting a route group that is currently in use, you must perform the following task:

- Remove the route group from all route lists to which it belongs before deleting the route group. See the [“Removing Route Groups from a Route List”](#) section on page 34-5.

**Tip**

To delete route groups and route patterns, first delete the route pattern; second, delete the route_list; and finally, delete the route group.

Procedure

-
- Step 1** Choose **Call Routing > Route/Hunt > Route Group**.
- Step 2** Locate the route group that you want to delete. See the [“Finding a Route Group” section on page 33-1](#).
- Step 3** Check the check box next to the route group that you want to delete and click **Delete Selected**.
A dialog box displays to warn you that you cannot undo deletion of route groups.
- Step 4** To delete the route group, click **OK** or to cancel the action, click **Cancel**. If you click **OK**, the Cisco Unified CallManager removes the route group from the route group list.



Note You can delete multiple route groups from the Find and List Route Groups window by checking the check boxes next to the appropriate route groups and clicking **Delete Selected**. You can delete all the route groups in the window by click **Select All** and then clicking **Delete Selected**.

Additional Information

See the [“Related Topics” section on page 33-7](#).

Related Topics

Route Groups

- [Finding a Route Group, page 33-1](#)
- [Configuring a Route Group, page 33-2](#)
- [Route Group Configuration Settings, page 33-3](#)
- [Adding Devices to a Route Group, page 33-5](#)
- [Removing Devices from a Route Group, page 33-6](#)
- [Deleting a Route Group, page 33-6](#)
- [Understanding Route Plans, Cisco Unified CallManager System Guide](#)

Route Lists

- [Adding a Route List, page 34-3](#)
- [Adding Route Groups to a Route List, page 34-4](#)



Route List Configuration

A route list associates a set of route groups in a specified priority order. A route list then associates with one or more route patterns and determines the order in which those route groups are accessed. The order controls the progress of the search for available devices for outgoing calls.

A route list can contain only route groups.

Each route list should have at least one route group. Each route group includes at least one device, such as a gateway, that is available. Based on device type, Cisco Unified CallManager can choose some, or all, ports as resources in each route group. Some devices, such as digital access, only allow you to choose all ports.

A Route Group can be added to any number of Route Lists.

Use the following topics to add or remove route lists or to add, remove, or change the order of route groups in a route list:

- [Finding Route Lists, page 34-1](#)
- [Adding a Route List, page 34-3](#)
- [Adding Route Groups to a Route List, page 34-4](#)
- [Removing Route Groups from a Route List, page 34-5](#)
- [Changing the Order of Route Groups in a Route List, page 34-6](#)
- [Deleting a Route List, page 34-6](#)

Finding Route Lists

Because you might have several route lists in your network, Cisco Unified CallManager lets you use specific criteria to locate specific route lists. To locate route lists, use the following procedure.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your route list search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your route list search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Call Routing > Route/Hunt > Route List**.

The Find and List Route Lists window displays. Use the two drop-down list boxes to search for a route list.

Step 2 From the first Find Route Lists where drop-down list box, choose one of the following criteria:

- Route List Name
- Description
- Pattern/Pilot Number



Note The criterion that you choose in this drop-down list box specifies how the list of route lists that your search generates will be sorted. For example, if you choose Description, the Description column will display as the left column of the results list.

From the second Find Route Lists where drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Note To find all route lists that are registered in the database, click **Find** without entering any search text.

A list of discovered route lists displays by

- Route list name
- Description
- Status
- Enabled



Tip To search for route lists within the search results, click the **Search Within Results** check box and enter your search criteria as described in this step.



Note You can delete multiple route lists from the Find and List Route Lists window by checking the check boxes next to the appropriate route lists and clicking **Delete Selected**. You can delete all route lists in the window by checking the check box in the matching records title bar and clicking **Delete Selected**.

- Step 4** Click the route list from the list of records that matches your search criteria. The window displays the route list that you choose.
-

Additional Information

See the [“Related Topics” section on page 34-7](#).

Adding a Route List

The following procedure describes how to add a route list.

Procedure

- Step 1** Choose **Call Routing > Route/Hunt > Route List**.
- Step 2** Click **Add New**.
- Step 3** In the Route List Name field, enter a name. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each route list name is unique to the route plan.



Timesaver

Use concise and descriptive names for your route lists. The CompanynameLocationCalltype format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a route list. For example, CiscoDallasMetro identifies a route list for toll-free, inter-local access transport area (LATA) calls from the Cisco office in Dallas.

Cisco Unified CallManager automatically inserts a description in the Description field. You can, however, edit this field.

- Step 4** From the drop-down list box, choose a Cisco Unified CallManager group.



Note The Route List registers with the first Cisco Unified CallManager in the group which is its primary Cisco Unified CallManager.



Note If you choose a Cisco Unified CallManager group that has only one Cisco Unified CallManager configured, you receive the following warning:

WARNING! The selected Cisco Unified CallManager Group has only one Cisco Unified CallManager configured. For the control process to have redundancy protection, please select a Cisco Unified CallManager Group with more than one Cisco Unified CallManager.

Step 5 To add this route list, click **Save**.



Note A popup message reminds you that you must add at least one route group to this route list for it to accept calls.

The Route List Configuration window displays the newly added route list.

Step 6 By default, the system checks the Enable this Route List check box for the new route list.

If you want to disable this route list, uncheck this check box. A popup window explains that calls in progress are not affected, but this route list will not accept additional calls.

Step 7 Add at least one route group to the new route list.

To add a route group to this list, click **Add Route Group** and perform [Step 4](#) through [Step 8](#) of the “Adding Route Groups to a Route List” section on [page 34-4](#).



Note For called party and calling party transformation information, you can click the name of a route group that belongs to this route list. The route group names display in the Route List Details list box at the bottom of the Route List Configuration window. This action displays the Route List Detail Configuration window for the route group that you choose.

Additional Information

See the “[Related Topics](#)” section on [page 34-7](#).

Adding Route Groups to a Route List

You can add route groups to a new route list or to an existing route list. Route groups can exist in one or more route lists. The following procedure describes adding a route group to an existing route list.



Note You cannot add route groups that contain MGCP gateways that use the QSIG protocol (a QSIG route group) and route groups that contain gateways that use the H.323 protocol (H.323 route group) to the same route list. For more information, refer to the “[Route Groups and Route Lists](#)” section in the *Cisco Unified CallManager System Guide*.

Before You Begin

Before performing this procedure, you must build one or more route groups and add a route list.

Procedure

Step 1 Choose **Call Routing > Route/Hunt > Route List**.

Step 2 Locate the route list to which you want to add route group. See the “[Finding Route Lists](#)” section on [page 34-1](#).

Step 3 To add a route group, click **Add Route Group**.

The Route List Detail Configuration window displays.

Step 4 From the Route Group drop-down list box, choose a route group to add to the route list.



Note If the route list contains a QSIG route group, H.323 route groups do not display in the drop-down list box. If the route group contains a H.323 route group, QSIG route groups do not display in the drop-down list box.

Step 5 If you need to manipulate the calling party number on calls that are routed through this route group, set up the calling party transformations in the appropriate fields.



Note For more information on calling party transformations, see the [“Calling and Called Party Transformations”](#) in the *Cisco Unified CallManager System Guide*.

Step 6 If you need to manipulate the dialed digits on calls that are routed through this route group, set up the called party transformations in the appropriate fields.



Note For more information on called party transformations, see the [“Called Party Number Transformations Settings”](#) in the *Cisco Unified CallManager System Guide*.

Step 7 To add the route group, click **Save**.

The route group details information appears in the Route List Details list on the left side of the window.

Step 8 To add more route groups to this list, click **Add Route Group** and repeat [Step 3](#) through [Step 7](#).

Step 9 When you finishing adding route groups to the route list, click **Save**.

Step 10 Click **Reset** for changes to take effect. When the popup windows display, click **OK**.

Additional Information

See the [“Related Topics”](#) section on page 34-7.

Removing Route Groups from a Route List

You can remove route groups from a new route list or from an existing route list. The following procedure describes removing a route group from an existing route list.

Procedure

Step 1 Choose **Call Routing > Route/Hunt > Route List** in the menu bar.

Step 2 Locate the route list from which you want to remove a route group. See the [“Finding Route Lists”](#) section on page 34-1.

Step 3 From the Selected Groups list, choose a route group name.



Note To select multiple route groups from the list, press the **Shift** key and click the desired route groups.

- Step 4** Click the down arrow below the Selected Groups list box to move the selected route group to the Removed Groups list.
 - Step 5** To remove the route group, click **Save**. If you click **OK**, when the window refreshes, the route group no longer appears in the route list.
 - Step 6** Click **Reset** for the changes to take effect. Click **OK** in response to the popup windows.
-

Additional Information

See the [“Related Topics” section on page 34-7](#).

Changing the Order of Route Groups in a Route List

Cisco Unified CallManager accesses route groups in the order in which they appear in the route list. The following procedure allows you to change the access order of route groups.

Procedure

- Step 1** Choose **Call Routing > Route/Hunt > Route List**.
- Step 2** Locate the route list in which you want to change the order of a route group. See the [“Finding Route Lists” section on page 34-1](#).
- Step 3** From the Selected Groups list, choose a route group.
- Step 4** To move the route group up or down in the list, select a route group, then click the up or down arrows on the right side of the list box.
- Step 5** Click **Save**.



Note For called party and calling party transformation information, click the route group icon or route group name in the Route List Details list at left. This action takes you to the Route List Detail Configuration window for the corresponding route group.

- Step 6** Click **Reset** for the changes to take effect. Click **OK** in response to the popup windows.
-

Additional Information

See the [“Related Topics” section on page 34-7](#).

Deleting a Route List

The Cisco Unified CallManager associates a route list with a route pattern. You cannot delete a route list if it is associated with a route pattern. To find out which route patterns are using the route list, click the **Dependency Records** link from the Route List Configuration window. If dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#).

**Tip**

To delete route groups and route patterns, first delete the route pattern; second, delete the route list; and finally, delete the route group.

The following procedure describes how to delete a route list.

Procedure

-
- Step 1** Choose **Call Routing > Route/Hunt > Route List**.
- Step 2** Locate the route list that you want to delete. See the [“Finding Route Lists” section on page 34-1](#).
- Step 3** Click **Delete Selected**.
- A dialog box displays to warn you that you cannot undo the deletion of a route list.
- Step 4** To delete the route list, click **OK** or to cancel the action, click **Cancel**.

**Caution**

You cannot delete a route list if it is associated with one or more route patterns.

Additional Information

See the [“Related Topics” section on page 34-7](#).

Related Topics

- [Finding Route Lists, page 34-1](#)
- [Adding a Route List, page 34-3](#)
- [Adding Route Groups to a Route List, page 34-4](#)
- [Removing Route Groups from a Route List, page 34-5](#)
- [Changing the Order of Route Groups in a Route List, page 34-6](#)
- [Deleting a Route List, page 34-6](#)
- [Understanding Route Plans, Cisco Unified CallManager System Guide](#)
- [Understanding How Presence Works with Route Lists, Cisco Unified CallManager Features and Services Guide](#)



Route Pattern Configuration

A route pattern comprises a string of digits (an address) and a set of associated digit manipulations that route calls to a route list or a gateway. Route patterns provide flexibility in network design. They work in conjunction with route filters and route lists to direct calls to specific devices and to include, exclude, or modify specific digit patterns.

Refer to [“Understanding Route Plans”](#) in *Cisco Unified CallManager System Guide* for more detailed route pattern information.

Use the following topics to find, add, update, copy, or delete a route pattern:

- [Finding a Route Pattern, page 35-1](#)
- [Configuring a Route Pattern, page 35-3](#)
- [Route Pattern Configuration Settings, page 35-4](#)
- [Deleting a Route Pattern, page 35-10](#)

Finding a Route Pattern

Because you might have several route patterns in your network, Cisco Unified CallManager lets you use specific criteria to locate specific route patterns. To locate route patterns, use the following procedure.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your route pattern search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your route pattern search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Call Routing > Route/Hunt > Route Pattern**.

The Find and List Route Patterns window displays. Use the two drop-down selection boxes to search for a route pattern.

- Step 2** From the first Find Route Patterns where drop-down selection box, choose Pattern, Description, or Partition.



Note The criterion that you choose in this drop-down list box specifies how the list of route patterns that your search generates will be sorted. For example, if you choose Description, the Description column will display as the left column of the results list.

- Step 3** From the second Find Route Patterns where drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is not empty
- is empty

- Step 4** Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Note To find all route patterns that are registered in the database, click **Find** without entering any search text.

A list of discovered route patterns displays by

- Route pattern icon
- Route pattern
- Partition
- Description
- Route Filter
- Gateway/Route List



Tip To search for route patterns within the search results, click the **Search Within Results** check box and enter your search criteria as described in this step.



Note You can delete multiple route patterns from the Find and List Route Patterns window by checking the check boxes next to the appropriate route patterns and clicking **Delete Selected**. You can delete all route patterns in the window by checking the check box in the matching records title bar and clicking **Delete Selected**.

- Step 5** Click the route pattern from the list of records that matches your search criteria.
The window displays the route pattern that you choose.

Additional Information

See the [“Related Topics”](#) section on page 35-11.

Configuring a Route Pattern

This section describes how to configure a route pattern.

Before You Begin

Ensure that the following items are configured in Cisco Unified CallManager:

- Gateway
- Route list
- Partition (unless you are using <None>)
- Route filter (unless you are using <None>)

**Timesaver**

Assigning 8XXX to a gateway routes all directory numbers 8000 to 8999 out the gateway. Similarly, 82XX routes directory numbers 8200 to 8299. See the [“Special Characters and Settings”](#) section in the *Cisco Unified CallManager System Guide* for more information about wildcards.

Procedure

Step 1 Choose **Call Routing > Route/Hunt > Route Pattern**.

Step 2 Perform one of the following tasks:

- To copy an existing route pattern, locate the appropriate route pattern as described in the [“Finding a Route Pattern”](#) section on page 35-1, click the **Copy** button next to the route pattern that you want to copy, and continue with [Step 3](#).
- To add a new route pattern, click the **Add New** button, and continue with [Step 3](#).
- To update an existing route pattern, locate the appropriate route pattern as described in the [“Finding a Route Pattern”](#) section on page 35-1, and continue with [Step 3](#).

**Note**

If you change the gateway or route list, you must click **Update** prior to choosing the **Edit** link. Otherwise, you get linked to the previous gateway or route list.

Step 3 In the Route Pattern Configuration window that displays, enter the appropriate settings as described in [Table 35-1](#).



Note The (**Edit**) link next to the Gateway or Route List field takes you to the Gateway Configuration or Route List Configuration window for reference, depending on whether the Gateway or Route List field contains a gateway or a route list. The Gateway Configuration window displays devices that are associated with the specified gateway. The Route List Configuration window displays the route groups that are associated with the specified route list.

Step 4 Click **Save**.

Additional Information

See the “[Related Topics](#)” section on [page 35-11](#).

Route Pattern Configuration Settings

[Table 35-1](#) describes the available fields in the Route Pattern Configuration window.

Table 35-1 *Route Pattern Configuration Settings*

Field	Description
Pattern Definition	
Route Pattern	Enter the route pattern, including numbers and wildcards (do not use spaces); for example, for NANP, enter 9.@ for typical local access, or 8XXX for a typical private network numbering plan. The uppercase characters A, B, C, and D are valid characters. Note Ensure that the directory route pattern, which uses the chosen partition, route filter, and numbering plan combination, is unique. Check the route pattern, translation pattern, directory number, call park number, call pickup number, message waiting on/off, or meet me number if you receive an error that indicates duplicate entries. You can also check the route plan report. See the “Wildcards and Special Characters in Route Patterns and Hunt Pilots” section in the <i>Cisco Unified CallManager System Guide</i> for more information about wildcards.

Table 35-1 **Route Pattern Configuration Settings (continued)**

Field	Description
Route Partition	If you want to use a partition to restrict access to the route pattern, choose the desired partition from the drop-down list box. If you do not want to restrict access to the route pattern, choose <i><None></i> for the partition. See the “Partition Configuration” section on page 42-1 for more information on how to use partitions. You can configure the number of partitions that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more than 250 partitions are specified by using the Max List Box Items enterprise parameter, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Partition window. Enter a partial partition name in the List items where Name contains field. Click the desired partition name in the list of partitions that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters. Note Make sure that the combination of route pattern, route filter, and partition is unique within the Cisco Unified CallManager cluster.
Description	Enter a description of the route pattern.
Numbering Plan	Choose a numbering plan.
Route Filter	If your route pattern includes the @ wildcard, you may choose a route filter. The optional act of choosing a route filter restricts certain number patterns. The route filters that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box. If more than 250 route filters exist, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Route Filters window. Enter a partial route filter name in the List items where Name contains field. Click the desired route filter name in the list of route filters that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.

Table 35-1 Route Pattern Configuration Settings (continued)

Field	Description
MLPP Precedence	Choose an MLPP precedence setting for this route pattern from the drop-down list box: • Executive Override—Highest precedence setting for MLPP calls. • Flash Override—Second highest precedence setting for MLPP calls. • Flash—Third highest precedence setting for MLPP calls. • Immediate—Fourth highest precedence setting for MLPP calls. • Priority—Fifth highest precedence setting for MLPP calls. • Routine—Lowest precedence setting for MLPP calls. • Default—Does not override the incoming precedence level but rather lets it pass unchanged. Note Refer to the “Precedence” section in the “Multilevel Precedence and Preemption” chapter of the <i>Cisco Unified CallManager Features and Services Guide</i> for more information.
Gateway/Route List	Choose the gateway or route list for which you are adding a route pattern. Note If the gateway is included in a Route Group, this drop-down list box does not display the gateway. When a gateway is chosen in the drop-down list box, Cisco Unified CallManager uses all the ports in the gateway to route/block this route pattern. This action does not apply for MGCP gateways.
Route Option	The Route Option designation indicates whether you want this route pattern to be used for routing calls (such as 9.@ or 8[2-9]XX) or for blocking calls. Choose the Route this pattern or Block this pattern radio button. If you choose the Block this pattern radio button, you must choose the reason for which you want this route pattern to block calls. Choose a value from the drop-down list box: • No Error • Unallocated Number • Call Rejected • Number Changed • Invalid Number Format • Precedence Level Exceeded
Call Classification	Call Classification indicates whether the call that is routed through this route pattern is considered either off (OffNet) or on (OnNet) the local network. The default value specifies OffNet. When adding a route pattern, if you uncheck the Provide Outside Dial Tone check box, you set Call Classification as OnNet.
Allow Device Override	This check box is unchecked by default. When checked, the system uses the Call Classification setting that is configured on the associated gateway or trunk to consider the outgoing call as OffNet or OnNet.
Provide Outside Dial Tone	Check this check box to provide outside dial tone. To route the call in the network, leave the check box unchecked.

Table 35-1 **Route Pattern Configuration Settings (continued)**

Field	Description
Allow Overlap Sending	With overlap sending enabled, when Cisco Unified CallManager passes a call to the PSTN, it relies on overlap sending in the PSTN to determine how many digits to collect and where to route the call. Check this check box for each route pattern that you consider to be assigned to a gateway or route list that routes the calls to a PSTN that supports overlap sending. The CMC and FAC features do not support overlap sending because the Cisco Unified CallManager cannot determine when to prompt the user for the code. If you check the Require Forced Authorization Code or the Require Client Matter Code check box, the Allow Overlap Sending check box becomes disabled.
Urgent Priority	If the dial plan contains overlapping route patterns, Cisco Unified CallManager would not route the call until the interdigit timer expires (even if it is possible to dial a sequence of digits to choose a current match). Check this check box to interrupt interdigit timing when Cisco Unified CallManager must route a call immediately.
Require Forced Authorization Code	If you want to use forced authorization codes with this route pattern, check this check box. The FAC feature does not support overlap sending because the Cisco Unified CallManager cannot determine when to prompt the user for the code. If you check the Allow Overlap Sending check box, the Require Forced Authorization Code check box becomes disabled.
Authorization Level	Enter the authorization level for the route pattern. The number that you specify in this field determines the minimum authorization level that is needed to successfully route a call through this route pattern. Tip To activate the authorization code, you must check the Require Forced Authorization Code. If you do not check the check box, a message displays when you insert the route pattern that indicates that the authorization code cannot be activated. To activate the code, click Cancel, check the Require Forced Authorization Code check box, and click Insert. To activate the code at a later time, click OK.
Require Client Matter Code	If you want to use client matter codes with this route pattern, check this check box. The CMC feature does not support overlap sending because the Cisco Unified CallManager cannot determine when to prompt the user for the code. If you check the Allow Overlap Sending check box, the Require Client Matter Code check box become disabled.
Calling Party Transformations	
Use Calling Party's External Phone Number Mask	Check the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls. You may also configure an External Phone Number Mask on all phone devices. Note The calling party transformation settings that are assigned to the route groups in a route list override any calling party transformation settings that are assigned to a route pattern that is associated with that route list.

Table 35-1 **Route Pattern Configuration Settings (continued)**

Field	Description
Calling Party Transform Mask	Enter a transformation mask value. Valid entries for the NANP include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); the uppercase characters A, B, C, and D; and blank. If this field is blank and the preceding field is not checked, no calling party transformation takes place. See the “ Calling Party Number Transformations Settings ” section in the <i>Cisco Unified CallManager System Guide</i> for more information.
Prefix Digits (Outgoing Calls)	Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries for the NANP include the digits 0 through 9; the wildcard characters asterisk (*) and octothorpe (#); the uppercase characters A, B, C, and D; and blank. Note The appended prefix digit does not affect which directory numbers route to the assigned device.
Calling Line ID Presentation	Cisco Unified CallManager uses calling line ID presentation (CLIP/CLIR) as a supplementary service to allow or restrict the originating caller’s phone number on a call-by-call basis. Choose whether you want the Cisco Unified CallManager to allow or restrict the display of the calling party’s phone number on the called party’s phone display for this route pattern. Choose <i>Default</i> if you do not want to change calling line ID presentation. Choose <i>Allowed</i> if you want Cisco Unified CallManager to allow the display of the calling number. Choose <i>Restricted</i> if you want Cisco Unified CallManager to block the display of the calling number. For more information about this field, see Table 17-6 in the “ Calling Party Number Transformations Settings ” section in the <i>Cisco Unified CallManager System Guide</i> .
Calling Name Presentation	Cisco Unified CallManager uses calling name presentation (CNIP/CNIR) as a supplementary service to allow or restrict the originating caller’s name on a call-by-call basis. Choose whether you want the Cisco Unified CallManager to allow or restrict the display of the calling party’s name on the called party’s phone display for this route pattern. Choose <i>Default</i> if you do not want to change calling name presentation. Choose <i>Allowed</i> if you want Cisco Unified CallManager to display the calling name information. Choose <i>Restricted</i> if you want Cisco Unified CallManager to block the display of the calling name information. For more information about this field, see Table 17-6 in the “ Calling Party Number Transformations Settings ” section in the <i>Cisco Unified CallManager System Guide</i> .

Table 35-1 **Route Pattern Configuration Settings (continued)**

Field	Description
Connected Party Transformations	
Connected Line ID Presentation	Cisco Unified CallManager uses connected line ID presentation (COLP/COLR) as a supplementary service to allow or restrict the called party's phone number on a call-by-call basis. Choose whether you want Cisco Unified CallManager to allow or restrict the display of the connected party's phone number on the calling party's phone display for this route pattern. Choose <i>Default</i> if you do not want to change the connected line ID presentation. Choose <i>Allowed</i> if you want to display the connected party's phone number. Choose <i>Restricted</i> if you want Cisco Unified CallManager to block the display of the connected party's phone number. For more information about this field, see Table 17-9 in the “Connected Party Presentation and Restriction Settings” section in the <i>Cisco Unified CallManager System Guide</i>.
Connected Name Presentation	Cisco Unified CallManager uses connected name presentation (CONP/CONR) as a supplementary service to allow or restrict the called party's name on a call-by-call basis. Choose whether you want Cisco Unified CallManager to allow or restrict the display of the connected party's name on the calling party's phone display for this route pattern. Choose <i>Default</i> if you do not want to change the connected name presentation. Choose <i>Allowed</i> if you want to display the connected party's name. Choose <i>Restricted</i> if you want Cisco Unified CallManager to block the display of the connected party's name. For more information about this field, see Table 17-9 in the “Connected Party Presentation and Restriction Settings” section in the <i>Cisco Unified CallManager System Guide</i>.
Called Party Transformations	
Discard Digits	From the Discard Digits drop-down list box, choose the discard digits instructions that you want to associate with this route pattern. The discard digits that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box. See the “Discard Digits Instructions” section in the <i>Cisco Unified CallManager System Guide</i> for more information on discard instructions for the North American Numbering Plan. Note The called party transformation settings that are assigned to the route groups in a route list override any called party transformation settings that are assigned to a route pattern that is associated with that route list.
Called Party Transform Mask	Enter a transformation mask value. Valid entries for the NANP include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); the uppercase characters A, B, C, and D; and blank. If the field is blank, no transformation takes place. Cisco Unified CallManager sends the dialed digits exactly as dialed.

Table 35-1 Route Pattern Configuration Settings (continued)

Field	Description
Prefix Digits (Outgoing Calls)	Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries for the NANP include the digits 0 through 9; the wildcard characters asterisk (*) and octothorpe (#); the uppercase characters A, B, C, and D; and blank. Note The appended prefix digit does not affect which directory numbers route to the assigned device.
ISDN Network-Specific Facilities Information Element	
Network Service Protocol	From the Network Service Protocol drop-down list box, choose the PRI protocol that matches the protocol of the terminating gateway.
Carrier Identification Code	Enter the appropriate carrier identification code (0, 3, or 4 digits) in the Carrier Identification Code field. Carrier identification codes allow customers to reach the services of interexchange carriers. The following list shows examples of commonly used carrier identification codes: • ATT—0288 • Sprint—0333 • WorldCom/MCI—0222 For a complete list of NANP carrier identification codes, go to http://www.nanpa.com/ .
Network Service	Choose the appropriate network service. The values vary depending on the network service protocol that you choose from the Network Service Protocol field.
Service Parameter Name	This field displays the service parameter name that is associated with the chosen network service. If no service parameter exists for the network service, the field displays <Not Exist>.
Service Parameter Value	Enter the appropriate service parameter value. Valid entries include the digits 0 through 9. If a service parameter does not exist for the network service, Cisco Unified CallManager Administration disables this field.

Additional Information

See the “[Related Topics](#)” section on page 35-11.

Deleting a Route Pattern

This section describes how to delete a route pattern.

Procedure

-
- Step 1** Choose **Call Routing > Route/Hunt > Route Pattern**.
- Step 2** Locate the route pattern that you want to delete. See the “[Finding a Route Pattern](#)” section on page 35-1.
- Step 3** Check the check box of the route pattern that you want to delete and click **Delete Selected**.
- A message that displays states that you cannot undo this action.

Step 4 To delete the route pattern, click **OK** or to cancel the deletion, click **Cancel**.

**Tip**

You can also delete a route pattern by locating and displaying the route pattern that you want to delete and clicking **Delete**.

Additional Information

See the [“Related Topics”](#) section on page 35-11.

Related Topics

- [Finding a Route Pattern, page 35-1](#)
- [Configuring a Route Pattern, page 35-3](#)
- [Route Pattern Configuration Settings, page 35-4](#)
- [Deleting a Route Pattern, page 35-10](#)
- [Wildcards and Special Characters in Route Patterns and Hunt Pilots, Cisco Unified CallManager System Guide](#)
- [Configuring a Route Filter, page 32-3](#)
- [Understanding Route Plans, Cisco Unified CallManager System Guide](#)



Line Group Configuration

A line group allows you to designate the order in which directory numbers are chosen. Cisco Unified CallManager distributes a call to idle or available members of a line group based on a call distribution algorithm and on the Ring No Answer Reversion (RNAR) Timeout setting.

Use the following topics to add or delete a line group or to add directory numbers to or to remove directory numbers from a line group:

- [Finding a Line Group, page 36-1](#)
- [Configuring a Line Group, page 36-2](#)
- [Line Group Configuration Settings, page 36-3](#)
- [Adding Members to a Line Group, page 36-8](#)
- [Removing Members from a Line Group, page 36-9](#)
- [Deleting a Line Group, page 36-9](#)

Finding a Line Group

Because you may have several line groups in your network, Cisco Unified CallManager lets you locate specific line groups based on specific criteria. Use the following procedure to locate line groups.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your line group search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your line group search preferences until you modify your search or close the browser.

Procedure

- Step 1** Choose **Call Routing > Route/Hunt > Line Group**.
- The Find and List Line Groups window displays.
- Step 2** From the drop-down list box, choose one of the following criteria:
- begins with
 - contains
 - is exactly

- ends with
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Note To find all line groups registered in the database, click **Find** without entering any search text.

A list of discovered line groups displays by line group name.



Tip To search for line groups within the search results, click the **Search Within Results** check box and enter your search criteria as described in this step.



Note You can delete multiple line groups from the Find and List Line Groups window by checking the check boxes next to the appropriate line groups and clicking **Delete Selected**. You can delete all of the line groups in the window by clicking **Select All** and clicking **Delete Selected**.

Step 4 From the list of records, click the line group that matches your search criteria.
The window displays the line group that you choose.

Additional Information

See the [“Related Topics” section on page 36-10](#).

Configuring a Line Group

The following procedure describes how to configure a line group.

Before You Begin

You must define one or more directory numbers before performing this procedure.

Procedure

Step 1 Choose **Call Routing > Route/Hunt > Line Group**.

Step 2 Perform one of the following tasks:

- To copy an existing line group, locate the appropriate line group as described in the [“Finding a Line Group” section on page 36-1](#), click the **Copy** button next to the line group that you want to copy, and continue with [Step 3](#).
- To add a new line group, click the **Add New** button, and continue with [Step 3](#).
- To update an existing line group, locate the appropriate line group as described in the [“Finding a Line Group” section on page 36-1](#), and continue with [Step 3](#).

- Step 3** In the Line Group Configuration window that displays, enter a name in the Line Group Name field. The name can contain up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each line group name is unique to the route plan.

**Timesaver**

Use concise and descriptive names for your line groups. The CompanynameLocationGroup format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a line group. For example, CiscoDallasAA1 identifies a Cisco Access Analog line group for the Cisco office in Dallas.

- Step 4** Choose the appropriate settings as described in [Table 36-1](#).
- Step 5** To add or update this line group, click **Save**.

Additional Information

See the [“Related Topics”](#) section on page 36-10.

Line Group Configuration Settings

[Table 36-1](#) describes the line group configuration settings.

Table 36-1 **Line Group Configuration Settings**

Field	Description
Line Group Information	
Line Group Name	Enter a name for this line group. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each line group name is unique to the route plan.
RNA Reversion Timeout	Enter a time, in seconds, after which Cisco Unified CallManager will distribute a call to the next available or idle member of this line group or to the next line group if the call is not answered and if the first hunt option, <i>Try next member; then, try next group in Hunt List</i> , is chosen. The RNA Reversion Timeout applies at the line-group level to all members.

Table 36-1 **Line Group Configuration Settings (continued)**

Field	Description
Distribution Algorithm	Choose a distribution algorithm, which applies at the line-group level, from the options in the drop-down list box: • Top Down—If you choose this distribution algorithm, Cisco Unified CallManager distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. • Circular—If you choose this distribution algorithm, Cisco Unified CallManager distributes a call to idle or available members starting from the $(n+1)^{\text{th}}$ member of a line group, where the n^{th} member is the member to which Cisco Unified CallManager most recently extended a call. If the n^{th} member is the last member of a line group, Cisco Unified CallManager distributes a call starting from the top of the line group. • Longest Idle Time—If you choose this distribution algorithm, Cisco Unified CallManager only distributes a call to idle members, starting from the longest idle member to the least idle member of a line group. • Broadcast—If you choose this distribution algorithm, Cisco Unified CallManager distributes a call to all idle or available members of a line group simultaneously. See the Note in the description of the Selected DN/Route Partition field for additional limitations in using the Broadcast distribution algorithm. The default value specifies <i>Longest Idle Time</i>.

Table 36-1 **Line Group Configuration Settings (continued)**

Field	Description
Hunt Options	
No Answer	For a given distribution algorithm, choose a hunt option for Cisco Unified CallManager to use if a call is distributed to a member of a line group that does not answer. This option gets applied at the member level. Choose from the options in the drop-down list box: • Try next member; then, try next group in Hunt List—If you choose this hunt option, Cisco Unified CallManager distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. If unsuccessful, Cisco Unified CallManager then tries the next line group in a hunt list. • Try next member, but do not go to next group—If you choose this hunt option, Cisco Unified CallManager distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. Cisco Unified CallManager stops trying upon reaching the last member of the current line group. • Skip remaining members, and go directly to next group—If you choose this hunt option, Cisco Unified CallManager skips the remaining members of this line group when the RNA reversion timeout value elapses for the first member. Cisco Unified CallManager then proceeds directly to the next line group in a hunt list. • Stop hunting—If you choose this hunt option, Cisco Unified CallManager stops hunting after trying to distribute a call to the first member of this line group and the member does not answer the call.

Table 36-1 **Line Group Configuration Settings (continued)**

Field	Description
Busy	For a given distribution algorithm, choose a hunt option for Cisco Unified CallManager to use if a call is distributed to a member of a line group that is busy. Choose from the options in the drop-down list box: • Try next member; then, try next group in Hunt List—If you choose this hunt option, Cisco Unified CallManager distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. If unsuccessful, Cisco Unified CallManager then tries the next line group in a hunt list. • Try next member, but do not go to next group—If you choose this hunt option, Cisco Unified CallManager distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. Cisco Unified CallManager stops trying upon reaching the last member of the current line group. • Skip remaining members, and go directly to next group—If you choose this hunt option, Cisco Unified CallManager skips the remaining members of this line group upon encountering a busy member. Cisco Unified CallManager proceeds directly to the next line group in a hunt list. • Stop hunting—If you choose this hunt option, Cisco Unified CallManager stops hunting after trying to distribute a call to the first busy member of this line group.

Table 36-1 **Line Group Configuration Settings (continued)**

Field	Description
Not Available	For a given distribution algorithm, choose a hunt option for Cisco Unified CallManager to use if a call is distributed to a member of a line group that is not available. The Not Available condition occurs when none of the phones that are associated with the DN in question are registered. Not Available also occurs when Extension Mobility is in use and the DN/user is not logged in. Choose from the options in the drop-down list box: • Try next member; then, try next group in Hunt List—If you choose this hunt option, Cisco Unified CallManager distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. If unsuccessful, Cisco Unified CallManager then tries the next line group in a hunt list. • Try next member, but do not go to next group—If you choose this hunt option, Cisco Unified CallManager distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. Cisco Unified CallManager stops trying upon reaching the last member of the current line group. • Skip remaining members, and go directly to next group—If you choose this hunt option, Cisco Unified CallManager skips the remaining members of this line group upon encountering the first unavailable member. Cisco Unified CallManager proceeds directly to the next line group in a hunt list. • Stop hunting—If you choose this hunt option, Cisco Unified CallManager stops hunting after trying to distribute a call to the first unavailable member of this line group.
Line Group Member Information	
Find Directory Numbers to Add to Line Group	
Partition	Choose a route partition for this line group from the drop-down list box. The default value specifies <i><None></i>. If you click Find, the Available DN/Route Partition list box displays all DNs that belong to the chosen partition.
Directory Number Contains	Enter the character(s) that are found in the directory number that you are seeking and click the Find button. Directory numbers that match the character(s) that you entered display in the Available DN/Route Partition box.
Available DN/Route Partition	Choose a directory number in the Available DN/Route Partition list box and add it to the Selected DN/Route Partition list box by clicking Add to Line Group .

Table 36-1 Line Group Configuration Settings (continued)

Field	Description
Current Line Group Members	
Selected DN/Route Partition	To change the priority of a directory number, choose a directory number in the Selected DN/Route Partition list box. Move the directory number up or down in the list by clicking the arrows on the right side of the list box. To reverse the priority order of the directory numbers in the Selected DN/Route Partition list box, click Reverse Order of Selected DNs/Route Partitions. For more information about the order of directory numbers in a line group, see “Route Plan Overview” in the <i>Cisco Unified CallManager System Guide</i>. Note Do not put DNs that are shared lines in a line group that uses the Broadcast distribution algorithm. Cisco Unified CallManager cannot display all DNs that are shared lines on devices where the DNs are configured as shared lines if the DNs are members of a line group that uses the Broadcast distribution algorithm.
Removed DN/Route Partition (to be removed from Line Group when you click Save)	Choose a directory number in the Selected DN/Route Partition list box and add it to the Removed DN/Route Partition list box by clicking the down arrow between the two list boxes.
Directory Numbers	
(list of DNs that currently belong to this line group)	Click on a directory number in this list to go to the Directory Number Configuration window for the specified directory number.

Additional Information

See the [“Related Topics”](#) section on page 36-10.

Adding Members to a Line Group

You can add members to a new line group or to an existing line group. The following procedure describes adding a member to an existing line group.

Before You Begin

You must define one or more directory numbers before performing this procedure.

Procedure

-
- Step 1** Choose **Call Routing > Route/Hunt > Line Group**.
- Step 2** Locate the line group to which you want to add a member. See the [“Finding a Line Group”](#) section on page 36-1.

- Step 3** If you need to locate a directory number, choose a route partition from the Partition drop-down list box, enter a search string in the Directory Number Contains field, and click **Find**. To find all directory numbers that belong to a partition, leave the Directory Number Contains field blank and click **Find**. A list of matching directory numbers displays in the Available DN/Route Partition list box.
- Step 4** In the Available DN/Route Partition list box, choose a directory number to add and click **Add to Line Group** to move it to the Selected DN/Route Partition list box. Repeat this step for each member that you want to add to this line group.
- Step 5** In the Selected DN/Route Partition list box, choose the order in which the new directory number(s) is to be accessed in this line group. To change the order, click on a directory number and use the Up and Down arrows to the right of the list box to change the order of directory numbers.
- Step 6** Click **Save** to add the new directory numbers and to update the directory number order for this line group.
-

Additional Information

See the [“Related Topics”](#) section on page 36-10.

Removing Members from a Line Group

You can remove members from a new line group or from an existing line group. The following procedure describes removing a directory number from an existing line group.

Procedure

- Step 1** Choose **Call Routing > Route/Hunt > Line Group**.
- Step 2** Locate the line group from which you want to remove a directory number. See the [“Finding a Line Group”](#) section on page 36-1.
- Step 3** In the Selected DN/Route Partition list box, choose a directory number to be deleted and click the down arrow below the list box to move the directory number to the Removed DN/Route Partition list box. Repeat this step for each member that you want to remove from this line group.
- Step 4** To remove the members, click **Save**.
-

Additional Information

See the [“Related Topics”](#) section on page 36-10.

Deleting a Line Group

The following procedure describes how to delete a line group.

Before You Begin

You cannot delete a line group that one or more route/hunt lists references. To find out which hunt lists are using the line group, in the Line Group Configuration window, choose **Dependency Records** from the Related Links drop-down list box and click **Go**. If the dependency records are not enabled for the

system, the Dependency Records Summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#). If you try to delete a line group that is in use, Cisco Unified CallManager displays an error message. Before deleting a line group that is currently in use, you must perform the following task:

- Remove the line group from all hunt lists to which it belongs before deleting the line group. See the [“Removing Route Groups from a Route List” section on page 34-5](#).

**Tip**

To delete line groups and hunt pilots; first, delete the hunt pilot; second, delete the hunt list; and finally, delete the line group.

Procedure

- Step 1** Choose **Call Routing > Route/Hunt > Line Group**.
- Step 2** Locate the line group that you want to delete. See the [“Finding a Line Group” section on page 36-1](#).
- Step 3** Check the check box next to the line group that you want to delete and click **Delete Selected**.
A dialog box displays to warn you that you cannot undo deletion of line groups.
- Step 4** To delete the line group, click **OK** or to cancel the action, click **Cancel**. If you click **OK**, the Cisco Unified CallManager removes the line group.

**Note**

You can delete multiple line groups from the Find and List Line Groups window by checking the check boxes next to the appropriate line groups and clicking **Delete Selected**. You can delete all the line groups in the window by clicking **Select All** and clicking **Delete Selected**.

Additional Information

See the [“Related Topics” section on page 36-10](#).

Related Topics

Line Groups

- [Finding a Line Group, page 36-1](#)
- [Configuring a Line Group, page 36-2](#)
- [Line Group Configuration Settings, page 36-3](#)
- [Adding Members to a Line Group, page 36-8](#)
- [Removing Members from a Line Group, page 36-9](#)
- [Deleting a Line Group, page 36-9](#)

Route Lists and Route Groups

- [Adding a Route List, page 34-3](#)
- [Adding Route Groups to a Route List, page 34-4](#)
- [Understanding Route Plans, Cisco Unified CallManager System Guide](#)



Hunt List Configuration

A Hunt List lists a set of Line groups in a specific order. A hunt list then associates with one or more hunt pilots and determines the order in which those line groups are accessed. The order controls the progress of the search for available directory numbers for incoming calls.

A hunt list comprises a collection of directory numbers as defined by line groups. After Cisco Unified CallManager determines a call that is to be routed through a defined hunt list, Cisco Unified CallManager finds the first available device on the basis of the order of the line group(s) that a hunt list defines.



Note

The Group Call Pickup feature does not work with hunt lists.

A hunt list can contain only line groups. Each hunt list should have at least one line group. Each line group includes at least one directory number. A single line group can appear in multiple hunt lists.

Use the following topics to add or remove hunt lists or to add, remove, or change the order of line groups in a hunt list:

- [Finding Hunt Lists, page 37-1](#)
- [Adding a Hunt List, page 37-3](#)
- [Adding Line Groups to a Hunt List, page 37-4](#)
- [Removing Line Groups from a Hunt List, page 37-5](#)
- [Changing the Order of Line Groups in a Hunt List, page 37-5](#)
- [Deleting a Hunt List, page 37-6](#)

Finding Hunt Lists

Because you might have several hunt lists in your network, Cisco Unified CallManager lets you use specific criteria to locate specific hunt lists. To locate hunt lists, use the following procedure.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your hunt list search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your hunt list search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Call Routing > Route/Hunt > Hunt List**.

The Find and List Hunt Lists window displays. Use the two drop-down list boxes to search for a hunt list.

Step 2 From the first Find Hunt Lists where drop-down list box, choose one of the following criteria:

- Hunt List Name
- Description
- Pattern/Pilot Number



Note The criterion that you choose in this drop-down list box specifies how the list of hunt lists that your search generates will be sorted. For example, if you choose Description, the Description column will display as the left column of the results list.

From the second Find Hunt Lists where drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Note To find all hunt lists that are registered in the database, click **Find** without entering any search text.

A list of discovered hunt lists displays by

- Hunt list name
- Description
- Status
- Enabled



Tip To search for hunt lists within the search results, click the **Search Within Results** check box and enter your search criteria as described in this step.



Note You can delete multiple hunt lists from the Find and List Hunt Lists window by checking the check boxes next to the appropriate hunt lists and clicking **Delete Selected**. You can delete all hunt lists in the window by checking the check box in the matching records title bar and clicking **Delete Selected**.

- Step 4** Click the hunt list from the list of records that matches your search criteria. The window displays the hunt list that you choose.
-

Additional Information

See the [“Related Topics”](#) section on page 37-6.

Adding a Hunt List

The following procedure describes how to add a hunt list.

Procedure

- Step 1** Choose **Call Routing > Route/Hunt > Hunt List**.
- Step 2** Click **Add New**.
- Step 3** In the Hunt List Name field, enter a name. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure each hunt list name is unique to the route plan.



Timesaver

Use concise and descriptive names for your hunt lists. The CompanynameLocationCalltype format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a hunt list. For example, CiscoDallasMetro identifies a hunt list for toll-free, inter-local access transport area (LATA) calls from the Cisco office in Dallas.

Cisco Unified CallManager automatically inserts a description in the Description field. You can, however, edit this field.

- Step 4** Choose a Cisco Unified CallManager group from the drop-down list box.



Note Hunt List registers to the first Cisco Unified CallManager in the Cisco Unified CallManager Group as primary Cisco Unified CallManager.



Note If you choose a Cisco Unified CallManager group that has only one Cisco Unified CallManager configured, you receive the following warning:

WARNING! The selected Cisco Unified CallManager Group has only one Cisco Unified CallManager configured. For the control process to have redundancy protection, please select a Cisco Unified CallManager Group with more than one Cisco Unified CallManager.

Step 5 To add this hunt list, click **Save**.



Note A popup message reminds you that you must add at least one line group to this hunt list for it to accept calls.

The Hunt List window displays the newly added hunt list.

Step 6 The system checks the Enable this Hunt List check box by default for the new hunt list.

If you want to disable this hunt list, uncheck this check box. A popup window explains that calls in progress are not affected, but this hunt list will not accept additional calls.

Step 7 Add at least one line group to the new hunt list.

To add a line group to this list, click **Add Line Group** and perform [Step 3](#) through [Step 6](#) of the “[Adding Line Groups to a Hunt List](#)” section on [page 37-4](#).

Additional Information

See the “[Related Topics](#)” section on [page 37-6](#).

Adding Line Groups to a Hunt List

You can add line groups to a new hunt list or to an existing hunt list. Line groups can exist in one or more hunt lists. The following procedure describes adding a line group to an existing hunt list.

Before You Begin

You must build one or more line groups and add a hunt list before performing this procedure.

Procedure

Step 1 Choose **Call Routing > Route/Hunt > Hunt List**.

Step 2 Locate the hunt list to which you want to add a line group. See the “[Finding Hunt Lists](#)” section on [page 37-1](#).

Step 3 To add a line group, click **Add Line Group**.

The Hunt List Detail Configuration window displays.

Step 4 From the Line Group drop-down list box, choose a line group to add to the hunt list.

Step 5 To add the line group, click **Save**.

The line group name displays in the Hunt List Details list on the left side of the window.

Step 6 To add more line groups to this list, click **Add Line Group** and repeat [Step 3](#) through [Step 5](#).

Step 7 When you finishing adding line groups to the hunt list, click **Save**.

Step 8 Click **Reset** to reset the hunt list. When the popup windows display, click **OK**.

Additional Information

See the “[Related Topics](#)” section on [page 37-6](#).

Removing Line Groups from a Hunt List

You can remove line groups from a new hunt list or from an existing hunt list. The following procedure describes removing a line group from an existing hunt list.

Procedure

-
- Step 1** Choose **Call Routing > Route/Hunt > Hunt List** in the menu bar.
- Step 2** Locate the hunt list from which you want to remove a line group. See the [“Finding Hunt Lists” section on page 37-1](#).
- Step 3** From the Selected Groups list, choose a line group name.
-
-  **Note** To choose multiple line groups from the list, press the **Shift** key and click the desired line groups.
-
- Step 4** Click the down arrow below the Selected Groups list box to move the chosen line group to the Removed Groups list.
- Step 5** To remove the line group, click **Update**. If you click **OK**, when the window refreshes, the line group no longer displays in the hunt list.
- Step 6** Click **Reset** for the changes to take effect. Click **OK** in response to the popup windows.
-

Additional Information

See the [“Related Topics” section on page 37-6](#).

Changing the Order of Line Groups in a Hunt List

Cisco Unified CallManager accesses line groups in the order in which they display in the hunt list. The following procedure allows you to change the access order of line groups.

Procedure

-
- Step 1** Choose **Call Routing > Route/Hunt > Hunt List**.
- Step 2** Locate the hunt list in which you want to change the order of a line group. See the [“Finding Hunt Lists” section on page 37-1](#).
- Step 3** From the Selected Groups list, choose a line group.
- Step 4** To move the line group up or down in the list, select a group, then click the up or down arrows on the right side of the list box.
- Step 5** Click **Save**.
- Step 6** Click **Reset** for the changes to take effect. Click **OK** in response to the popup windows.
-

Additional Information

See the [“Related Topics”](#) section on page 37-6.

Deleting a Hunt List

Cisco Unified CallManager associates hunt lists with line groups and hunt pilots; however, deletion of line groups and hunt pilots does not occur when the hunt list is deleted. To find out which hunt pilots are using the hunt list, click the **Dependency Records** link from the Hunt List Configuration window. If dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records”](#) section on page A-2.

**Tip**

To delete line groups and hunt pilots, first delete the hunt pilot; second, delete the hunt list; and finally, delete the line group.

The following procedure describes how to delete a hunt list.

Procedure

-
- Step 1** Choose **Call Routing > Route/Hunt > Hunt List**.
- Step 2** Locate the hunt list that you want to delete. See the [“Finding Hunt Lists”](#) section on page 37-1.
- Step 3** Click **Delete**.
- A dialog box displays to warn you that you cannot undo the deletion of a hunt list.
- Step 4** To delete the hunt list, click **OK** or to cancel the action, click **Cancel**.

**Caution**

You cannot delete a hunt list if it is associated with one or more hunt pilots.

Additional Information

See the [“Related Topics”](#) section on page 37-6.

Related Topics

- [Finding Hunt Lists, page 37-1](#)
- [Adding a Hunt List, page 37-3](#)
- [Adding Line Groups to a Hunt List, page 37-4](#)
- [Removing Line Groups from a Hunt List, page 37-5](#)
- [Changing the Order of Line Groups in a Hunt List, page 37-5](#)
- [Deleting a Hunt List, page 37-6](#)
- [Understanding Route Plans, Cisco Unified CallManager System Guide](#)



Hunt Pilot Configuration

A hunt pilot comprises a string of digits (an address) and a set of associated digit manipulations that route calls to a hunt list. Hunt pilots provide flexibility in network design. They work in conjunction with route filters and hunt lists to direct calls to specific devices and to include, exclude, or modify specific digit patterns.

Refer to [“Understanding Route Plans”](#) in *Cisco Unified CallManager System Guide* for more detailed hunt pilot information.

Use the following topics to add, configure, or delete a hunt pilot:

- [Finding a Hunt Pilot, page 38-1](#)
- [Configuring a Hunt Pilot, page 38-3](#)
- [Deleting a Hunt Pilot, page 38-4](#)
- [Hunt Pilot Configuration Settings, page 38-4](#)

Finding a Hunt Pilot

Because you may have several hunt pilots in your network, Cisco Unified CallManager lets you use specific criteria to locate specific hunt pilots. To locate hunt pilots, use the following procedure.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your hunt pilot search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your hunt pilot search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Call Routing > Route/Hunt > Hunt Pilot**.

The Find and List Hunt Pilots window displays. Use the two drop-down selection boxes to search for a hunt pilot.

Step 2 From the first Find Hunt Pilots where drop-down selection box, choose Pattern, Description, or Partition.



Note The criterion that you choose in this drop-down list box specifies how the list of hunt pilots that your search generates will be sorted. For example, if you choose Description, the Description column will display as the left column of the results list.

Step 3 From the second Find Hunt Pilots where drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is not empty
- is empty

Step 4 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Note To find all hunt pilots that are registered in the database, click **Find** without entering any search text.

A list of discovered hunt pilots displays by

- Hunt pilot icon
- Hunt pilot
- Partition
- Description
- Route Filter
- Hunt List



Tip To search for hunt pilots within the search results, click the **Search Within Results** check box and enter your search criteria as described in this step.



Note You can delete multiple hunt pilots from the Find and List Hunt Pilots window by checking the check boxes next to the appropriate hunt pilots and clicking **Delete Selected**. You can delete all hunt pilots in the window by checking the check box in the matching records title bar and clicking **Delete Selected**.

Step 5 Click the hunt pilot from the list of records that matches your search criteria.
The window displays the hunt pilot that you choose.

Additional Information

See the [“Related Topics”](#) section on page 38-11.

Configuring a Hunt Pilot

This section describes how to configure a hunt pilot.

Before You Begin

Ensure that the following items are configured in Cisco Unified CallManager:

- Hunt list
- Partition (unless you are using <None>)
- Route filter (unless you are using <None>)



Timesaver

Assigning 8XXX to a hunt pilot causes hunting through all directory numbers 8000 to 8999. Similarly, 82XX hunts through directory numbers 8200 to 8299. See the [“Special Characters and Settings”](#) section in the *Cisco Unified CallManager System Guide* for more information about wildcards.

Procedure

Step 1 Choose **Call Routing > Route/Hunt > Hunt Pilot**.

The Find and List Hunt Pilots window displays.

Step 2 Perform one of the following tasks:

- To copy an existing hunt pilot, locate the appropriate hunt pilot as described in [“Finding a Hunt Pilot”](#) section on page 38-1. Click the **Copy** button next to the hunt pilot that you want to copy. The window displays the copy of the hunt pilot. Change the value in the Hunt Pilot field, and continue with [Step 3](#).
- To add a new hunt pilot, click the **Add New** button, and continue with [Step 3](#).
- To update an existing hunt pilot, locate the appropriate hunt pilot as described in [“Finding a Hunt Pilot”](#) section on page 38-1, and continue with [Step 3](#).

Step 3 Enter the appropriate settings as described in [Table 38-1](#).

Step 4 Click **Save**.



Note

After you choose a hunt list from the Hunt List drop-down list box, you can use the (**Edit**) link that displays next to the Hunt List field to take you to the Hunt List Configuration window for the hunt list that you choose. Use the Hunt List Configuration window to see the line group(s) that are included in that hunt list.

Additional Information

See the [“Related Topics”](#) section on page 38-11.

Deleting a Hunt Pilot

This section describes how to delete a hunt pilot.

Procedure

-
- Step 1** Choose **Call Routing > Route/Hunt > Hunt Pilot**.
- Step 2** Locate the hunt pilot that you want to delete. See the [“Finding a Hunt Pilot”](#) section on page 38-1.
- Step 3** Check the check box of the hunt pilot that you want to delete and click **Delete Selected**.
A message that displays states that you cannot undo this action.
- Step 4** To delete the hunt pilot, click **OK** or to cancel the deletion, click **Cancel**.



Tip You can also delete a hunt pilot by locating and displaying the hunt pilot that you want to delete and clicking **Delete**.

Additional Information

See the [“Related Topics”](#) section on page 38-11.

Hunt Pilot Configuration Settings

[Table 38-1](#) describes the available fields in the Hunt Pilot Configuration window.

Table 38-1 *Hunt Pilot Configuration Settings*

Field	Description
Pattern Definition	
Hunt Pilot	Enter the hunt pilot, including numbers and wildcards (do not use spaces); for example, for NANP, enter 9.@ for typical local access, or 8XXX for a typical private network numbering plan. The uppercase characters A, B, C, and D are valid characters. Note Ensure that the directory hunt pilot, which uses the chosen partition, route filter, and numbering plan combination, is unique. Check the hunt pilot, translation pattern, directory number, call park number, call pickup number, message waiting on/off, or meet me number if you receive an error that indicates duplicate entries. You can also check the route plan report. See the “Wildcards and Special Characters in Route Patterns and Hunt Pilots” section in the <i>Cisco Unified CallManager System Guide</i> for more information about wildcards.

Table 38-1 **Hunt Pilot Configuration Settings (continued)**

Field	Description
Partition	If you want to use a partition to restrict access to the hunt pilot, choose the desired partition from the drop-down list box. If you do not want to restrict access to the hunt pilot, choose <None> for the partition. See the “Partition Configuration” section on page 42-1 for more information on how to use partitions. You can configure the number of partitions that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more than 250 partitions are specified by using the Max List Box Items enterprise parameter, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Partition window. Enter a partial partition name in the List items where Name contains field. Click the desired partition name in the list of partitions that display in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose Unified CMAAdmin Parameters. Note Make sure that the combination of hunt pilot, route filter, and partition is unique within the Cisco Unified CallManager cluster.
Description	Enter a description of the hunt pilot.
Numbering Plan	Choose a numbering plan.
Route Filter	If your hunt pilot includes the @ wildcard, you may choose a route filter. The optional act of choosing a route filter restricts certain number patterns. The route filters that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box. If more than 250 route filters exist, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Route Filters window. Enter a partial route filter name in the List items where Name contains field. Click the desired route filter name in the list of route filters that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose Unified CMAAdmin Parameters.

Table 38-1 **Hunt Pilot Configuration Settings (continued)**

Field	Description
MLPP Precedence	Choose an MLPP precedence setting for this hunt pilot from the drop-down list box: • Executive Override—Highest precedence setting for MLPP calls. • Flash Override—Second highest precedence setting for MLPP calls. • Flash—Third highest precedence setting for MLPP calls. • Immediate—Fourth highest precedence setting for MLPP calls. • Priority—Fifth highest precedence setting for MLPP calls. • Routine—Lowest precedence setting for MLPP calls. • Default—Does not override the incoming precedence level but rather lets it pass unchanged. Note Refer to the “Precedence” section in the “Multilevel Precedence and Preemption” chapter of the <i>Cisco Unified CallManager Features and Services Guide</i> for more information.
Hunt List	Choose the hunt list for which you are adding a hunt pilot from the drop-down list box.
Route Option	The Route Option designation indicates whether you want this hunt pilot to be used for routing calls (such as 9.@ or 8[2-9]XX) or for blocking calls. Choose the Route this pattern or Block this pattern radio button. If you choose the Block this pattern radio button, you must choose the reason for which you want this hunt pilot to block calls. Choose a value from the drop-down list box: • No Error • Unallocated Number • Call Rejected • Number Changed • Invalid Number Format • Precedence Level Exceeded
Provide Outside Dial Tone	Outside Dial Tone indicates that Cisco Unified CallManager routes the calls off the local network. Check this check box for each hunt pilot that routes the call off the local network and provides outside dial tone to the calling device. To route the call in the network, leave the check box unchecked.
Urgent Priority	If the dial plan contains overlapping hunt lists, Cisco Unified CallManager would not route the call until the interdigit timer expires (even if it is possible to dial a sequence of digits to choose a current match). Check this check box to interrupt interdigit timing when Cisco Unified CallManager must route a call immediately.

Table 38-1 **Hunt Pilot Configuration Settings (continued)**

Field	Description
Hunt Forward Settings	
Forward Hunt No Answer	When the call distributed through the hunt list is not answered in a specific period of time, this field specifies the destination to forward the call. Choose from the following options: • Use Personal Preferences—Use this check box to enable the Call Forward No Coverage (CFNC) settings for the original called number that forwarded the call to this hunt pilot. The CFNC setting specifies a call forwarding reason that you administer in the Directory Number Configuration window. Calls get diverted based on the value in the directory number's Coverage/Destination field when a call to the directory number first diverts to coverage, and coverage either exhausts or times out, and the associated hunt pilot for coverage specifies Use Personal Preferences for its final forwarding. Note When this check box is checked, Cisco Unified CallManager ignores the settings in the Destination box and Calling Search Space. • Destination—This setting indicates the directory number to which calls are forwarded. • Calling Search Space—This setting applies to all devices that are using this directory number.
Forward Hunt Busy	When the call distributed through the hunt list is busy in a specific period of time, this field specifies the destination to forward the call. Choose from the following options: • Use Personal Preferences—Use this check box to enable the Call Forward No Coverage (CFNC) settings for the original called number that forwarded the call to this hunt pilot. The CFNC setting specifies a call forwarding reason that you administer in the Directory Number Configuration window. Calls get diverted based on the value in the directory number's Coverage/Destination field when a call to the directory number first diverts to coverage, and coverage either exhausts or times out, and the associated hunt pilot for coverage specifies Use Personal Preferences for its final forwarding. Note When this check box is checked, Cisco Unified CallManager ignores the settings in the Destination box and Calling Search Space. • Destination—This setting indicates the directory number to which calls are forwarded. • Calling Search Space—This setting applies to all devices that are using this directory number.

Table 38-1 **Hunt Pilot Configuration Settings (continued)**

Field	Description
Maximum Hunt Timer	Enter a value (in seconds) that specifies the maximum time for hunting. Valid values specify 1 to 3600. The default value specifies 1800 seconds (30 minutes). This timer cancels if either a hunt member answers the call or if the hunt list gets exhausted before the timer expires. If you do not specify a value for this timer, hunting continues until a hunt member answers or hunting exhausts. If neither event takes place, hunting continues for 30 minutes, after which the call gets taken for final treatment. Note If hunting exceeds the number of hops that the Forward Maximum Hop Count service parameter specifies, hunting expires before the 30-minute maximum hunt timer value and the caller receives a reorder tone.
Calling Party Transformations	
Use Calling Party's External Phone Number Mask	Check the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls. You may also configure an External Phone Number Mask on all phone devices. Note The calling party transformation settings that are assigned to the line groups in a hunt list override any calling party transformation settings that are assigned to a hunt pilot that is associated with that hunt list.
Calling Party Transform Mask	Enter a transformation mask value. Valid entries for the NANP include the digits 0 through 9, the wildcard character X, asterisk (*), and octothorpe (#); the uppercase characters A, B, C, and D; and blank. If this field is blank and the preceding field is not checked, no calling party transformation takes place. See the “Calling Party Number Transformations Settings” section in the <i>Cisco Unified CallManager System Guide</i> for more information.
Prefix Digits (Outgoing Calls)	Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries for the NANP include the digits 0 through 9; the wildcard characters asterisk (*) and octothorpe (#); the uppercase characters A, B, C, and D; and blank. Note The appended prefix digit does not affect which directory numbers route to the assigned device.

Table 38-1 **Hunt Pilot Configuration Settings (continued)**

Field	Description
Calling Line ID Presentation	Cisco Unified CallManager uses calling line ID presentation (CLIP/CLIR) as a supplementary service to allow or restrict the originating caller's phone number on a call-by-call basis. Choose whether you want the Cisco Unified CallManager to allow or restrict the display of the calling party's phone number on the called party's phone display for this hunt pilot. Choose <i>Default</i> if you do not want to change calling line ID presentation. Choose <i>Allowed</i> if you want Cisco Unified CallManager to allow the display of the calling number. Choose <i>Restricted</i> if you want Cisco Unified CallManager to block the display of the calling number. For more information about this field, see Table 17-6 in the “Calling Party Number Transformations Settings” section in the <i>Cisco Unified CallManager System Guide</i>.
Calling Name Presentation	Cisco Unified CallManager uses calling name presentation (CNIP/CNIR) as a supplementary service to allow or restrict the originating caller's name on a call-by-call basis. Choose whether you want the Cisco Unified CallManager to allow or restrict the display of the calling party's name on the called party's phone display for this hunt pilot. Choose <i>Default</i> if you do not want to change calling name presentation. Choose <i>Allowed</i> if you want Cisco Unified CallManager to display the calling name information. Choose <i>Restricted</i> if you want Cisco Unified CallManager to block the display of the calling name information. For more information about this field, see Table 17-6 in the “Calling Party Number Transformations Settings” section in the <i>Cisco Unified CallManager System Guide</i>.
Connected Party Transformations	
Connected Line ID Presentation	Cisco Unified CallManager uses connected line ID presentation (COLP/COLR) as a supplementary service to allow or restrict the called party's phone number on a call-by-call basis. Choose whether you want Cisco Unified CallManager to allow or restrict the display of the connected party's phone number on the calling party's phone display for this hunt pilot. Choose <i>Default</i> if you do not want to change the connected line ID presentation. Choose <i>Allowed</i> if you want to display the connected party's phone number. Choose <i>Restricted</i> if you want Cisco Unified CallManager to block the display of the connected party's phone number. For more information about this field, see Table 17-9 in the “Connected Party Presentation and Restriction Settings” section in the <i>Cisco Unified CallManager System Guide</i>.

Table 38-1 *Hunt Pilot Configuration Settings (continued)*

Field	Description
Connected Name Presentation	Cisco Unified CallManager uses connected name presentation (CONP/CONR) as a supplementary service to allow or restrict the called party's name on a call-by-call basis. Choose whether you want Cisco Unified CallManager to allow or restrict the display of the connected party's name on the calling party's phone display for this hunt pilot. Choose <i>Default</i> if you do not want to change the connected name presentation. Choose <i>Allowed</i> if you want to display the connected party's name. Choose <i>Restricted</i> if you want Cisco Unified CallManager to block the display of the connected party's name. For more information about this field, see Table 17-9 in the “Connected Party Presentation and Restriction Settings” section in the <i>Cisco Unified CallManager System Guide</i>.
Called Party Transformations	
Discard Digits	From the Discard Digits drop-down list box, choose the discard digits instructions that you want to associate with this hunt pilot. The discard digits that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box. See the “Discard Digits Instructions” section in the <i>Cisco Unified CallManager System Guide</i> more information on discard instructions for the North American Numbering Plan. Note The called party transformation settings that are assigned to the line groups in a hunt list override any called party transformation settings that are assigned to a hunt pilot that is associated with that hunt list.
Called Party Transform Mask	Enter a transformation mask value. Valid entries for the NANP include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); the uppercase characters A, B, C, and D; and blank. If the field is blank, no transformation takes place. Cisco Unified CallManager sends the dialed digits exactly as dialed.
Prefix Digits (Outgoing Calls)	Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries for the NANP include the digits 0 through 9; the wildcard characters asterisk (*) and octothorpe (#); the uppercase characters A, B, C, and D; and blank. Note The appended prefix digit does not affect which directory numbers route to the assigned device.

Table 38-1 **Hunt Pilot Configuration Settings (continued)**

Field	Description
AAR Group Settings	
AAR Group	Choose an Automated Alternate Routing (AAR) group from the drop-down list box. Note You can enable AAR for this hunt pilot only if all members of the line group are in the same location.
External Number Mask	Enter an external number mask value for the hunt pilot. Cisco Unified CallManager uses this mask to format calling line identification for external (outbound) calls. When AAR initiates a reroute, the system applies this external number mask to the hunt pilot number to form a fully qualified DN of the called party, which allows AAR to reroute properly in out-of-bandwidth conditions.

Additional Information

See the [“Related Topics”](#) section on page 38-11.

Related Topics

- [Finding a Hunt Pilot, page 38-1](#)
- [Configuring a Hunt Pilot, page 38-3](#)
- [Deleting a Hunt Pilot, page 38-4](#)
- [Hunt Pilot Configuration Settings, page 38-4](#)
- [Understanding Route Plans, Cisco Unified CallManager System Guide](#)
- [Wildcards and Special Characters in Route Patterns and Hunt Pilots, Cisco Unified CallManager System Guide](#)
- [Configuring a Route Filter, page 32-3](#)



SIP Route Pattern Configuration

Cisco Unified CallManager uses SIP route patterns to route or block both internal and external calls. The domain name or IP address provides the basis for routing. The administrator can add domains, IP addresses, and IP network (subnet) addresses and associate them to SIP trunks (only). This method allows requests that are destined for these domains to be routed through particular SIP trunk interfaces.



Note

Since there are no default SIP route patterns in Cisco Unified CallManager, they must be set up by the Administrators.

Domain name examples: cisco.com, my-pc.cisco.com, *.com, rtp-ccm[1-5].cisco.com

Valid characters for domain names: [, - , . , 0-9, A-Z, a-z, *, and].

IP address examples: 172.18.201.119 or 172.18.201.119/32 (explicit IP host address); 172.18.0.0/16 (IP subnet); 172.18.201.18.21 (IP subnet).

Valid characters for IP addresses: 0-9, ., and /.

Finding a SIP Route Pattern

Because you can have several SIP route patterns in your network, Cisco Unified CallManager lets you locate specific SIP route patterns on the basis of specific criteria. Use the following procedure to locate SIP route patterns.



Note

During your work in a browser session, the cookies on the client machine store your find/list search preference. If you navigate to other menu items and return to this menu item, or if you close the browser and then reopen a new browser window, the machine retains your Cisco Unified CallManager search preferences until you modify your search.

Procedure

Step 1 Choose **Call Routing > SIP Route Pattern**.

The Find and List SIP Route Patterns window displays. Use the two drop-down list boxes to search for a SIP route pattern.

Step 2 From the first Find SIP Route Patterns window drop-down list box, choose one of the following criteria:

- Pattern
- Description
- Route Partition

From the second Find Servers window drop-down list box, choose one of the following criteria:

- begins with
- contains
- is exactly
- ends with
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**.



Tip

To find all SIP route patterns that are registered in the database, click **Find** without entering any search text.

A list of discovered SIP route patterns displays by

- Pattern
- Description
- Route Partition



Note

You can delete multiple SIP route patterns from the Find and List Servers window by checking the check boxes next to the appropriate servers and clicking **Delete Selected**. You can delete all SIP route patterns in the window by checking the check box in the Matching records title bar and clicking **Delete Selected**.



Note

If the search returns too many results for you to easily locate the SIP route pattern for which you are searching, check the **Search Within Results** check box and click **Find**. If the check box is checked, when you click the Find button, the system searches results from the previous query. If you no longer want to search within the results, uncheck the check box and the next query will search as a new search.

Step 4 From the list of records, click the SIP route pattern that matches your search criteria.

The window displays the SIP route pattern that you choose.

Additional Information

See the [“Related Topics” section on page 39-7](#).

Configuring a SIP Route Pattern

This section describes how to add, update or copy a SIP route pattern.

Procedure

- Step 1** Perform one of the following tasks:
- To add a SIP route pattern, choose **Call Routing > SIP Route Pattern** and click **Add New**.
 - To update a SIP route pattern, find the pattern by using the procedure in the [“Finding a SIP Route Pattern” section on page 39-1](#)
 - To copy a SIP route pattern, find the pattern you wish to copy by using the procedure in the [“Finding a SIP Route Pattern” section on page 39-1](#). Click the Copy icon associated with the pattern you wish to copy.
- The SIP Route Pattern Configuration window displays.
- Step 2** Enter the appropriate settings as described in [Table 39-1](#).
- Step 3** To save the data and to add the server to the database, click the **Save** icon that displays in the tool bar in the upper, left corner of the window (or click the **Save** button that displays at the bottom of the window).

Additional Information

See the [“Related Topics” section on page 39-7](#).

SIP Route Pattern Configuration Settings

Before you begin:

At least one SIP Profile and SIP Trunk must be configured before you can configure a SIP route pattern. [Table 39-1](#) describes the SIP route pattern configuration settings. For related procedures, see the [“Related Topics” section on page 39-7](#).

Table 39-1 *SIP Route Pattern Configuration Settings*

Field	Description
Pattern Definition	
Pattern Usage	(Required) From the drop-down list, choose either Domain Routing or IP Address Routing.
Pattern	(Required) Enter the domain, sub-domain, IP address, or IP subnetwork address. Note For the IP subnetwork address, in Classless Inter-Domain Routing (CIDR) notation, X.X.X.X/Y; where Y is the network prefix denoting the number of bits in the address that will be the network address.
Description	For this optional entry, enter a description of the SIP Route Pattern.

Table 39-1 SIP Route Pattern Configuration Settings (continued)

Field	Description
Pattern Definition	
Route Partition	If you want to use a partition to restrict access to the SIP route pattern, choose the desired partition from the drop-down list box. If you do not want to restrict access to the SIP route pattern, choose <None> for the partition. See the “Partition Configuration” section on page 42-1 for more information on how to use partitions. You can configure the number of partitions that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more than 250 partitions are specified by using the Max List Box Items enterprise parameter, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Partition window. Enter a partial partition name in the List items where Name contains field. Click the desired partition name in the list of partitions that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAAdmin Parameters. Note Make sure the combination of SIP route pattern, route filter, and partition is unique within the Cisco Unified CallManager cluster.
SIP Trunk List	(Required) Use the drop-down list to choose the SIP trunk to which the SIP route pattern should be associated.
Block Pattern	If you do not want this pattern to be used for routing calls, choose the Block pattern radio button.
Calling Party Transformations	
Use Calling Party's External Phone Mask	Check the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls. You may also configure an External Phone Number Mask on all phone devices.
Calling Party Transformation Mask	Enter a transformation mask value. Valid entries include the digits 0 through 9, the wildcard characters X, asterisk (*), and octothorpe (#). If this field is blank and the preceding field is not checked, no calling party transformation takes place. See the “Calling Party Number Transformations Settings” section in the <i>Cisco Unified CallManager System Guide</i> for more information.
Prefix Digits (Outgoing Calls)	Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries include the digits 0 through 9, the wildcard characters asterisk (*) and octothorpe (#). Note The appended prefix digit does not affect which directory numbers route to the assigned device.

Table 39-1 SIP Route Pattern Configuration Settings (continued)

Field	Description
Pattern Definition	
Calling Line ID Presentation	Cisco Unified CallManager uses calling line ID presentation (CLIP/CLIR) as a supplementary service to allow or restrict the originating caller's phone number on a call-by-call basis. Choose whether you want the Cisco Unified CallManager to allow or restrict the display of the calling party's phone number on the called party's phone display for this SIP route pattern. Choose Default if you do not want to change calling line ID presentation. Choose Allowed if you want Cisco Unified CallManager to allow the display of the calling number. Choose Restricted if you want Cisco Unified CallManager to block the display of the calling number. For more information about this field, see Table 17-6 in the “Calling Party Number Transformations Settings” section in the <i>Cisco Unified CallManager System Guide</i>.
Calling Line Name Presentation	Cisco Unified CallManager uses calling name presentation (CNIP/CNIR) as a supplementary service to allow or restrict the originating caller's name on a call-by-call basis. Choose whether you want the Cisco Unified CallManager to allow or restrict the display of the calling party's name on the called party's phone display for this SIP route pattern. Choose Default if you do not want to change calling name presentation. Choose Allowed if you want Cisco Unified CallManager to display the calling name information. Choose Restricted if you want Cisco Unified CallManager to block the display of the calling name information. For more information about this field, see Table 17-6 in the “Calling Party Number Transformations Settings” section in the <i>Cisco Unified CallManager System Guide</i>.

Table 39-1 SIP Route Pattern Configuration Settings (continued)

Field	Description
Pattern Definition	
Connected Party Transformations	
Connected Line ID Presentation	Cisco Unified CallManager uses connected line ID presentation (COLP/COLR) as a supplementary service to allow or restrict the called party's phone number on a call-by-call basis. Choose whether you want Cisco Unified CallManager to allow or restrict the display of the connected party's phone number on the calling party's phone display for this SIP route pattern. Choose Default if you do not want to change the connected line ID presentation. Choose Allowed if you want to display the connected party's phone number. Choose Restricted if you want Cisco Unified CallManager to block the display of the connected party's phone number. For more information about this field, see Table 17-9 in the “Connected Party Presentation and Restriction Settings” section in the <i>Cisco Unified CallManager System Guide</i>.
Connected Line Name Presentation	Cisco Unified CallManager uses connected name presentation (CONP/CONR) as a supplementary service to allow or restrict the called party's name on a call-by-call basis. Choose whether you want Cisco Unified CallManager to allow or restrict the display of the connected party's name on the calling party's phone display for this SIP route pattern. Choose Default if you do not want to change the connected name presentation. Choose Allowed if you want to display the connected party's name. Choose Restricted if you want Cisco Unified CallManager to block the display of the connected party's name. For more information about this field, see Table 17-9 in the “Connected Party Presentation and Restriction Settings” section in the <i>Cisco Unified CallManager System Guide</i>.

Deleting a SIP Route Pattern

This section describes how to delete a SIP route pattern from the Cisco Unified CallManager database.

Procedure

- Step 1** Find the SIP route pattern by using the procedure in the “[Finding a SIP Route Pattern](#)” section on [page 39-1](#).
- Step 2** From the list of matching records, choose the SIP route pattern that you want to delete.

Step 3 To delete the SIP route pattern, click the **Delete Selected Item** icon that displays in the tool bar in the upper, left corner of the window (or click the **Delete Selected** button that displays at the bottom of the window).

If the SIP route pattern is not in use, Cisco Unified CallManager deletes it. If it is in use, a message displays.

Additional Information

See the [“Related Topics”](#) section on page 39-7.

Related Topics

- [Finding a SIP Route Pattern, page 39-1](#)
- [Configuring a SIP Route Pattern, page 39-3](#)
- [Deleting a SIP Route Pattern, page 39-6](#)
- [SIP Route Pattern Configuration Settings, page 39-3](#)



Time Period Configuration

A time period comprises a time range that is defined by a start time and end time. Time periods also specify a repetition interval either as days of the week or a specified date on the yearly calendar. Administrators define time periods and then associate the time periods with time schedules. Administrators then associate time schedules with partitions to set up time-of-day call routing. For more detailed information on time periods and time schedules, refer to [“Time-of-Day Routing”](#) in the *Cisco Unified CallManager System Guide*.

Use the following topics to add, update, copy, or delete a time period:

- [Finding a Time Period, page 40-1](#)
- [Configuring a Time Period, page 40-2](#)
- [Deleting a Time Period, page 40-3](#)
- [Time Period Configuration Settings, page 40-4](#)

Finding a Time Period

Because you might have several time periods in your network, Cisco Unified CallManager lets you locate specific time periods by using specific criteria as the basis. Use the following procedure to locate time periods.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your time period search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your time period search preferences until you modify your search or close the browser.

Procedure

- Step 1** Choose **Route Plan > Class of Control > Time Period**.
The Find and List Time Periods window displays.
- Step 2** From the drop-down list box, choose one of the following criteria:
- begins with
 - contains

- ends with
- is exactly

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Note To find all time periods that are registered in the database, click **Find** without entering any search text.

A list of discovered time periods displays by

- Time period icon
- Time period name



Tip To search for time periods within the search results, click the **Search Within Results** check box and enter your search criteria as described in this step.



Note You can delete multiple time periods from the Find and List Time Periods window by checking the check boxes next to the appropriate time periods and clicking **Delete Selected**. You can choose all time periods in the window by checking the check box in the matching records title bar and clicking **Delete Selected**.

Step 4 From the list of records, click the time period that matches your search criteria.
The window displays the time period that you choose.

Additional Information

See the [“Related Topics” section on page 40-5](#).

Configuring a Time Period

The following procedure describes how to configure a time period.

Procedure

Step 1 In the menu bar, choose **Route Plan > Class of Control > Time Period**.

The Find and List Time Periods window displays.

Step 2 Perform one of the following tasks:

- To copy an existing time period, locate the appropriate time period as described in [“Finding a Time Period” section on page 40-1](#). Click the **Copy** button next to the time period that you want to copy. The window displays the copy of the time period. Change the value in the Name field, and continue with [Step 3](#).
- To add a new time period, click the **Add New** button, and continue with [Step 3](#).

- To update an existing time period, locate the appropriate time period as described in [“Finding a Time Period” section on page 40-1](#), and continue with [Step 3](#).

Step 3 Enter the appropriate settings as described in [Table 40-1](#).

Step 4 Click **Save**.

Additional Information

See the [“Related Topics” section on page 40-5](#).

Deleting a Time Period

The following procedure describes how to delete a time period.

Before You Begin

You cannot delete time periods that time schedules are using. To find out which time schedules or other items are using the time period, click the **Dependency Records** link from the Time Period Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#). If you try to delete a time period that is in use, Cisco Unified CallManager displays an error message. Before deleting a time period that is currently in use, you must perform either or both of the following tasks:

- Assign a different time period to any time schedules that are using the time period that you want to delete. See the [“Configuring a Time Schedule” section on page 41-2](#).
- Delete the time schedules that are using the time period that you want to delete. See the [“Deleting a Time Schedule” section on page 41-3](#).

Procedure

Step 1 In the menu bar, choose **Route Plan > Class of Control > Time Period**.

Step 2 Locate the time period that you want to delete. See the [“Finding a Time Period” section on page 40-1](#).

Step 3 Check the check box of the time period that you want to delete and click **Delete Selected**.

A message displays that states that you cannot undo this action.

Step 4 Click **OK** to delete the time period or click **Cancel** to cancel the deletion.



Caution

Before initiating this action, check carefully to ensure that you are deleting the correct time period. You cannot retrieve deleted time periods. If a time period is accidentally deleted, you must rebuild it.



Tip

You can also delete a time period by locating and displaying the time period that you want to delete and clicking **Delete**.

Additional Information

See the [“Related Topics”](#) section on page 40-5.

Time Period Configuration Settings

Table 40-1 describes the time period configuration settings.

Table 40-1 Time Period Configuration Settings

Field	Description
Time Period Information	
Name	Enter a name in the Time Period Name field. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure each time period name is unique to the plan. Note Use concise and descriptive names for your time periods. The hours_or_days format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a time period. For example, office_M_to_F identifies a time period for the business hours of an office from Monday to Friday.
Time Of Day Start	From the drop-down list box, choose the time when this time period starts. The available listed start times comprise 15-minute intervals throughout a 24-hour day. The default value is <i>No Office Hours</i>. Note To start a time period at midnight, choose the 0:00 value.

Table 40-1 Time Period Configuration Settings (continued)

Field	Description
Time of Day End	From the drop-down list box, choose the time when this time period ends. The available listed end times comprise 15-minute intervals throughout a 24-hour day. The default value is <i>No Office Hours</i>. Note You must choose an End Time that is later than the Start Time that you chose. Note To end a time period at midnight, choose the 24:00 value.
Repeat Every	Click on one of the radio buttons: - Week from—If you click on the Week from radio button, use the drop-down list boxes next to <i>from</i> and <i>through</i> to choose the days of the week during which this time period applies. Examples: Choose a <i>from</i> value of Mon(day) and a <i>through</i> value of Fri(day) to define a time period that applies from Monday through Friday. Choose a <i>from</i> value of Sat(urday) and a <i>through</i> value of Sat(urday) to define a time period that applies only on Saturdays. - Year on—If you click on the Year on radio button, use the drop-down list boxes to choose the month and day of the year on which this time period applies. Example: Choose the month <i>Jan(uary)</i> and the day <i>1</i> to define a time period that applies yearly on New Year's Day.

Additional Information

See the [“Related Topics” section on page 40-5](#).

Related Topics

- [Finding a Time Period, page 40-1](#)
- [Configuring a Time Period, page 40-2](#)
- [Deleting a Time Period, page 40-3](#)
- [Time Period Configuration Settings, page 40-4](#)
- [Time-of-Day Routing, Cisco Unified CallManager System Guide](#)



Time Schedule Configuration

A time schedule comprises a group of time periods. Time schedules get assigned to partitions. Time schedules determine the partitions where calling devices search when they are attempting to complete a call during a particular time of day. For more detailed information on time schedules, refer to [“Time-of-Day Routing”](#) in the *Cisco Unified CallManager System Guide*.

Use the following topics to find, add, update, copy, or delete a time schedule:

- [Finding a Time Schedule, page 41-1](#)
- [Configuring a Time Schedule, page 41-2](#)
- [Deleting a Time Schedule, page 41-3](#)
- [Time Schedule Configuration Settings, page 41-4](#)

Finding a Time Schedule

Because you might have several time schedules in your network, Cisco Unified CallManager lets you locate specific time schedules by using specific criteria as the basis. Use the following procedure to locate time schedules.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your time schedule search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your time schedule search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Route Plan > Class of Control > Time Schedule**.

The Find and List Time Schedules window displays.

Step 2 From the drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly

- Step 3** Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Note To find all time schedules that are registered in the database, click **Find** without entering any search text.

A list of discovered time schedules displays by

- Time schedule icon
- Time schedule name



Tip To search for time schedules within the search results, click the **Search Within Results** check box and enter your search criteria as described in this step.



Note You can delete multiple time schedules from the Find and List Time Schedules window by checking the check boxes next to the appropriate time schedules and clicking **Delete Selected**. You can choose all time schedules in the window by checking the check box in the matching records title bar and clicking **Delete Selected**.

- Step 4** From the list of records, click the time schedule that matches your search criteria.
The window displays the time schedule that you choose.

Additional Information

See the [“Related Topics” section on page 41-5](#).

Configuring a Time Schedule

The following procedure describes how to add a time schedule.

Procedure

- Step 1** In the menu bar, choose **Route Plan > Class of Control > Time Schedule**.
The Find and List Time Schedules window displays.
- Step 2** Perform one of the following tasks:
- To copy an existing time schedule, locate the appropriate time schedule as described in the [“Finding a Time Schedule” section on page 41-1](#). Click the **Copy** button next to the time schedule that you want to copy. The window displays the copy of the time schedule. Change the value in the Name field, and continue with [Step 3](#).
 - To add a new time schedule, click the **Add New** button and continue with [Step 3](#).
 - To update an existing time schedule, locate the appropriate time schedule as described in the [“Finding a Time Schedule” section on page 41-1](#), and continue with [Step 3](#).

- Step 3** Enter the appropriate settings as described in [Table 41-1](#).
- Step 4** Click **Save**.
-

Additional Information

See the [“Related Topics”](#) section on page 41-5.

Deleting a Time Schedule

The following procedure describes how to delete a time schedule.

Before You Begin

You cannot delete time schedules that partitions are using. To find out which items are using the time schedule, click the **Dependency Records** link from the Time Schedule Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records”](#) section on page A-2. If you try to delete a time schedule that is in use, Cisco Unified CallManager displays an error message. Before deleting a time schedule that is currently in use, you must perform either or both of the following tasks:

- Assign a different time schedule to any partitions that are using the time schedule that you want to delete. See the [“Configuring a Partition”](#) section on page 42-2.
- Delete the partitions that are using the time schedule that you want to delete. See the [“Partition Configuration”](#) chapter.

Procedure

- Step 1** In the menu bar, choose **Route Plan > Class of Control > Time Schedule**.
- Step 2** Locate the time schedule that you want to delete. See the [“Finding a Time Schedule”](#) section on page 41-1.
- Step 3** Check the check box of the time schedule that you want to delete and click **Delete Selected**.
A message displays that states that you cannot undo this action.
- Step 4** To delete the time schedule, click **OK** or to cancel the deletion, click **Cancel**.



Caution

Before initiating this action, check carefully to ensure that you are deleting the correct time schedule. You cannot retrieve deleted time schedules. If a time schedule is accidentally deleted, you must rebuild it.



Tip

You can also delete a time schedule by locating and displaying the time schedule that you want to delete and clicking **Delete**.

Additional Information

See the [“Related Topics”](#) section on page 41-5.

Time Schedule Configuration Settings

[Table 41-1](#) describes the time schedule configuration settings.

Table 41-1 Time Schedule Configuration Settings

Field	Description
Time Schedule Information	
Name	Enter a name in the Name field. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure each time schedule name is unique to the plan. Note Use concise and descriptive names for your time schedules.
Time Period Information	
Available Time Periods	Choose a time period in the Available Time Periods list box and add it to the Selected Time Periods list box by clicking the down arrow button between the two list boxes. To add a range of time periods at once, click the first time period in the range; then, hold down the Shift key while clicking the last time period in the range. Click the down arrow button between the two list boxes to add the range of time periods. To add multiple time periods that are not contiguous, hold down the Control (Ctrl) key while clicking multiple time periods. Click the down arrow button between the two list boxes to add the chosen time periods.
Selected Time Periods	This list box lists the time periods that were selected for this time schedule. To remove a time period from the list of selected time periods, choose the time period to remove and click the up arrow between the two list boxes. Note If multiple time periods get associated to a time schedule and the time periods overlap, time periods with Day of Year settings take precedence over time periods with Day of Week settings. Example: If a Time Period configured for January 1st is configured as No Office Hours and another time period is configured for the same day of the week (for example, Sunday to Saturday) as 08:00 to 17:00, the time period for January 1st gets used. In this example, No Office Hours takes precedence. Note Time interval settings take precedence over No Office Hour settings for the same day of the year or day of the week. Example: One time period specifies for Saturday as No Office Hours. Another time period specifies Saturday hours of 08:00 to 12:00. In this example, the resulting time interval specifies 08:00 to 12:00 for Saturday.

Additional Information

See the [“Related Topics”](#) section on page 41-5.

Related Topics

- [Finding a Time Schedule](#), page 41-1
- [Configuring a Time Schedule](#), page 41-2
- [Deleting a Time Schedule](#), page 41-3
- [Time Schedule Configuration Settings](#), page 41-4
- [Time-of-Day Routing](#), *Cisco Unified CallManager System Guide*



Partition Configuration

A partition contains a list of route patterns (directory number (DN) and route patterns). Partitions facilitate call routing by dividing the route plan into logical subsets that are based on organization, location, and call type. For more information about partitions, refer to “[Partitions and Calling Search Spaces](#)” in the *Cisco Unified CallManager System Guide*.

Use the following topics to find, add, update, or delete route partitions:

- [Finding a Partition, page 42-1](#)
- [Configuring a Partition, page 42-2](#)
- [Deleting a Partition, page 42-3](#)
- [Partition Configuration Settings, page 42-4](#)

Finding a Partition

Because you might have several partitions in your network, Cisco Unified CallManager lets you locate specific partitions based on specific criteria. Use the following procedure to locate partitions.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your partition search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your partition search preferences until you modify your search.

Procedure

- Step 1** Choose **Route Plan > Class of Control > Partition**.
- The Find and List Partitions window displays.
- Step 2** From the drop-down list box, choose one of the following criteria:
- begins with
 - contains

- ends with
- is exactly
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Note To find all partitions that are registered in the database, click **Find** without entering any search text.

A list of discovered partitions displays by

- Partition name
- Description



Tip To search for partitions within the search results, click the **Search Within Results** check box and enter your search criteria as described in this step.



Note You can delete multiple partitions from the Find and List Partitions window by checking the check boxes next to the appropriate partitions and clicking **Delete Selected**. You can delete all partitions in the window by clicking **Select All** and clicking **Delete Selected**.

Step 4 From the list of records, click the partition that matches your search criteria.
The window displays the partition that you chose.

Additional Information

See the [“Related Topics”](#) section on page 42-6.

Configuring a Partition

Perform the following procedure to add a partition.

Procedure

- Step 1** In the menu bar, choose **Route Plan > Class of Control > Partition**.
The Find and List Partitions window displays.
- Step 2** Perform one of the following tasks:
- To add a new partition, click the Add New. button, and continue with [Step 3](#).
 - To update an existing partition, locate the appropriate partition as described in [“Finding a Partition”](#) section on page 42-1, and continue with [Step 3](#).
- Step 3** Enter the appropriate settings as described in [Table 42-1](#).

Step 4 Click **Save**.

If you are updating a partition, click **Reset**. When you reset devices that are associated with the partition, all calls on affected gateways drop.

**Note**

You can configure multiple partitions. To enter multiple partitions, use one line for each partition entry. You can enter up to 75 partitions; the names and descriptions can have a total of up to 1475 characters. Use a comma (,) to separate the partition name and description on each line. If you do not enter a description, Cisco Unified CallManager uses the name as the description.

Additional Information

See the [“Related Topics” section on page 42-6](#).

Deleting a Partition

The following procedure describes how to delete a partition.

Before You Begin

You cannot delete a partition if it is assigned to an item such as calling search space or to a route pattern. To find out which calling search spaces or other items are using the partition, choose **Dependency Records** from the Related Links drop-down list box in the Partition Configuration window and click **Go**. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, refer to the [“Accessing Dependency Records” section on page A-2](#). If you try to delete a partition that is in use, Cisco Unified CallManager displays a message. Before deleting a partition that is currently in use, you must perform either or both of the following tasks:

- Assign a different partition to any calling search spaces, devices, or other items that are using the partition that you want to delete.
- Delete the calling search spaces, devices, or other items that are using the partition that you want to delete.

Procedure

Step 1 In the menu bar, choose **Route Plan > Class of Control > Partition**.

Step 2 Locate the partition that you want to delete. See the [“Finding a Partition” section on page 42-1](#).

Step 3 Check the check box of the partition that you want to delete and click **Delete Selected**.

**Tip**

You can delete all the partitions in the list by clicking **Select All** and then clicking **Delete Selected**.

A message displays that states that you cannot undo this action.

Step 4 To delete the partition, click **OK** or to cancel the deletion, click **Cancel**.



Caution

Before initiating this action, check carefully to ensure that you are deleting the correct partition. You cannot retrieve deleted partitions. If a partition is accidentally deleted, you must rebuild it.



Tip

You can also delete a partition by locating and displaying the partition that you want to delete and clicking **Delete**.

Additional Information

See the [“Related Topics” section on page 42-6](#).

Partition Configuration Settings

[Table 42-1](#) describes the partition configuration settings. For related procedures, see the [“Related Topics” section on page 42-6](#).

Table 42-1 *Partition Configuration Settings*

Field	Description
(Partition Name, Description)	Enter a name in the partition name and description box. Ensure each partition name is unique to the route plan. Partition names can contain alphanumeric characters, as well as spaces, hyphens (-), and underscore characters (_). Note The length of the partition names limits the maximum number of partitions that can be added to a calling search space. Table 42-2 provides examples of the maximum number of partitions that can be added to a calling search space if partition names are of fixed length. Follow the partition name by a comma (,); then, enter a description on the same line as the Partition Name. If you do not enter a description, Cisco Unified CallManager automatically enters the partition name in this field. Use a new line for each partition and description.

Table 42-1 *Partition Configuration Settings (continued)*

Field	Description
Time Schedule	From the drop-down list box, choose a time schedule to associate with this partition. The associated time schedule specifies when the partition is available to receive incoming calls. The default value specifies <i>None</i>, which implies that time-of-day routing is not in effect and the partition remains active at all times. In combination with the Time Zone value in the following field, association of a partition with a time schedule configures the partition for time-of-day routing. The system checks incoming calls to this partition against the specified time schedule.
Time Zone	Choose one of the following options to associate a partition with a time zone: • Originating Device—If you choose this option, the system checks the partition against the associated time schedule with the time zone of the calling device. • Specific Time Zone—If you choose this option, choose a time zone from the drop-down list box. The system checks the partition against the associated time schedule at the time that is specified in this time zone. These options all specify the Time Zone. When there is an incoming call, the current time on the Cisco Unified CallManager is converted into the specific time zone set when one of the options is chosen. This specific time is validated against the value in the Time Schedule field.

**Timesaver**

Use concise and descriptive names for your partitions. The CompanynameLocationCalltype format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a partition. For example, CiscoDallasMetroPT identifies a partition for toll-free, inter-local access and transport area (LATA) calls from the Cisco office in Dallas.

**Tip**

You can enter multiple partitions at the same time by entering the partition name and description, if applicable, in the Partition Name & Description text box. Remember to use one line for each partition entry and to separate the partition name and description with a comma.

[Table 42-2](#) provides examples of the maximum number of partitions that can be added to a calling search space if partition names are of fixed length. Refer to “[Partition Name Limitations](#)” in the *Cisco Unified CallManager System Guide* for details about how this maximum number is calculated.

Table 42-2 *Calling Search Space Partition Limitations*

Partition Name Length	Maximum Number of Partitions
2 characters	170
3 characters	128
4 characters	102

Table 42-2 *Calling Search Space Partition Limitations (continued)*

Partition Name Length	Maximum Number of Partitions
5 characters	86
...	...
10 characters	46
15 characters	32

Additional Information

See the [“Related Topics”](#) section on page 42-6.

Searching for a Partition

If more than 250 partitions exist, the ellipsis (...) button displays next to the Partition drop-down list box on the Cisco Unified CallManager Administration windows where the button appears. You can click the (...) button to search for the partition that you want. Use the following procedure to search for a partition.

Procedure

-
- Step 1** Click the ... button next to the Partition drop-down list box.
- The Select Partition window displays.
- Step 2** In the **List items where Name contains** field, enter a partial partition name.
- Step 3** In the list of partitions that displays in the **Select item to use** box, click the desired partition name and click **OK**.
-

Additional Information

See the [“Related Topics”](#) section on page 42-6.

Related Topics

- [Finding a Partition, page 42-1](#)
- [Configuring a Partition, page 42-2](#)
- [Deleting a Partition, page 42-3](#)
- [Partition Configuration Settings, page 42-4](#)
- [Searching for a Partition, page 42-6](#)



Calling Search Space Configuration

A calling search space comprises an ordered list of route partitions that are typically assigned to devices. Calling search spaces determine the partitions that calling devices search when they are attempting to complete a call. For more detailed information on calling search spaces and partitions, refer to [“Partitions and Calling Search Spaces”](#) in the *Cisco Unified CallManager System Guide*.

Finding a Calling Search Space

Because you might have several calling search spaces in your network, Cisco Unified CallManager lets you locate specific calling search spaces by using specific criteria as the basis. Use the following procedure to locate calling search spaces.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your calling search space search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your calling search space search preferences until you modify your search.

Procedure

- Step 1** Choose **Route Plan > Class of Control > Calling Search Space**.
The Find and List Calling Search Spaces window displays.
- Step 2** From the drop-down list box, choose one of the following criteria:
- begins with
 - contains
 - ends with
 - is exactly
 - is empty
 - is not empty
- Step 3** Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.

**Note**

To find all calling search spaces that are registered in the database, click **Find** without entering any search text.

A list of discovered calling search spaces displays by

- CSS name
- Description

**Tip**

To search for calling search spaces within the search results, click the **Search Within Results** check box and enter your search criteria as described in this step.

**Note**

You can delete multiple calling search spaces from the Find and List Calling Search Spaces window by checking the check boxes next to the appropriate calling search spaces and clicking **Delete Selected**. You can delete all calling search spaces in the window by checking the check box in the matching records title bar and clicking **Delete Selected**.

- Step 4** From the list of records, click the calling search space that matches your search criteria.
The window displays the calling search space that you choose.

Additional Topics

See the [“Related Topics” section on page 43-6](#).

Configuring a Calling Search Space

The following procedure describes how to copy, add and update a calling search space.

Procedure

- Step 1** In the menu bar, choose **Route Plan > Class of Control > Calling Search Space**.
- Step 2** Perform one of the followings tasks:
- To copy an existing calling search space, locate the appropriate calling search space as described in [“Finding a Calling Search Space” section on page 43-1](#). Click the **Copy** button next to the calling search space that you want to copy. The window displays the copy of the calling search space. Change the Calling Search Space Name, and continue with [Step 3](#).
 - To add a calling search space, click the **Add New** button, and continue with [Step 3](#).

**Note**

To add more calling search spaces, click **Add New** and repeat this procedure.

- To update an existing calling search space, locate the appropriate calling search space as described in [“Finding a Calling Search Space” section on page 43-1](#), and continue with [Step 3](#).

- Step 3** Enter the appropriate settings as described in [Table 43-1](#).
- Step 4** Click **Save**.

Additional Topics

See the [“Related Topics”](#) section on page 43-6.

Calling Search Space Configuration Settings

[Table 43-1](#) describes the calling search space configuration settings.

Table 43-1 *Calling Search Space Configuration Settings*

Field	Description
Calling Search Space Information	
Name	Enter a name in the Calling Search Space Name field. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure each calling search space name is unique to the system. Note Use concise and descriptive names for your calling search spaces. The CompanynameLocationCalltype format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a calling search space. For example, CiscoDallasMetroCS identifies a calling search space for toll-free, inter-local access and transport area (LATA) calls from the Cisco office in Dallas.
Description	Enter a description in the Description field. The description can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

Table 43-1 *Calling Search Space Configuration Settings (continued)*

Field	Description
Route Partitions for this Calling Search Space	
Available Partitions	Choose a partition in the Available Partitions list box and add it to the Selected Partitions list box by clicking the arrow button between the two list boxes. To add a range of partitions at once, click the first partition in the range; then, hold down the Shift key while clicking the last partition in the range. Click the arrow button between the two list boxes to add the range of partitions. To add multiple partitions that are not contiguous, hold down the Control (Ctrl) key while clicking multiple partitions. Click the arrow button between the two list boxes to add the chosen partitions. Note The length of the partition names limits the maximum number of partitions that can be added to a calling search space. Table 43-2 provides examples of the maximum number of partitions that can be added to a calling search space if partition names are of fixed length.
Selected Partitions (Ordered by highest priority)	To change the priority of a partition, choose a partition name in the Selected Partitions list box. Move the partition up or down in the list by clicking the arrows on the right side of the list box.

[Table 43-2](#) provides examples of the maximum number of partitions that can be added to a calling search space if partition names are of fixed length. Refer to “[Partition Name Limitations](#)” in the *Cisco Unified CallManager System Guide* for details about how this maximum number is calculated.

Table 43-2 *Calling Search Space Partition Limitations*

Partition Name Length	Maximum Number of Partitions
2 characters	170
3 characters	128
4 characters	102
5 characters	86
...	...
10 characters	46
15 characters	32

Additional Topics

See the “[Related Topics](#)” section on page 43-6.

Deleting a Calling Search Space

The following procedure describes how to delete a calling search space.

Before You Begin

You cannot delete calling search spaces that devices, lines (DNs), translation patterns, or other items are using. To find out which devices, lines, translation patterns, or other items are using the calling search space, choose the **Dependency Records** from the Related Links drop-down list box in the Calling Search Space Configuration window and click **Go**. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, refer to the [“Accessing Dependency Records” section on page A-2](#). If you try to delete a calling search space that is in use, Cisco Unified CallManager displays a message. Before deleting a calling search space that is currently in use, you must perform either or both of the following tasks:

- Assign a different calling search space to any devices, lines, or translation patterns that are using the calling search space that you want to delete. Refer to the [“Directory Number Configuration Overview” section on page 49-1](#) and the [“Configuring a Translation Pattern” section on page 46-3](#).
- Delete the devices, lines, or translation patterns that are using the calling search space that you want to delete. Refer to the [“Removing a Directory Number from a Phone” section on page 49-4](#), and the [“Deleting a Translation Pattern” section on page 46-9](#).

Procedure

-
- Step 1** In the menu bar, choose **Route Plan > Class of Control > Calling Search Space**.
- Step 2** Locate the calling search space that you want to delete. See the [“Finding a Calling Search Space” section on page 43-1](#).
- Step 3** Check the check box of the calling search space that you want to delete and click **Delete Selected**.
A message displays that states that you cannot undo this action.
- Step 4** To delete the calling search space, Click **OK** or click **Cancel**.



Caution

Before initiating this action, check carefully to ensure that you are deleting the correct calling search space. You cannot retrieve deleted calling search spaces. If a calling search space is accidentally deleted, you must rebuild it.



Tip

You can also delete a calling search space by locating and displaying the calling search space that you want to delete and clicking **Delete**.

Additional Topics

See the [“Related Topics” section on page 43-6](#).

Related Topics

Use the following topics to find, add, update, copy, or delete a calling search space:

- [Finding a Calling Search Space, page 43-1](#)
- [Configuring a Calling Search Space, page 43-2](#)
- [Calling Search Space Configuration Settings, page 43-3](#)
- [Deleting a Calling Search Space, page 43-5](#)



Client Matter Codes

Client Matter Codes (CMC) assists with call accounting and billing for billable clients. CMC forces the user to enter a code to specify that the call relates to a specific client matter. You can assign client matter codes to customers, students, or other populations for call accounting and billing purposes.

The CMC feature requires that you make changes to route patterns and update your dial plan documents to reflect that you enabled or disabled CMC for each route pattern. You can access the Client Matter Codes search and configuration windows from **Call Routing > Client Matter Codes** in Cisco Unified CallManager Administration.

For detailed information about client matter codes, see the [“Client Matter Codes and Forced Authorization Codes”](#) chapter in the *Cisco Unified CallManager Features and Services Guide*.

Additional Cisco Documentation

- *Cisco Unified CallManager Bulk Administration Guide*
- *Cisco Unified CallManager Serviceability System Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*



Forced Authorization Code

Forced Authorization Codes (FAC) allow you to manage call access and accounting. This feature regulates the types of calls that certain users can place, forcing the user to enter a valid authorization code before the call completes.

The FAC feature requires that you make changes to route patterns and update your dial plan documents to reflect that you enabled or disabled FAC for each route pattern. You can access the Forced Authorization Code search and configuration windows from **Call Routing > Forced Authorization Codes**, in Cisco Unified CallManager Administration.

For detailed information about client matter codes, see the [“Client Matter Codes and Forced Authorization Codes”](#) chapter in the *Cisco Unified CallManager Features and Services Guide*.

Additional Cisco Documentation

- *Cisco Unified CallManager Bulk Administration Guide*
- *Cisco Unified CallManager Serviceability System Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*



Translation Pattern Configuration

Cisco Unified CallManager uses translation patterns to manipulate dialed digits before it routes a call. In some cases, the system does not use the dialed number. In other cases, the public switched telephone network (PSTN) does not recognize the dialed number.

Use the following topics to add, update, copy, or delete a translation pattern:

- [Finding a Translation Pattern, page 46-1](#)
- [Configuring a Translation Pattern, page 46-3](#)
- [Deleting a Translation Pattern, page 46-9](#)
- [Translation Pattern Configuration Settings, page 46-4](#)

Finding a Translation Pattern

Because you might have several translation patterns in your network, Cisco Unified CallManager lets you locate specific translation patterns by using specific criteria as the basis. Use the following procedure to locate translation patterns.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your translation pattern search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your translation pattern search preferences until you modify your search or close the browser.

Procedure

- Step 1** Choose **Call Routing > Translation Pattern**.
- The Find and List Translation Patterns window displays.
- Step 2** From the first drop-down list box, choose one of the following criteria:
- Pattern (to search by translation pattern names)
 - Description (to search by translation pattern descriptions)
 - Partition (to search by the partition name)

**Note**

The criterion that you choose in this drop-down list box specifies how the list of translation patterns that your search generates will be sorted. For example, if you choose Description, the Description column will display as the left column of the results list.

From the second drop-down list box, choose one of the following criteria:

- begins with
- contains
- is exactly
- ends with
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.

**Note**

To find all translation patterns that are registered in the database, click **Find** without entering any search text.

A list of discovered translation patterns displays by

- Translation Pattern
- Partition
- Description
- Route Filter

**Note**

You can delete multiple translation patterns from the Find and List Translation Patterns window by checking the check boxes next to the appropriate translation patterns and clicking **Delete Selected**. You can delete all the translation patterns in the window by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records, click the translation pattern that matches your search criteria.

The Translation Pattern Configuration window displays the translation pattern that you choose.

Additional Information

See the [“Related Topics”](#) section on page 46-9.

Configuring a Translation Pattern

This section describes how to configure a translation pattern.

Before You Begin

Configure the following Cisco Unified CallManager items before configuring a translation pattern:

- Partition
- Route filter
- Calling search space

Procedure

Step 1 Choose **Call Routing > Translation Pattern**.

The Find and List Translation Patterns window displays.

Step 2 Perform one of the followings tasks:

- To copy an existing translation pattern, locate the appropriate translation pattern as described in the [“Finding a Translation Pattern” section on page 46-1](#), click the **Copy** button next to the translation pattern that you want to copy, and continue with [Step 3](#).
- To add a new translation pattern, click the **Add New** button, and continue with [Step 3](#).
- To update an existing translation pattern, locate the appropriate translation pattern as described in the [“Finding a Phone” section on page 70-29](#), and continue with [Step 3](#).

Step 3 In the Translation Pattern Configuration window that displays, enter the appropriate configuration settings as described in [Table 46-1](#).

Step 4 Click **Save**.



Note Ensure that the translation pattern, that uses the selected partition, route filter, and numbering plan combination, is unique. Check the route pattern/hunt pilot, translation pattern, directory number, call park number, call pickup number, or meet-me number configuration windows if you receive an error that indicates duplicate entries.

The Translation Pattern Configuration window displays the newly configured translation pattern.

Additional Information

See the [“Related Topics” section on page 46-9](#).

Translation Pattern Configuration Settings

Table 46-1 describes the available fields in the Translation Pattern Configuration window.

Table 46-1 Translation Pattern Configuration Settings

Field	Description
Pattern Definition	
Translation Pattern	Enter the translation pattern, including numbers and wildcards (do not use spaces), in the Translation Pattern field. For example, for the NANP, enter 9.@ for typical local access or 8XXX for a typical private network numbering plan. Valid characters include the uppercase characters A, B, C, and D. If you leave this field blank, you must select a partition from the Partition drop-down list box. Note Ensure that the translation pattern, which uses the chosen partition, route filter, and numbering plan combination, is unique. Check the route pattern/hunt pilot, translation pattern, directory number, call park number, call pickup number, or meet-me number if you receive a message that indicates duplicate entries. Alternatively, check the route plan report if you receive a message that indicates duplicate entries.
Partition	Choose a partition. If you do not want to assign a partition, choose <i><None></i>. If you choose <i><None></i>, you must enter a value in the Translation Pattern field. You can configure the number of partitions that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more partitions exist than the number that are configured in the Max List Box Items enterprise parameter, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Partition window. Enter a partial partition name in the List items where Name contains field. Click the desired partition name in the list of partitions that display in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters. Note Make sure that the combination of translation pattern, route filter, and partition is unique within the Cisco Unified CallManager cluster.
Description	Enter a description for the translation pattern.
Numbering Plan	Choose a numbering plan. If your translation pattern includes the @ wildcard, you may choose a numbering plan. The optional act of choosing a numbering plan restricts certain number patterns.

Table 46-1 Translation Pattern Configuration Settings (continued)

Field	Description
Route Filter	Choosing an optional route filter restricts certain number patterns. Refer to the “Wildcards and Special Characters in Route Patterns and Hunt Pilots” section in the <i>Cisco Unified CallManager System Guide</i> and the “Route Filter Configuration Settings” section on page 32-4 for more information. The route filters that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box. If more than 250 route filters exist, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Route Filters window. Enter a partial route filter name in the List items where Name contains field. Click the desired route filter name in the list of route filters that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.
MLPP Precedence	Choose an MLPP precedence setting for this translation pattern from the drop-down list box: • Executive Override—Highest precedence setting for MLPP calls. • Flash Override—Second highest precedence setting for MLPP calls. • Flash—Third highest precedence setting for MLPP calls. • Immediate—Fourth highest precedence setting for MLPP calls. • Priority—Fifth highest precedence setting for MLPP calls. • Routine—Lowest precedence setting for MLPP calls. • Default—Does not override the incoming precedence level but rather lets it pass unchanged. Note Refer to the “Precedence” section in the “Multilevel Precedence and Preemption” chapter of the <i>Cisco Unified CallManager Features and Services Guide</i> for more information.
Calling Search Space	From the drop-down list box, choose the calling search space for which you are adding a translation pattern, if necessary. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the number that are configured in the Max List Box Items enterprise parameter, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Calling Search Space window. Enter a partial calling search space name in the List items where Name contains field. Click the desired calling search space name in the list of calling search spaces that display in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.

Table 46-1 Translation Pattern Configuration Settings (continued)

Field	Description
Route Option	The Route Option designation indicates whether you want this translation pattern to be used for routing calls (such as 9.@ or 8[2-9]XX) or for blocking calls. Choose the Route this pattern or Block this pattern radio button. If you choose the Block this pattern radio button, you must choose the reason for which you want this translation pattern to block calls. Choose a value from the drop-down list box: • No Error • Unallocated Number • Call Rejected • Number Changed • Invalid Number Format • Precedence Level Exceeded
Provide Outside Dial Tone	Outside dial tone indicates that Cisco Unified CallManager routes the calls off the local network. Check this check box for each translation pattern that you consider to be off network.
Urgent Priority	Cisco Unified CallManager sets all translation patterns with urgent priority, and you cannot change the priority of the translation patterns.
Calling Party Transformations	
Use Calling Party's External Phone Number Mask	Check the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls.
Calling Party Transform Mask	Enter a transformation mask value. Valid entries for the NANP include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#); the uppercase characters A, B, C, and D; and blank. If this field is blank and the preceding field is not checked, no calling party transformation takes place. Refer to the “Adding a Route List” section on page 34-3 for more detailed information.
Prefix Digits (Outgoing Calls)	Enter prefix digits. Valid entries for the NANP include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#); the uppercase characters A, B, C, and D. Note The appended prefix digit does not affect which directory numbers route to the assigned device.

Table 46-1 Translation Pattern Configuration Settings (continued)

Field	Description
Calling Line ID Presentation	Cisco Unified CallManager uses calling line ID presentation (CLIP/CLIR) as a supplementary service to allow or restrict the originating caller's phone number on a call-by-call basis. Choose whether you want the Cisco Unified CallManager to allow or restrict the display of the calling party's phone number on the called party's phone display for this translation pattern. Choose <i>Default</i> if you do not want to change calling line ID presentation. Choose <i>Allowed</i> if you want Cisco Unified CallManager to allow the display of the calling number. Choose <i>Restricted</i> if you want Cisco Unified CallManager to block the display of the calling number. For more information about this field, see Table 17-6 in the “Calling Party Number Transformations Settings” section in the <i>Cisco Unified CallManager System Guide</i>. Note Use this parameter and the Connected Line ID Presentation parameter, in combination with the Ignore Presentation Indicators (internal calls only) device-level parameter, to configure call display restrictions. Together, these settings allow you to selectively present or restrict calling and/or connected line display information for each call. See the “Configuring a New User Device Profile” section on page 75-2 and Table 70-1 in the “Phone Configuration Settings” section on page 70-6 for information about the Ignore Presentation Indicators (internal calls only) field. For more information about call display restrictions, refer to the Call Display Restrictions chapter in the <i>Cisco Unified CallManager Features and Services Guide</i>.
Calling Name Presentation	Cisco Unified CallManager uses calling name presentation (CNIP/CNIR) as a supplementary service to allow or restrict the originating caller's name on a call-by-call basis. Choose whether you want the Cisco Unified CallManager to allow or restrict the display of the calling party's name on the called party's phone display for this translation pattern. Choose <i>Default</i> if you do not want to change calling name presentation. Choose <i>Allowed</i> if you want Cisco Unified CallManager to display the calling name information. Choose <i>Restricted</i> if you want Cisco Unified CallManager to block the display of the calling name information. For more information about this field, see Table 17-6 in the “Calling Party Number Transformations Settings” section in the <i>Cisco Unified CallManager System Guide</i>.

Table 46-1 Translation Pattern Configuration Settings (continued)

Field	Description
Connected Party Transformations	
Connected Line ID Presentation	Cisco Unified CallManager uses connected line ID presentation (COLP/COLR) as a supplementary service to allow or restrict the called party's phone number on a call-by-call basis. Choose whether you want Cisco Unified CallManager to allow or restrict the display of the connected party's phone number on the calling party's phone display for this translation pattern. Choose <i>Default</i> if you do not want to change the connected line ID presentation. Choose <i>Allowed</i> if you want to display the connected party's phone number. Choose <i>Restricted</i> if you want Cisco Unified CallManager to block the display of the connected party's phone number. For more information about this field, see Table 17-9 in the “Connected Party Presentation and Restriction Settings” section in the <i>Cisco Unified CallManager System Guide</i>.
Connected Name Presentation	Cisco Unified CallManager uses connected name presentation (CONP/CONR) as a supplementary service to allow or restrict the called party's name on a call-by-call basis. Choose whether you want Cisco Unified CallManager to allow or restrict the display of the connected party's name on the calling party's phone display for this translation pattern. Choose <i>Default</i> if you do not want to change the connected name presentation. Choose <i>Allowed</i> if you want to display the connected party's name. Choose <i>Restricted</i> if you want Cisco Unified CallManager to block the display of the connected party's name. For more information about this field, see Table 17-9 in the “Connected Party Presentation and Restriction Settings” section in the <i>Cisco Unified CallManager System Guide</i>.
Called Party Transformations	
Discard Digits	Choose the discard digits instructions that you want to be associated with this translation pattern. See the “Discard Digits Instructions” section in the <i>Cisco Unified CallManager System Guide</i> for more information. Note The discard digits that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box.
Called Party Transform Mask	Enter a transformation mask value. Valid entries for the NANP include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#); the uppercase characters A, B, C, and D; and blank. If the field is blank, no transformation takes place. The dialed digits get sent exactly as dialed.
Prefix Digits (Outgoing Calls)	Enter prefix digits. Valid entries for the NANP include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#); the uppercase characters A, B, C, and D; and blank. Note The appended prefix digit does not affect which directory numbers route to the assigned device.

Additional Information

See the [“Related Topics”](#) section on page 46-9.

Deleting a Translation Pattern

This section describes how to delete a translation pattern.

Procedure

-
- Step 1** Choose **Call Routing > Translation Pattern**.
- Step 2** Locate the translation pattern that you want to delete. See the [“Finding a Translation Pattern”](#) section on page 46-1.
- Step 3** Check the check box of the translation pattern that you want to delete and click **Delete Selected**.
A message displays that states that you cannot undo this action.
- Step 4** To delete the translation pattern, click **OK** or to cancel the deletion, click **Cancel**.

**Caution**

Check carefully to ensure that you are deleting the correct translation pattern before you initiate this action. You cannot retrieve deleted translation patterns. If you accidentally delete a translation pattern, you must rebuild it.

**Tip**

You can also delete a translation pattern by locating and displaying the translation pattern that you want to delete and clicking **Delete**.

Additional Information

See the [“Related Topics”](#) section on page 46-9.

Related Topics

- [Finding a Translation Pattern, page 46-1](#)
- [Configuring a Translation Pattern, page 46-3](#)
- [Translation Pattern Configuration Settings, page 46-4](#)
- [Deleting a Translation Pattern, page 46-9](#)
- [Understanding Route Plans, Cisco Unified CallManager System Guide](#)



Call Park

The Call Park feature allows you to place a call on hold, so it can be retrieved from another phone in the Cisco Unified CallManager system (for example, a phone in another office or in a conference room). If you are on an active call at your phone, you can park the call to a call park extension by pressing the Park softkey or the Call Park button. Someone on another phone in your system can then dial the call park extension to retrieve the call.

For more information on how to use and configure the Call Park feature, refer to the [Call Park](#) chapter in the *Cisco Unified CallManager Features and Services Guide*.



Call Pickup Group

The feature, call pickup group, allows you to answer a call that comes in on a directory number other than your own. When you hear an incoming call ringing on another phone, you can redirect the call to your phone by using this feature.

Cisco IP Phones provide three types of call pickup:

- Call pickup allows users to pick up incoming calls within their own group. Cisco Unified CallManager automatically dials the appropriate call pickup group number when a user activates this feature on a phone.
- Group call pickup allows users to pick up incoming calls in another group. Users must dial the appropriate call pickup group number when they activate this feature on a phone.
- Other group call pickup allow users to pick up incoming calls in a group that is associated with their own group. When a phone rings in a group that is associated with the user's group, Cisco Unified CallManager automatically searches for the incoming call in the associated groups when they activate this feature on a phone.

For more information on how to use and configure the Call Pickup Group feature, refer to the [Call Pickup Group](#) chapter in the *Cisco Unified CallManager Features and Services Guide*.



Directory Number Configuration

The following sections provide information about working with and configuring directory numbers (DNs) in Cisco Unified CallManager Administration:

- [Directory Number Configuration Overview, page 49-1](#)
- [Finding a Directory Number, page 49-2](#)
- [Configuring a Directory Number, page 49-2](#)
- [Removing a Directory Number from a Phone, page 49-4](#)
- [Creating a Cisco Unity or Cisco Unity Connection Voice Mailbox, page 49-4](#)
- [Directory Number Configuration Settings, page 49-6](#)
- [Related Topics, page 49-23](#)

Directory Number Configuration Overview

Using Cisco Unified CallManager Administration, configure and modify directory numbers (DNs) that are assigned to specific phones. These sections provide instructions for working with directory numbers.

Use the Directory Number Configuration window to perform the following tasks:

- Add or remove directory numbers.
- Configure call forward, call pickup, call waiting, and multilevel precedence and preemption (MLPP) options.
- Set the display text that appears on the called party phone when a call is placed from a line.
- Configure ring settings.
- Configure Cisco Unity or Cisco Unity Connection subscriber voice mailboxes.

Additional Topics

See the [“Related Topics” section on page 49-23](#).

Finding a Directory Number

Use the following procedure to find a directory number (DN).

Procedure

Step 1 Choose **Call Routing > Directory Number**.

The Find and List Directory Numbers window displays.

Step 2 From the first Find Directory Number drop-down list box, choose the field that you want to use to search for directory numbers; for example, Directory Number, Route Partition, or Description.



Note To find all directory numbers that are registered in the database, do not enter any search text and click **Find**. A list of directory numbers that matches your search criteria displays.

Step 3 From the second Find Directory Number drop-down list box, choose a search pattern for your text search; for example, begins with, contains, or ends with.

Step 4 Specify the appropriate search text, if applicable, and click **Find**.

The records that match your search criteria display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.



Tip To search for directory numbers within the search results, click the **Search Within Results** check box and enter your search criteria as described in this step.



Note You can delete multiple directory numbers by checking the check boxes next to the appropriate directory numbers and clicking **Delete Selected**. You can delete all the directory numbers in the window by clicking **Select All** and then clicking **Delete Selected**.

Step 5 From the list of records that match your search criteria, click the name of the directory number that you want to view.

The Directory Number Configuration window displays with the directory number that you choose.

Additional Topics

See the [“Related Topics” section on page 49-23](#).

Configuring a Directory Number

Follow these instructions to add or update a directory number (DN). You can configure the call forward, call pickup, and MLPP phone features while you are adding the directory number.

**Tip**

You can assign patterns to directory numbers; for example, 352XX. To avoid user confusion when you assign a pattern to a directory number, add text or digits to the DN configuration fields, Line Text Label, Display (Internal Caller ID), and External Phone Number Mask. (These fields display for a directory number only after you add the directory number *and* you associate the directory number with a phone.)

For example, add the user's name to the line text label and internal caller ID, but add the outside line number to the external number mask, so when the calling information displays, it says John Chan, not 352XX.

Procedure

Step 1 Choose **Call Routing > Directory Number**.

The Find and List Directory Numbers window displays.

Step 2 To locate a specific directory number, enter search criteria and click **Find**.

A list of directory numbers that match the search criteria displays.

Step 3 Perform one of the followings tasks:

- To add a directory number, click the **Add New** button to add a new directory number. The Directory Number Configuration window displays.

**Note**

The Phone Configuration window provides an alternate method for adding a directory number. Use the **Device > Phone** menu option and create a new phone or search for an existing phone. After you create the new phone or display the existing phone, click either the *Line [1] - Add a new DN* or *Line [2] - Add a new DN* link in the Association Information area on the left side of the Phone Configuration window. The Directory Number Configuration window displays, and you can continue with [Step 4](#) of this procedure.

- To update a directory number, click the directory number that you want to update. The Directory Number Configuration window displays.

Step 4 Update the appropriate settings as described in [Table 49-1](#).

Step 5 Click **Save**.

Step 6 Click **Reset Phone**. For more information, refer to the [“Resetting a Phone” section on page 70-4](#).

**Tip**

If you need more than two lines, you can increase the lines by modifying the phone button template for the phone type (such as Cisco IP Phone model 7960). Some phone types, however, only support one or two lines (such as Cisco IP Phone model 7902).

**Note**

Restart devices as soon as possible. During this process, the system may drop calls on gateways.

Additional Topics

See the [“Related Topics” section on page 49-23](#).

Removing a Directory Number from a Phone

Perform the following procedure to remove a directory number (DN) from a specific phone.

Before You Begin

If you try to remove a directory number that is in use, Cisco Unified CallManager displays a message. To find out which line groups are using the directory number, click the **Dependency Records** link from the Directory Number Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, refer to the [“Accessing Dependency Records” section on page A-2](#).

When you remove a directory number from a phone, the number still exists within Cisco Unified CallManager. To see a list of directory numbers that are not associated with phones, use the Route Plan Report menu option. For more information, refer to the [“Deleting Unassigned Directory Numbers” section on page 51-3](#).

Procedure

-
- Step 1** Choose **Device > Phone**.
The Find and List Phones window displays.
 - Step 2** To locate a specific phone, enter the search criteria and click **Find**.
A list of phones that match the search criteria displays.
 - Step 3** Choose the device name that contains the directory number that you want to remove.
The Phone Configuration window displays.
 - Step 4** In the Association Information area on the left, choose the line that you want to remove.
The Directory Number Configuration window displays.
 - Step 5** In the Associated Devices pane, choose the device name of the phone from which you want to remove this directory number.
 - Step 6** Click the down arrow below the Associated Devices pane.
The phone name moves to the Dissociate Devices pane.
 - Step 7** Click the **Save** button at the bottom of the Directory Number Configuration window.
The Phone Configuration window displays with the directory number removed. The change gets automatically applied to the phone; however, you can click **Reset Phone**. For more information, refer to the [“Resetting a Phone” section on page 70-4](#).
-

Additional Topics

See the [“Related Topics” section on page 49-23](#).

Creating a Cisco Unity or Cisco Unity Connection Voice Mailbox

The “Create Cisco Unity User” link on the Directory Number Configuration window allows administrators to create individual Cisco Unity and Cisco Unity Connection voice mailboxes from Cisco Unified CallManager Administration.

Before You Begin

- Ensure the Unity administrator installs the appropriate software, which includes installing the Voice Mailbox asp page on the Cisco Unified CallManager server. Refer to the *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.0* or the *Cisco Unified CallManager 5.0 SCCP Integration Guide for Cisco Unity Connection 2.1*.
- You must configure Cisco Unified CallManager for voice-messaging service. Refer to [Cisco Unity Configuration Checklist](#) in the *Cisco Unified CallManager System Guide*.
- You must configure Cisco Unity or Cisco Unity Connection servers. Refer to the applicable Cisco Unity installation guide.
- Ensure the Cisco Unity or Cisco Unity Connection Cisco Unified CallManager Integrated Voice Mailbox Configuration is enabled on the Cisco Unity or Cisco Unity Connection server. Refer to the *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.0* or the *Cisco Unified CallManager 5.0 SCCP Integration Guide for Cisco Unity Connection 2.1*.
- Ensure the Cisco RIS Data Collector service is activated. Refer to the *Cisco Unified CallManager Serviceability System Guide* and the *Cisco Unified CallManager Serviceability Administration Guide*.
- On the Directory Number configuration window, ensure the Voice Mail Profile setting is configured and contains a pilot number, or the Voice Mail Profile setting should be configured to *None*. If the Voice Mail Profile is set to No Voice Mail, the “Create Cisco Unity User” link does not display.

**Note**

The End User Configuration window also includes the “Create Cisco Unity User” link.

Procedure

- Step 1** Choose **Call Routing > Directory Number** and click **Add New**.
- Step 2** Enter the appropriate settings in [Table 49-1](#).
- Step 3** From the Related Links drop-down list box, in the upper, right corner of the window, choose the “Create Cisco Unity User” link and click **Go**.
The Add Cisco Unity User dialog box displays.
- Step 4** From the Application Server drop-down list box, choose the Cisco Unity or Cisco Unity Connection server on which you want to create a Cisco Unity user and click **Next**.
- Step 5** From the Subscriber Template drop-down list box, choose the subscriber template that you want to use.
- Step 6** Click **Save**.

The Cisco Unity or Cisco Unity Connection mailbox gets created. The link, in Related Links, changes to “Edit Cisco Unity User” in the Directory Number Configuration window.

From Cisco Unity Administration, you can now see the mailbox that you created. Refer to the Cisco Unity or Cisco Unity Connection documentation.

**Note**

Cisco Unity monitors the syncing of data from Cisco Unified CallManager. You can configure the sync time in Cisco Unity Administration under Tools (Import CallManager Users, Sync CallManager). Refer to the Cisco Unity documentation.

Additional Topics

See the [“Related Topics”](#) section on page 49-23.

Directory Number Configuration Settings

Table 49-1 describes the fields that are available in the Directory Number Configuration window.

Table 49-1 *Directory Number Configuration Settings*

Field	Description
Directory Number Information	
Directory Number	Enter a dialable phone number. Values can include numeric characters and route pattern wildcards and special characters except for (.) and (@). Note When a pattern is used as a directory number, the display on the phone and the caller ID that displays on the dialed phone will both contain characters other than digits. To avoid this, Cisco recommends that you provide a value for Display (Internal Caller ID), Line text label, and External phone number mask. The directory number that you enter can appear in more than one partition. Note If a JTAPI or TAPI application controls or monitors a device, you should not configure multiple instances of the same DN (with different partitions) on that device.
Route Partition	Choose the partition to which the directory number belongs. Make sure that the directory number that you enter in the Directory Number field is unique within the partition that you choose. If you do not want to restrict access to the directory number, choose <None> for the partition. You can configure the number of partitions that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more partitions exist than the Max List Box Items enterprise parameter specifies, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Partition window. Enter a partial partition name in the List items where Name contains field. Click the desired partition name in the list of partitions that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.
Description	Enter a description of the directory number and route partition.

Table 49-1 **Directory Number Configuration Settings (continued)**

Field	Description
Alerting Name	Enter a name that you want to display on the phone of the caller. This setting, which supports the Identification Services for the QSIG protocol, applies to shared and nonshared directory numbers. If you configure an alerting name for a directory number with shared-line appearances, when the phone rings at the terminating PINX, the system performs the following tasks: • Forwards the name of the caller that is assigned to the directory number. • Applies the Connected Name Restrictions (CONR) that are configured for the translation pattern (if restrictions exist); the originating PINX may modify the CONR, depending on the route pattern configuration. If you do not configure an alerting name, “Name Not Available” may display on the caller phone. If you do not enter a name for the Display (Internal Caller ID) field, the information in the Alerting Name field displays in the Display (Internal Caller ID) field.
ASCII Alerting Name	This field provides the same information as the <i>Alerting Name</i> field, but you must limit input to ASCII characters. Devices that do not support Unicode (internationalized) characters display the content of the <i>Alerting Name ASCII</i> field.
Active	To view this check box on the Directory Number Configuration window, access an unassigned directory number from the Route Plan Report window. Checking this check box allows calls to this DN to be forwarded (if forwarding is configured). If check box is not checked, Cisco Unified CallManager ignores the DN.
Allow Control of Device from CTI	Check this check box to allow CTI to control and monitor a line on a device with which this directory number is associated If the directory number specifies a shared line, ensure the check box is enabled as long as at least one associated device specifies a combination of device type and protocol that CTI supports.
Line Group	From this drop-down list box, choose a line group with which to associate this DN. To edit or view the line group information for a line group, choose a line group from the drop-down list box and click the Edit Line Group button. See the “Line Group Configuration” section on page 36-1 for more information about configuring line groups.

Table 49-1 *Directory Number Configuration Settings (continued)*

Field	Description
Associated Devices	After you associate this DN with a phone(s), this pane displays the phones with which this DN is associated. To edit a phone with which this DN is associated, choose a device name in the Associated Devices pane and click the Edit Device button. The Phone Configuration window displays for the device that you choose. See the “Cisco Unified IP Phone Configuration” chapter for more information about configuring phones. To edit a line appearance that has been defined for this DN, choose a device name in the Associated Devices pane and click the Edit Line Appearance button. The Directory Number Configuration window refreshes to show the line appearance for this DN on the device that you choose.
Dissociate Devices	If you choose to dissociate a DN from a device, this pane displays the device(s) from which you dissociate this DN.
Directory Number Settings	
Voice Mail Profile	Choose from list of Voice Mail Profiles that the Voice Mail Profile Configuration defines. The first option specifies <None>, which represents the current default Voice Mail Profile that is configured in the Voice Mail Profile Configuration.

Table 49-1 **Directory Number Configuration Settings (continued)**

Field	Description
Calling Search Space	From the drop-down list box, 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 are using this directory number. For configuration information about calling search space for directory numbers, see the “Calling Search Space” section on page 49-23. Changes result in an update of the numbers that the Call Pickup Group field lists. You can configure calling search space for Forward All, Forward Busy, Forward No Answer, Forward No Coverage, and Forward on Failure directory numbers. The value that you choose applies to all devices that are using this directory number. You must configure either primary Forward All Calling Search Space or Secondary Forward All Calling Search Space or both for Call Forward All to work properly. The system uses these concatenated fields (Primary CFA CSS + Secondary CFA CSS) to validate the CFA destination and forward the call to the CFA destination. Note If the system is using partitions and calling search spaces, Cisco recommends that the other call forward calling search spaces are configured as well. When a call is forwarded or redirected to the call forward destination, the configured call forward calling search space gets used to forward the call. If the forward calling search space is None, the forward operation may fail if the system is using partitions and calling search spaces. For example, if the Forward Busy Destination is configured, the Forward Busy Calling Search Space should also be configured. If the Forward Busy Calling Search Space is not configured and the Forward Busy destination is in a partition, the forward operation will fail. When you forward calls by using the Cisco IP Phone User Options windows or the CFwdAll softkey on the phone, the automatic combination of the line CSS and device CSS does not get used. Only the configured Primary CFA CSS and Secondary CFA CSS gets used. If both of these fields are <None>, the combination results in two null partitions, which will cause the operation to fail. If you want to restrict users from forwarding calls on their phones, you must choose a restrictive calling search space from the Forward All Calling Search Space field. For more information, refer to Partitions and Calling Search Spaces, in the <i>Cisco Unified CallManager System Guide</i>.

Table 49-1 **Directory Number Configuration Settings (continued)**

Field	Description
Presence Group	Configure this field with the Presence feature. From the drop-down list box, choose a Presence group for this directory number. The selected group specifies the devices, end users, and application users that can monitor this directory number. The default value for Presence Group specifies Standard Presence group, configured with installation. Presence groups that are configured in Cisco Unified CallManager Administration also appear in the drop-down list box. Presence authorization works with presence groups to allow or block presence requests between groups. Refer to the “Presence” chapter in the <i>Cisco Unified CallManager Features and Services Guide</i> for information about configuring permissions between groups
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.
User Hold Audio Source	Choose the audio source that plays when a user initiates a hold action.
Network Hold Audio Source	Choose the audio source that plays when the network initiates a hold action.
Auto Answer	Choose one of the following options to activate the Auto Answer feature for this directory number: • Auto Answer Off <Default> • Auto Answer with Headset • Auto Answer with Speakerphone Note Make sure that the headset or speakerphone is not disabled when you choose Auto Answer with headset or Auto Answer with speakerphone. Note Do not configure Auto Answer for devices that have shared lines.

Table 49-1 **Directory Number Configuration Settings (continued)**

Field	Description
Call Forward and Call Pickup Settings	
Forward All	The settings in this row of fields specify the forwarding treatment for calls to this directory number if the directory number is set to forward all calls. The Calling Search Space field gets used to validate the Forward All destination that is entered when the user activates Call Forward All from the phone. This field also gets used to redirect the call to the Call Forward All destination. Specify the following values: - Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window. Note When this check box is checked, Cisco Unified CallManager ignores the settings in the Destination box and Calling Search Space. - Destination—This setting indicates the directory number to which all calls are forwarded. Use any dialable phone number, including an outside destination. - Calling Search Space—This setting applies to all devices that are using this directory number.
Secondary Calling Search Space for Forward All	Because call forwarding is a line-based feature, in cases where the device calling search space is unknown, the system uses only the line calling search space to forward the call. If the line calling search space is restrictive and not routable, the forward attempt fails. Addition of a secondary calling search space for Call Forward All provides a solution to enable forwarding. The primary calling search space for Call Forward All and secondary calling search space for Call Forward All get concatenated (Primary CFA CSS + Secondary CFA CSS). Call Forward All gets processed. Cisco Unified CallManager uses this combination to validate the CFA destination and to forward the call.

Table 49-1 *Directory Number Configuration Settings (continued)*

Field	Description
Forward Busy Internal	The settings in this row of fields specify the forwarding treatment for internal calls to this directory number if the directory number is busy. The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Specify the following values: - Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window for internal calls. Note When this check box is checked, the calling search space of the voice mail pilot gets used. Cisco Unified CallManager ignores the settings in the Destination box and Calling Search Space. If you set Calling Search Space to None, the calling search space of the originating device gets used. Note When this check box is checked for internal calls, the system automatically checks the Voice Mail check box for external calls. If you do not want external calls to forward to the voice-messaging system, you must uncheck the Voice Mail check box for external calls. - Destination—Use any dialable phone number, including an outside destination. Note When you enter a destination value for internal calls, the system automatically copies this value to the Destination field for external calls. If you want external calls to forward to a different destination, you must enter a different value in the Destination field for external calls. - Calling Search Space—This setting applies to all devices that are using this directory number. Note When you choose a Calling Search Space for internal calls, the system automatically copies this setting to the Calling Search Space setting for external calls. If you want external calls to forward to a different calling search space, you must choose a different setting in the Calling Search Space drop-down list box for external calls.

Table 49-1 **Directory Number Configuration Settings (continued)**

Field	Description
Forward Busy External	The settings in this row of fields specify the forwarding treatment for external calls to this directory number if the directory number is busy. The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Specify the following values: - Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window for external calls. Note When this check box is checked, the calling search space of the voice mail pilot gets used. Cisco Unified CallManager ignores the settings in the Destination box and Calling Search Space. If you set Calling Search Space to None, the calling search space of the originating device gets used. Note When the Voice Mail check box is checked for internal calls, the system automatically checks the Voice Mail check box for external calls. If you do not want external calls to forward to the voice-messaging system, you must uncheck the Voice Mail check box for external calls. - Destination—Use any dialable phone number, including an outside destination. Note When you enter a destination value for internal calls, the system automatically copies this value to the Destination field for external calls. If you want external calls to forward to a different destination, you must enter a different value in the Destination field for external calls. - Calling Search Space—This setting applies to all devices that are using this directory number. Note When you choose a Calling Search Space for internal calls, the system automatically copies this setting to the Calling Search Space setting for external calls. If you want external calls to forward to a different calling search space, you must choose a different setting in the Calling Search Space drop-down list box for external calls.

Table 49-1 **Directory Number Configuration Settings (continued)**

Field	Description
Forward No Answer Internal	The settings in this row of fields specify the forwarding treatment for internal calls to this directory number if the directory number does not answer. The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Specify the following values: - Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window. Note When this check box is checked, the calling search space of the voice mail pilot gets used. Cisco Unified CallManager ignores the settings in the Destination box and Calling Search Space. If you set Calling Search Space to None, the calling search space of the originating device gets used. Note When this check box is checked for internal calls, the system automatically checks the Voice Mail check box for external calls. If you do not want external calls to forward to the voice-messaging system, you must uncheck the Voice Mail check box for external calls. - Destination—This setting indicates the directory number to which an internal call is forwarded when the call is not answered. Use any dialable phone number, including an outside destination. Note When you enter a destination value for internal calls, the system automatically copies this value to the Destination field for external calls. If you want external calls to forward to a different destination, you must enter a different value in the Destination field for external calls. - Calling Search Space—This setting applies to all devices that are using this directory number. Note When you choose a Calling Search Space for internal calls, the system automatically copies this setting to the Calling Search Space setting for external calls. If you want external calls to forward to a different calling search space, you must choose a different setting in the Calling Search Space drop-down list box for external calls.

Table 49-1 **Directory Number Configuration Settings (continued)**

Field	Description
Forward No Answer External	The settings in this row of fields specify the forwarding treatment for external calls to this directory number if the directory number does not answer. The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Specify the following values: - Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window. Note When this check box is checked, the calling search space of the voice mail pilot gets used. Cisco Unified CallManager ignores the settings in the Destination box and Calling Search Space. If you set Calling Search Space to None, the calling search space of the originating device gets used. Note When this check box is checked for internal calls, the system automatically checks the Voice Mail check box for external calls. If you do not want external calls to forward to the voice-messaging system, you must uncheck the Voice Mail check box for external calls. - Destination—This setting indicates the directory number to which an external call is forwarded when the call is not answered. Use any dialable phone number, including an outside destination. Note When you enter a destination value for internal calls, the system automatically copies this value to the Destination field for external calls. If you want external calls to forward to a different destination, you must enter a different value in the Destination field for external calls. - Calling Search Space—This setting applies to all devices that are using this directory number. Note When you choose a Calling Search Space for internal calls, the system automatically copies this setting to the Calling Search Space setting for external calls. If you want external calls to forward to a different calling search space, you must choose a different setting in the Calling Search Space drop-down list box for external calls.

Table 49-1 *Directory Number Configuration Settings (continued)*

Field	Description
Forward No Coverage Internal	The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Specify the following values: - Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window. Note When this check box is checked, Cisco Unified CallManager ignores the settings in the Destination box and Calling Search Space. When this check box is checked for internal calls, the system automatically checks the Voice Mail check box for external calls. If you do not want external calls to forward to the voice-messaging system, you must uncheck the Voice Mail check box for external calls. - Destination—This setting specifies the directory number to which an internal nonconnected call is forwarded when an application that controls that directory number fails. Use any dialable phone number, including an outside destination. Note When you enter a destination value for internal calls, the system automatically copies this value to the Destination field for external calls. If you want external calls to forward to a different destination, you must enter a different value in the Destination field for external calls. - Calling Search Space—This setting applies to all devices that are using this directory number. Note When you choose a Calling Search Space for internal calls, the system automatically copies this setting to the Calling Search Space setting for external calls. If you want external calls to forward to a different calling search space, choose a different setting in the Calling Search Space for external calls.

Table 49-1 **Directory Number Configuration Settings (continued)**

Field	Description
Forward No Coverage External	The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Specify the following values: - Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window. Note When this check box is checked, Cisco Unified CallManager ignores the settings in the Destination box and Calling Search Space. When this check box is checked for internal calls, the system automatically checks the Voice Mail check box for external calls. If you do not want external calls to forward to the voice-messaging system, you must uncheck the Voice Mail check box for external calls. - Destination—This setting specifies the directory number to which an internal nonconnected call is forwarded when an application that controls that directory number fails. Use any dialable phone number, including an outside destination. Note When you enter a destination value for internal calls, the system automatically copies this value to the Destination field for external calls. If you want external calls to forward to a different destination, you must enter a different value in the Destination field for external calls. - Calling Search Space—This setting applies to all devices that are using this directory number. Note When you choose a Calling Search Space for internal calls, the system automatically copies this setting to the Calling Search Space setting for external calls. If you want external calls to forward to a different calling search space, choose a different setting in the Calling Search Space for external calls.

Table 49-1 *Directory Number Configuration Settings (continued)*

Field	Description
Forward on CTI Failure	This field applies only to CTI route points and CTI ports. The settings in this row specify the forwarding treatment for external calls to this CTI route point or CTI port if the CTI route point or CTI port fails. Specify the following values: - Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window. Note When this check box is checked, Cisco Unified CallManager ignores the settings in the Destination box and Calling Search Space. When this check box is checked for internal calls, the system automatically checks the Voice Mail check box for external calls. If you do not want external calls to forward to the voice-messaging system, you must uncheck the Voice Mail check box for external calls. - Destination—This setting specifies the directory number to which an internal nonconnected call is forwarded when an application that controls that directory number fails. Use any dialable phone number, including an outside destination. Note When you enter a destination value for internal calls, the system automatically copies this value to the Destination field for external calls. If you want external calls to forward to a different destination, you must enter a different value in the Destination field for external calls. - Calling Search Space—This setting applies to all devices that are using this directory number. Note When you choose a Calling Search Space for internal calls, the system automatically copies this setting to the Calling Search Space setting for external calls. If you want external calls to forward to a different calling search space, choose a different setting in the Calling Search Space for external calls.
No Answer Ring Duration (seconds)	Used in conjunction with Call Forward No Answer Destination, this field sets the timer for how long the phone will ring before it gets forwarded. Leave this setting blank to use the value that is set in the Cisco CallManager service parameter, Forward No Answer Timer.  Caution By default, Cisco Unified CallManager makes the time for the T301 timer longer than the No Answer Ring Duration time; if the set time for the T301 timer expires before the set time for the No Answer Ring Duration expires, the call ends, and no call forwarding can occur. If you choose to do so, you can configure the time for the No Answer Ring Duration to be greater than the time for the T301 timer. For information on the T301 timer, choose System > Service Parameters; choose the server, the Cisco CallManager service, and then the parameter in the window that displays.

Table 49-1 **Directory Number Configuration Settings (continued)**

Field	Description
Call Pickup Group	Choose the number that can be dialed to answer calls to this directory number (in the specified partition).
MLPP Alternate Party Settings	
Target (Destination)	Enter the number to which MLPP precedence calls should be directed if this directory number receives a precedence call and neither this number nor its call forward destination answers the precedence call. Values can include numeric characters, octothorpe (#), and asterisk (*).
MLPP Calling Search Space	From the drop-down list box, choose the calling search space to associate with the MLPP alternate party target (destination) number. For configuration information about calling search space for directory numbers, see the “Calling Search Space” section on page 49-23 .
MLPP No Answer Ring Duration (seconds)	Enter the number of seconds (between 4 and 60) after which an MLPP precedence call will be directed to this directory number’s alternate party if this directory number and its call-forwarding destination have not answered the precedence call. Leave this setting blank to use the value that is set in the Cisco Unified CallManager enterprise parameter, Precedence Alternate Party Timeout.
Line [number] on Device [device name]	
Note These fields display only after you associate this directory number with a device.	
Display (Internal Caller ID)	Leave this field blank to have the system display the extension. Use a maximum of 30 alphanumeric characters. Typically, use the user name or the directory number (if using the directory number, the person receiving the call may not see the proper identity of the caller). Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.)
ASCII Display (Internal Caller ID)	This field provides the same information as the <i>Display (Internal Caller ID)</i> field, but you must limit input to ASCII characters. Devices that do not support Unicode (internationalized) characters display the content of the <i>ASCII Display (Internal Caller ID)</i> field. Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.)

Table 49-1 **Directory Number Configuration Settings (continued)**

Field	Description
Line Text Label	Use this field only if you do not want the directory number to show on the line appearance. Enter text that identifies this directory number for a line/phone combination. Suggested entries include boss's name, department's name, or other appropriate information to identify multiple directory numbers to secretary/assistant who monitors multiple directory numbers. Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.)
ASCII Line Text Label	This field provides the same information as the <i>Line Text Label</i> field, but you must limit input to ASCII characters. Devices that do not support Unicode (internationalized) characters display the content of the <i>ASCII Line Text Label</i> field. Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.)
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. For example, if you specify a mask of 972813XXXX, an external call from extension 1234 displays a caller ID number of 9728131234. Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.)
Message Waiting Lamp Policy	Use this field to configure the handset lamp illumination policy. Choose one of the following options: • Use System Policy (The directory number refers to the service parameter "Message Waiting Lamp Policy" setting.) • Light and Prompt • Prompt Only • Light Only • None Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.)

Table 49-1 **Directory Number Configuration Settings (continued)**

Field	Description
Ring Setting (Phone Idle)	Use this field to configure the ring setting for the line appearance when an incoming call is received and no other active calls exist on that device. Choose one of the following options: • Use system default • Disable • Flash only • Ring once • Ring Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.) Note Turning on MLPP Indication (at the enterprise parameter, device pool, or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device.
Ring Setting (Phone Active)	From the drop-down list box, choose the ring setting that is used when this phone has another active call on a different line. Choose one of the following options: • Use system default • Disable • Flash only • Ring once • Ring • Beep only Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.) Note Turning on MLPP Indication (at the enterprise parameter, device pool, or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device.

Table 49-1 **Directory Number Configuration Settings (continued)**

Field	Description
Multiple Call/Call Waiting Settings on Device [device name]	
Note These fields display only after you associate this directory number with a device.	
Maximum Number of Calls	You can configure up to 200 calls for a line on a device, with the limiting factor being the total number of calls that are configured on the device. As you configure the number of calls for one line, the calls that are available for another line decrease. The default specifies 4. If the phone does not allow multiple calls for each line, the default specifies 2. For CTI route points, you can configure up to 10,000 calls for each port. The default specifies 5000 calls. Use this field in conjunction with the Busy Trigger field.  Note Although the default specifies 5000 calls for maximum number of active calls that can be configured on a CTI route point, Cisco recommends that you set the maximum number of calls to no more than 200 per route point. This will prevent system performance degradation. If the CTI application needs more than 200 calls, Cisco recommends that you configure multiple CTI route points. Tip To review how this setting works for devices with shared line appearances, refer to “Shared Line Appearance” in the <i>Cisco Unified CallManager System Guide</i>.
Busy Trigger	This setting, which works in conjunction with Maximum Number of Calls and Call Forward Busy, determines the maximum number of calls to be presented at the line. If maximum number of calls is set for 50 and the busy trigger is set to 40, incoming call 41 gets rejected with a busy cause (and will get forwarded if Call Forward Busy is set). If this line is shared, all the lines must be busy before incoming calls get rejected. Use this field in conjunction with Maximum Number of Calls for CTI route points. The default specifies 4500 calls. Tip To review how this setting works for devices with shared line appearances, refer to “Shared Line Appearance” in the <i>Cisco Unified CallManager System Guide</i>.
Forwarded Call Information Display on Device [device name]	
Note These fields display only after you associate this directory number with a device.	
Caller Name	Checking this check box will cause the caller name to display upon call forward.
Caller Number	Checking this check box will cause the caller number to display upon call forward.

Table 49-1 **Directory Number Configuration Settings (continued)**

Field	Description
Redirected Number	Checking this check box will cause the number that was redirected to display upon call forward.
Dialed Number	Checking this check box will cause the original dialed number to display upon call forward.

Calling Search Space

You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the Max List Box Items enterprise parameter specifies, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Calling Search Space window. Enter a partial calling search space name in the **List items where Name contains** field. Click the desired calling search space name in the list of calling search spaces that displays in the **Select item to use** box and click **OK**.

**Note**

To set the maximum list box items, choose **System > Enterprise Parameters** and choose **CCMAdmin Parameters**.

Additional Topic

See the “[Related Topics](#)” section on page 49-23.

Related Topics

- [Directory Number Configuration Overview, page 49-1](#)
- [Finding a Directory Number, page 49-2](#)
- [Configuring a Directory Number, page 49-2](#)
- [Removing a Directory Number from a Phone, page 49-4](#)
- [Creating a Cisco Unity or Cisco Unity Connection Voice Mailbox, page 49-4](#)
- [Directory Number Configuration Settings, page 49-6](#)
- [Understanding Directory Numbers, Cisco Unified CallManager System Guide](#)
- [Directory Number Configuration Checklist, Cisco Unified CallManager System Guide](#)
- [Line Group Configuration, page 36-1](#)
- [Deleting Unassigned Directory Numbers, page 51-3](#)
- [Gateway Configuration, page 69-1](#)
- [Resetting a Phone, page 70-4](#)
- [Finding a Phone, page 70-29](#)
- [Configuring Cisco Unified IP Phones, page 70-2](#)
- [Cisco Unified IP Phones, Cisco Unified CallManager System Guide](#)
- [Phone Features, Cisco Unified CallManager System Guide](#)
- [Phone Configuration Checklist, Cisco Unified CallManager System Guide](#)

- [Cisco Unity Cisco Unified CallManager Integrated Mailbox Configuration](#), *Cisco Unified CallManager System Guide*
- [Cisco Unity Configuration Checklist](#), *Cisco Unified CallManager System Guide*
- [Presence](#), *Cisco Unified CallManager Features and Services Guide*



Meet-Me Number/Pattern Configuration

Meet-Me conferences require an allocation of directory numbers. Cisco Unified CallManager Administration provides the Meet-Me conference directory number range to users, so they can access the feature.

Finding a Meet-Me Number/Pattern

Because you might have several meet-me numbers/patterns in your network, Cisco Unified CallManager lets you locate specific meet-me numbers/patterns on the basis of specific criteria. Use the following procedure to locate meet-me numbers/patterns.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your meet-me number/pattern search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your meet-me number/pattern search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Call Routing > Meet-Me Number/Pattern**.

The Find and List Meet-Me Numbers window displays. Use the two drop-down list boxes to search for a meet-me number/pattern.

Step 2 From the first Find Number/Pattern where drop-down list box, choose one of the following criteria:

- Number
- Partition
- Description



Note

The criterion that you choose in this drop-down list box specifies how the list of meet-me numbers/patterns that your search generates will be sorted. For example, if you choose Partition, the Partition column will display as the left column of the results list.

From the second Find Number/Pattern where drop-down list box, choose one of the following criteria:

- begins with
- contains

- ends with
- is exactly
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Tip To find all meet-me numbers/patterns that are registered in the database, click **Find** without entering any search text.

A list of discovered meet-me numbers/patterns displays by

- Meet-Me Number/Pattern
- Partition
- Description



Note You can delete multiple meet-me numbers/patterns from the Find and List Meet-Me Numbers window by checking the check boxes next to the appropriate meet-me numbers/patterns and clicking **Delete Selected**. You can delete all meet-me numbers/patterns in the window by checking the check box in the Matching records title bar and clicking **Delete Selected**.

Step 4 From the list of records, click the number, associated partition, or description that matches your search criteria.

The window displays the meet-me number/pattern that you choose.

Additional Topics

See the [“Related Topics” section on page 50-5](#).

Configuring a Meet-Me Number/Pattern

This section describes how to add, copy and update a Meet-Me Number/Pattern.

Before You Begin

Make sure that the following prerequisites are met before proceeding with the steps:

- Configure the servers. Refer to the [“Server Configuration” section on page 2-1](#).
- Configure the device pools. Refer to the [“Device Pool Configuration” section on page 9-1](#).

Procedure

-
- Step 1** Choose **Call Routing > Meet-Me Number/Pattern**.
- Step 2** Perform one of the followings tasks:
- To copy an existing Meet-Me Number/Pattern, locate the appropriate Meet-Me Number/Pattern as described in [“Finding a Meet-Me Number/Pattern” section on page 50-1](#). Click the Meet-Me Number/Pattern that you want to copy. The Meet-Me Number/Pattern Configuration window displays. Click **Copy**, and continue with [Step 3](#).
 - To add a Meet-Me Number/Pattern, click the **Add New** button, and continue with [Step 3](#).
 - To update an existing Meet-Me Number/Pattern, locate the appropriate Meet-Me Number/Pattern as described in [“Finding a Meet-Me Number/Pattern” section on page 50-1](#). Click the Meet-Me Number/Pattern that you want to update, and continue with [Step 3](#).



Note You can change the number or pattern as needed (example, changing 5000 to 500X).

- Step 3** Enter the appropriate settings as described in [Table 50-1](#).
- Step 4** Click **Save**.
-

Additional Topics

See the [“Related Topics” section on page 50-5](#).

Meet-Me Number/Pattern Configuration Settings

[Table 50-1](#) describes the meet-me number/pattern configuration settings.

Table 50-1 *Meet-Me Number/Pattern Configuration Settings*

Field	Description
Directory Number or Pattern	Enter a Meet-Me Numbers/pattern or a range of numbers (such as 8000 to 8009).
Description	Enter up to 30 alphanumeric characters for a description of the meet-me number/pattern.

Table 50-1 *Meet-Me Number/Pattern Configuration Settings (continued)*

Field	Description
Partition	To use a partition to restrict access to the meet-me/number pattern, choose the desired partition from the drop-down list box. If you do not want to restrict access to the meet-me number/pattern, choose <None> for the partition. Refer to the “Partition Configuration” section on page 42-1 for more information. You can configure the number of partitions that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more partitions exist than the Max List Box Items enterprise parameter specifies, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Partition window. Enter a partial partition name in the List items where Name contains field. Click the desired partition name in the list of partitions that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and update the Max List Box Items field under CCMAdmin Parameters. Note Make sure that the combination of meet-me number/pattern and partition is unique within the Cisco Unified CallManager cluster.

Additional Topics

See the [“Related Topics” section on page 50-5](#).

Deleting a Meet-Me Number/Pattern

This section describes how to delete a Meet-Me Number/Pattern.

Before You Begin

Make sure that the following prerequisites are met before proceeding with the steps:

- Configure the servers.
- Configure the device pools.
- Configure the meet-me number/pattern.

Procedure

-
- Step 1** Find the meet-me number/pattern by using the procedure in the [“Finding a Meet-Me Number/Pattern” section on page 50-1](#).
- Step 2** Click the Meet-Me Number/Pattern that you want to delete.
- Step 3** Click **Delete**.
-

Additional Topics

See the [“Related Topics”](#) section on page 50-5.

Related Topics

- [Partition Configuration](#), page 42-1
- [Finding a Meet-Me Number/Pattern](#), page 50-1
- [Configuring a Meet-Me Number/Pattern](#), page 50-2
- [Deleting a Meet-Me Number/Pattern](#), page 50-4
- [Meet-Me Number/Pattern Configuration Settings](#), page 50-3
- [Adding a Hardware Conference Device](#), page 54-4
- [Adding a Cisco IOS Conference Bridge Device](#), page 54-5
- [Updating a Conference Device](#), page 54-10
- [Deleting a Conference Device](#), page 54-10
- [Conference Bridges](#), *Cisco Unified CallManager System Guide*



Route Plan Report

The route plan report lists all assigned and unassigned directory numbers (DN), call park numbers, call pickup numbers, conference numbers, route patterns, translation patterns, message-waiting indicators, voice mail ports, and Cisco Unified CallManager Attendant Console pilot numbers in the system. The route plan report allows you to view either a partial or full list and to go directly to the associated configuration windows by clicking the Pattern/Directory Number, Partition, or Route Detail fields.

In addition, the route plan report allows you to save report data into a .csv file that you can import into other applications. The .csv file contains more detailed information than the web pages, including directory numbers for phones, route patterns, pattern usage, device name, and device description.

Cisco Unified CallManager uses the route plan to route both internal calls and external public switched telephone network (PSTN) calls. For more detailed information on the route plan, refer to the [“Understanding Route Plans”](#) section in *Cisco Unified CallManager System Guide*.

Use the following procedures to view route plan records:

- [Viewing Route Plan Records, page 51-1](#)
- [Deleting Unassigned Directory Numbers, page 51-3](#)
- [Viewing Route Plan Reports in a File, page 51-4](#)

Viewing Route Plan Records

This section describes how to view route plan records. Because you might have several records in your network, Cisco Unified CallManager Administration lets you locate specific route plan records on the basis of specific criteria. Use the following procedure to generate customized route plan reports.

Procedure

Step 1 Choose **Call Routing > Route Plan Report**.

The Route Plan Report window displays. Use the three drop-down list boxes to specify a route plan report that meets your requirements.

Step 2 From the first Find drop-down list box, choose one of the following criteria:

- All Patterns
- Unassigned DN
- Call Park
- Conference

- Directory Number
- Translation Pattern
- Call Pickup Group
- Route Pattern
- Message Waiting
- Hunt Pilot
- Voice Mail Port
- Attendant Console
- Domain Routing
- IP Routing

From the second Find where drop-down list box, choose one of the following criteria:

- Pattern/Directory Number
- Partition

From the third Find where drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is not empty
- is empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Tip

To find all route plans that are registered in the database, click **Find** without entering any search text.



Note

The route plan report shows the pattern/directory number, the corresponding partition and pattern type, and the route detail. The Route Detail column shows route list (with route group and line groups and associated gateway, and ports used information) or gateway information.

A list of discovered route plans displays by

- Pattern/Directory Number icon
- Pattern/Directory Number
- Partition
- Type
- Route Detail

- Step 4** Click the pattern/directory number icon or name, the associated partition, or the route detail from the list of records that matches your search criteria.
- The window displays the pattern that you choose.
-

Additional Information

See the [“Related Topics” section on page 51-5](#).

Deleting Unassigned Directory Numbers

This section describes how to delete an unassigned directory number from the route plan report. Directory numbers get configured and removed in the Directory Number Configuration window of Cisco Unified CallManager Administration. When a directory number gets removed from a device or a phone gets deleted, the directory number still exists in the Cisco Unified CallManager database. To delete the directory number from the database, use the Route Plan Report window.

Procedure

- Step 1** Choose **Call Routing > Route Plan Report**.
- The Route Plan Report window displays. Use the three drop-down list boxes to specify a route plan report that lists all unassigned DNs.
- Step 2** Three ways exist to delete directory numbers:
- Click the directory number that you want to delete. When the Directory Number Configuration window displays, click **Delete**.
 - Check the check box next to the directory number that you want to delete. Click **Delete Selected**.
 - To delete all found unassigned directory numbers, click **Delete all Found Items**.
- A warning message verifies that you want to delete the directory number.
- Step 3** To delete the directory number, click **OK**. To cancel the delete request, click **Cancel**.
-

Additional Information

See the [“Related Topics” section on page 51-5](#).

Updating Unassigned Directory Numbers

This section describes how to update the settings of an unassigned directory number from the route plan report. Directory numbers get configured and removed in the Directory Number Configuration window of Cisco Unified CallManager Administration. When a directory number gets removed from a device, the directory number still exists in the Cisco Unified CallManager database. To update the settings of the directory number, use the Route Plan Report window.

Procedure

Step 1 Choose **Call Routing > Route Plan Report**.

The Route Plan Report window displays. Use the three drop-down list boxes to specify a route plan report that lists all unassigned DNs.

Step 2 Click the directory number that you want to update.

The Directory Number Configuration window displays.



Note You can update all the settings of the directory number except the directory number and partition.

Step 3 Make the required updates such as calling search space or forwarding options.

Step 4 Click **Save**.

The Directory Number Configuration window redisplay, and the directory number field is blank.

Additional Information

See the [“Related Topics” section on page 51-5](#).

Viewing Route Plan Reports in a File

This section contains information on how to view route plan reports in a .csv file.

Procedure

Step 1 Choose **Call Routing > Route Plan Report**.

The Route Plan Report window displays.

Step 2 Choose **View In File** from the Related Links drop-down list box on the Route Plan Report window, and click **Go**. A dialog box displays.

From this dialog box, you can either save the file or import it into another application.

Step 3 Click **Save**.

Another window displays that allows you to save this file to a location of your choice.



Note You may also save the file as a different file name, but the file name must have a .csv extension.

Step 4 Choose the location in which to save the file and click **Save**. This action should save the file to the location that you designated.

Step 5 Locate the .csv file that you just saved and double-click its icon to view it.

Related Topics

- [Route Plan Report, page 51-1](#)
- [Viewing Route Plan Records, page 51-1](#)
- [Deleting Unassigned Directory Numbers, page 51-3](#)
- [Configuring a Directory Number, page 49-2](#)
- [Understanding Route Plans, *Cisco Unified CallManager System Guide*](#)



Installing Dial Plans

You can install Cisco International Dial Plan and use it to create a unique numbering plan that is specific to a country, other than one in North America. Cisco Unified CallManager provides North American Numbering Plan (NANP) by default. Because dial plan requirements of other countries are unique to those countries, the default NANP configuration may not be the best suited configuration to create a dial plan for those countries. Cisco International Dial Plan allows you to create and update unique dial plans and make them available for use to Cisco customers worldwide.

This chapter describes how to install a dial plan on Cisco Unified CallManager server.

Before you install a dial plan on the server, you should download the equivalent dial plan COP (Cisco Option Package) file to the Cisco Unified CallManager server.

You can find COP files for all the available dial plans that you can download, install, and integrate with Cisco Unified CallManager systems at the following URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/IDP>

For details on installing a COP file, see the *Cisco Unified CallManager Dial Plan Guide*.

For details on how to install a dial plan from this location, see “[Installing a Dial Plan on Cisco Unified CallManager](#)” section on page 52-3.

Use the following procedures to find and install dial plans on Cisco Unified CallManager.

- [Finding a Dial Plan, page 52-2](#)
- [Editing a Dial Plan, page 52-3](#)
- [Installing a Dial Plan on Cisco Unified CallManager, page 52-3](#)
- [Configuring Route Pattern Details for a non-NANP Dial Plan, page 52-4](#)
- [Upgrading a Dial Plan, page 52-4](#)
- [Uninstalling a Dial Plan, page 52-6](#)
- [Restarting the Cisco CallManager Service, page 52-6](#)
- [Related Topics, page 52-7](#)

Finding a Dial Plan

Use the following procedure to find a dial plan on a Cisco Unified CallManager system.

Procedure

Step 1 From Cisco Unified CallManager Administration window, choose **Call Routing > Dial Plan Installer**. The Find and List Dial Plans window displays

Because you might have several dial plans in your network, Cisco Unified CallManager lets you locate specific dial plans on the basis of specific criteria. Use the following procedure to locate servers.



Note

During your work in a browser session, cookies on the client machine store your find/list search preferences. If you navigate to other menu items and return to this menu item, or if you close the browser and then open a new browser window, the system retains your Cisco Unified CallManager search preferences until you modify your search.

Step 2 From the first Find Dial Plan where drop-down list box, choose one of the following criteria:

- Dial Plan
- Description

From the second Find Dial Plan where drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**.



Tip

To find all dial plans that are registered in the database, click **Find** without entering any search text.

A list of discovered servers displays by

- Dial Plans
- Description
- Installed Version
- System Version



Note

Installed version refers to the dial plan version that is installed on the node. System version refers to the latest version of the dial plan that is available on the first node of the cluster.

Additional Information

See the [“Related Topics” section on page 52-7](#).

Editing a Dial Plan

Use the following procedures to install, upgrade, or uninstall dial plans.

Procedure

-
Step 1	Find the Dial Plan that you want to install by using the procedure defined in the “Finding a Dial Plan” section on page 52-2
Step 2	From the list of records, click the Dial Plan name that matches your search criteria. The Dial Plan Configuration window displays.
Step 3	Complete one of the following tasks: • To install a dial plan, see the “Installing a Dial Plan on Cisco Unified CallManager” section on page 52-3. • To upgrade a dial plan, see the “Upgrading a Dial Plan” section on page 52-4. • To uninstall a dial plan, see the “Uninstalling a Dial Plan” section on page 52-6.
-

Additional Information

See the [“Related Topics” section on page 52-7](#).

Installing a Dial Plan on Cisco Unified CallManager

Use the following procedure to install a dial plan.

Procedure

-
Step 1	Find the Dial Plan that you want to install by using the procedure that is defined in the “Finding a Dial Plan” section on page 52-2 .
Step 2	From the list of records, click the Dial Plan name that matches your search criteria. The Dial Plan Configuration window displays.
Step 3	The dial plan name and description display in the Dial Plan and Description fields.
Step 4	The Installed Version displays the current version that is installed on Cisco Unified CallManager server. If no version of the dial plan is installed, the Installed Version displays Not Installed.
Step 5	Choose the dial plan version that you want to install from the Available Version drop-down list box.
Step 6	Click Install . The Status displays that the dial plan has been installed. The Installed Version field displays the dial plan version that is installed on Cisco Unified CallManager server.

Step 7 Repeat [Step 1](#) to [Step 6](#) to install the dial plans on all the nodes Cisco Unified CallManager cluster.

**Note**

After installation of the dial plans, restart the Cisco CallManager service to load the dial plan.

Additional Information

See the [“Related Topics”](#) section on page 52-7.

Configuring Route Pattern Details for a non-NANP Dial Plan

If you have installed a non-NANP dial plan on your Cisco Unified CallManager system, you can choose the required dial plan when you set up route pattern details in the Route Details Configuration window in Cisco Unified CallManager.

Note the following points when you configure route pattern details:

1. For a non-NANP dial plan, if you want to retain the settings at the Route Pattern level, make one of the following choices in the Route Details Configuration window:
 - a. Choose None in the Discard Digits field. Choosing None DDI in the Discard Digits field represents the same as not choosing a dial plan.
 - b. Choose a non-NANP dial plan:No Digits in the Discard Digits field. (For Example, AMNP:No Digits.)
2. If you want to specify settings at the Route Group level that will override the Route Pattern settings, choose the appropriate DDI for that dial plan from the Discard Digits field. Examples of DDI: NANP:PreDot, AMNP:PreDot.

Additional Information

See the [“Related Topics”](#) section on page 52-7.

Upgrading a Dial Plan

If you have installed a non-NANP dial plan, you can upgrade the dial plan that is installed on your Cisco Unified CallManager system with an upgraded version of the dial plan.

**Caution**

Upgrading a dial plan will fail if you configured one or more tags as a clause for a route filter in the existing version of the dial plan and the upgrade version does not contain these tags. After you upgrade to the new dial plan, the upgrade will list all such tags. You need to disassociate these tags from the route filter and run the dial plan upgrade again on the Cisco Unified CallManager system.

**Caution**

Upgrading a dial plan will fail if you have associated one or more DDIs with Route Patterns/Translation Patterns/Route Lists in the existing version of the dial plan and the upgrade version does not contain these DDIs. The dial plan upgrade will list all such DDIs. You need to disassociate these DDIs from Route Patterns/Translation Patterns/Route Lists and run the dial plan upgrade again on the Cisco Unified CallManager system.

**Note**

Make sure that you update the dial plans on the first node server of the Cisco Unified CallManager cluster before updating them on subscribers or other nodes in the cluster.

Use the following procedure to upgrade an existing dial plan.

Procedure

-
- Step 1** Find the Dial Plan that you want to upgrade by using the procedure that is defined in the [“Finding a Dial Plan”](#) section on page 52-2
- Step 2** From the list of records, click the Dial Plan name that matches your search criteria.
The Dial Plan Configuration window displays.
- Step 3** The dial plan name and description display in the Dial Plan and Description fields.
- Step 4** The Installed Version displays the current version that is installed on Cisco Unified CallManager server. If no version of the dial plan is installed, the Installed Version displays Not Installed.
- Step 5** Choose the dial plan version that you want to upgrade from the Available Version drop-down list box.
- Step 6** Click **Install**.
The Status displays that the dial plan has been upgraded.
The Installed Version field displays the latest dial plan version.
- Step 7** Repeat [Step 1](#) to [Step 6](#) to upgrade the dial plans on all nodes of Cisco Unified CallManager cluster where the Cisco CallManager service is installed.

**Note**

After upgrading the dial plans, restart the Cisco CallManager service for the changes to take effect. See the [“Restarting the Cisco CallManager Service”](#) section on page 52-6.

**Note**

When dial plans are migrated from 4.0x to 5.0x, all configurations, like route patterns, get retained; the dial plans do not display in the Find and List Dial Plans window. To update dial plans, you must install the COP file, as described in the *Cisco Unified CallManager Dial Plan Guide* and install the dial plans that you want. See the [“Installing a Dial Plan on Cisco Unified CallManager”](#) section on page 52-3.

**Note**

When you upgrade from 4.0x to 5.0x, to retain the dial plan and the dial plan configurations like route pattern/route filter associated for a dial plan, install the latest dial plans available on CCO.

Additional Information

See the [“Related Topics”](#) section on page 52-7.

Uninstalling a Dial Plan

**Caution**

Before you uninstall a dial plan, ensure that you remove the route patterns, translation patterns, route lists, and route filters that are configured in the dial plan on the Cisco Unified CallManager system.

Use the following procedure to uninstall a dial plan.

Procedure

-
- Step 1** Find the Dial Plan that you want to delete by using the procedure that is defined in the [“Finding a Dial Plan” section on page 52-2](#).
- Step 2** From the list of records, click the Dial Plan name that matches your search criteria.
The Dial Plan Configuration window displays.
- Step 3** The dial plan name and description display in the Dial Plan and Description fields.
- Step 4** The Installed Version displays the current version that is installed on the Cisco Unified CallManager server.
- Step 5** Click **Uninstall**.

**Note**

Dial plans should be uninstalled first from the first node in the cluster and then from the subsequent nodes.

The Status displays that the dial plan was deleted.

The Installed Version field displays Not Installed.

- Step 6** Repeat [Step 1](#) to [Step 5](#) to uninstall the dial plans on all nodes of the Cisco Unified CallManager cluster.
-

Additional Information

See the [“Related Topics” section on page 52-7](#).

Restarting the Cisco CallManager Service

Use the following procedure to restart the Cisco CallManager service.

Procedure

-
- Step 1** In the Cisco Unified CallManager Serviceability window, choose **Tools > Control Center - Feature Services**.
The Control Center–Feature Services window displays.
- Step 2** Choose the Cisco Unified CallManager server from the Servers drop-down list box.
In the CM Services area, Cisco CallManager displays in the Service Name column.

**Note**

Click the radio button corresponding to the Cisco CallManager service.

- Step 3** If you want to restart the Cisco CallManager service, click **Restart**.
The service restarts, and the message, Service Successfully Restarted, displays.
- Step 4** If you want to start a stopped Cisco CallManager service, click **Start**.
The service starts, and the message, Service Successfully Started, displays.
-

Additional Information

See the [“Related Topics” section on page 52-7](#).

Related Topics

- [Finding a Dial Plan, page 52-2](#)
- [Editing a Dial Plan, page 52-3](#)
- [Installing a Dial Plan on Cisco Unified CallManager, page 52-3](#)
- [Configuring Route Pattern Details for a non-NANP Dial Plan, page 52-4](#)
- [Upgrading a Dial Plan, page 52-4](#)
- [Uninstalling a Dial Plan, page 52-6](#)
- [Restarting the Cisco CallManager Service, page 52-6](#)
- *Cisco Unified CallManager Dial Plan Guide.*



PART 4

Media Resource Configuration





Annunciator Configuration

An annunciator, an SCCP device that uses the Cisco Media Streaming Application service, enables Cisco Unified CallManager to play prerecorded announcements (.wav files) and tones to Cisco Unified IP Phones and gateways. The annunciator, which works with Cisco Multilevel Precedence and Preemption (MLPP), enables Cisco Unified CallManager to alert callers as to why the call fails. Annunciator can also play tones for some transferred calls and some conferences.

Use the following topics to find and update annunciators:

- [Before You Begin, page 53-1](#)
- [Finding an Annunciator, page 53-1](#)
- [Updating an Annunciator, page 53-2](#)
- [Annunciator Configuration Settings, page 53-3](#)
- [Resetting an Annunciator, page 53-4](#)

Before You Begin

Verify that you have activated the Cisco IP Voice Media Streaming Application service on the server where you plan to configure the annunciator.



Tip

When you add a Cisco Unified CallManager server, the annunciator for the server will automatically get added to the database. After you activate the Cisco IP Voice Media Streaming Application service, the annunciator device registers with Cisco Unified CallManager; verify whether the annunciator exists by using the [“Finding an Annunciator” section on page 53-1](#).

Finding an Annunciator

Perform the following procedure to find an annunciator:

Procedure

- Step 1** Choose **Media Resources > Annunciator**.
The Find and List Annunciators window displays.

**Tip**

To find all annunciators that are registered in the database, click **Find** without entering any search text.

To find a specific annunciator quickly, specify the search criteria by performing the following procedure.

- Step 2** From the first Find Annunciators where drop-down list box, choose Name or Description.
- Step 3** From the second Find Annunciators where drop-down list box, choose one of the following criteria:
- begins with
 - contains
 - ends with
 - is exactly
 - is empty
 - is not empty
- Step 4** Enter the appropriate search text, if applicable, and click **Find**.
A list of configured annunciators displays.
- Step 5** Click the annunciator name from the list of records that match your search criteria.
The window displays the annunciator that you choose.

Additional Information

See the [“Related Topics”](#) section on page 53-4.

Updating an Annunciator

This section describes how to update an annunciator.

Before You Begin

Before you update an annunciator, verify that you have completed the following tasks:

- Configured the appropriate servers
- Configured device pools

Procedure

- Step 1** Choose **Media Resources > Annunciator**.
The Find and List Annunciators window displays.
- Step 2** To update an annunciator, locate the appropriate annunciator as described in the [“Finding an Annunciator”](#) section on page 53-1.

**Tip**

When you add a Cisco Unified CallManager server, the annunciator for the sever will automatically get added to the database. After you activate the Cisco IP Voice Media Streaming Application service, the annunciator device registers with Cisco Unified CallManager.

- Step 3** Click the annunciator you want to update and continue with [Step 4](#).
- Step 4** Enter the appropriate settings as described in [Table 53-1](#).
- Step 5** Click **Save**.
- Step 6** Be sure the Cisco IP Voice Media Streaming Application service has been activated. For information on activating services, refer to the *Cisco Unified CallManager Serviceability Administration Guide*.

Additional Information

See the “[Related Topics](#)” section on [page 53-4](#).

Annunciator Configuration Settings

[Table 53-1](#) describes the annunciator configuration settings. For more information about related procedures, see the “[Related Topics](#)” section on [page 53-4](#).

Table 53-1 **Annunciator Configuration Settings**

Field	Description
Server	The system automatically displays the preconfigured server (servers get added at installation).
Name	This field designates the name that is used when the device registers with the Cisco Unified CallManager. Enter a name of up to 15 alphanumeric characters (periods, dashes, and underscores are allowed).
Description	Enter a description of up to 54 alphanumeric characters (periods, dashes, and underscores are allowed). By default, the server name, which includes the prefix ANN_, is used.
Device Pool	Choose Default or choose a device pool from the drop-down list of configured device pools.
Location	Choose the appropriate location for this annunciator. A location setting of <i>Hub_None</i> means that the locations feature does not keep track of the bandwidth that this annunciator consumes.

Resetting an Annunciator

To reset an annunciator, perform the following procedure:

Procedure

-
Step 1	Locate the annunciator by using the procedure in the “Finding an Annunciator” section on page 53-1.
Step 2	Click the annunciator that you want to reset.
Step 3	Click the Reset button.
Step 4	The Device Reset Window displays. To continue, click Reset .
-

Additional Information

See the [“Related Topics”](#) section on page 53-4.

Related Topics

- [Updating an Annunciator](#), page 53-2
- [Annunciator Configuration Settings](#), page 53-3
- [Resetting an Annunciator](#), page 53-4
- [Multilevel Precedence and Preemption](#), *Cisco Unified CallManager Features and Services Guide*
- [Annunciator](#), *Cisco Unified CallManager System Guide*



Conference Bridge Configuration

Conference Bridge for Cisco Unified CallManager, a software or hardware application, allows both ad hoc and meet-me voice conferencing. Each conference bridge can host several simultaneous, multiparty conferences.

Both hardware and software conference bridges can be active at the same time. Software and hardware conference devices differ in the number of streams and the types of codec that they support.

Refer to the “[Conference Bridges](#)” chapter of the *Cisco Unified CallManager System Guide* for more information about conference bridges.



Note

The hardware model type for Conference Bridge contains a specific Media Access Control (MAC) address and device pool information.



Note

Be aware that different conference bridge fields display in Cisco Unified CallManager Administration, depending on the conference bridge type that you choose.

Use the following topics to configure conference bridges:

- [Finding a Conference Bridge, page 54-2](#)
- [Understanding Software Conference Bridge Configuration, page 54-3](#)
- [Software Conference Bridge Configuration Settings, page 54-3](#)
- [Adding a Hardware Conference Device, page 54-4](#)
- [Hardware Conference Bridge Configuration Settings, page 54-5](#)
- [Adding a Cisco IOS Conference Bridge Device, page 54-5](#)
- [Cisco IOS Conference Bridge Configuration Settings, page 54-6](#)
- [Adding a Cisco Video Conference Bridge Device, page 54-6](#)
- [Cisco Video Conference Bridge Configuration Settings, page 54-7](#)
- [Adding a Cisco Unified CallManager Conference Bridge \(WS-SVC-CMM\) Device, page 54-8](#)
- [Cisco Unified CallManager Conference Bridge \(WS-SVC-CMM\) Configuration Settings, page 54-9](#)
- [Updating a Conference Device, page 54-10](#)
- [Deleting a Conference Device, page 54-10](#)
- [Configuring a Meet-Me Number/Pattern, page 50-2](#)

- [Meet-Me Number/Pattern Configuration Settings, page 50-3](#)
- [Deleting a Meet-Me Number/Pattern, page 50-4](#)

Finding a Conference Bridge

Because you may have several conference bridges in your network, Cisco Unified CallManager lets you locate specific conference bridges on the basis of specific criteria. Use the following procedure to locate conference bridges.

**Note**

During your work in a browser session, Cisco Unified CallManager Administration retains your conference bridge search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your conference bridge search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Media Resources > Conference Bridge**.

The Find and List Conference Bridges window displays. Use the two drop-down list boxes to search for a conference bridge.

Step 2 From the first Find Conference Bridges where drop-down list box, choose one of the following criteria:

- Name
- Description
- Device Pool

From the second Find Conference Bridges where drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is not empty
- is empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.

**Tip**

To find all conference bridges that are registered in the database, click **Find** without entering any search text.

A list of discovered conference bridges displays by

- Conference Bridge icon
- Conference Bridge name
- Description

- Device Pool
- Status
- IP Address



Note You can delete multiple conference bridges from the Find and List Conference Bridges window by checking the check boxes next to the appropriate conference bridges and clicking **Delete Selected**. You can delete all conference bridges in the window by checking the check box in the Matching records title bar and clicking **Delete Selected**.

Step 4 From the list of records, click the Conference Bridge icon or name or the associated Device Pool that matches your search criteria.

The window displays the conference bridge that you choose.

Additional Information

See the [“Related Topics” section on page 54-11](#).

Understanding Software Conference Bridge Configuration

Administrators cannot add software conference bridges to Cisco Unified CallManager by using Conference Bridge Configuration. Software conference bridges are automatically added when a Cisco Unified CallManager server gets added (see the [“Configuring a Server” section on page 2-2](#) for more information). After a Cisco Unified CallManager server gets added, the software conference bridge gets displayed in the Find/List Conference Bridges window (by default, the first software conference bridge gets configured during Cisco Unified CallManager installation) when the administrator performs a search. Software conference bridges can be updated, but they cannot be deleted.

Additional Information

See the [“Related Topics” section on page 54-11](#).

Software Conference Bridge Configuration Settings

[Table 54-1](#) describes the software conference bridge configuration settings.

Table 54-1 **Software Conference Bridge Configuration Settings**

Field	Description
Conference Bridge Type	This field automatically displays Cisco Unified CallManager Conference Bridge Software.
Host Server	This field automatically displays the Cisco Unified CallManager server to which this software conference bridge was configured.

Table 54-1 Software Conference Bridge Configuration Settings (continued)

Field	Description
Conference Bridge Name	This field automatically displays the software conference bridge name. The format of the name specifies CFB_ followed by a digit representing the value of the software conference bridge; for example, CFB_3 represents the third conference bridge in the Cisco Unified CallManager system.
Description	This field automatically displays a description, but the administrator can update this field.
Device Pool	Choose a device pool that has the highest priority within the Cisco Unified CallManager group that you are using or choose Default .
Location	Choose the appropriate location for this conference bridge. The location specifies the total bandwidth that is available for calls to and from this location. A location setting of <i>Hub_None</i> means that the locations feature does not keep track of the bandwidth that this conference bridge consumes.

Additional Information

See the [“Related Topics”](#) section on page 54-11.

Adding a Hardware Conference Device

This section describes how to add a hardware conference device.

Before You Begin

Configure the Device pools. Refer to the [“Device Pool Configuration”](#) section on page 9-1.

Procedure

-
- Step 1** Choose **Media Resources > Conference Bridge**.
- Step 2** Click **Add New**.
- The Conference Bridge Configuration window displays.
- Step 3** Enter the appropriate settings as described in [Table 54-2](#).
- Step 4** Click **Save**.
- Step 5** To reset the conference bridge device and apply your changes, click **Reset**.
- The Device Reset window displays.
- Step 6** Click **Reset** and close the window.
-

Additional Information

See the [“Related Topics”](#) section on page 54-11.

Hardware Conference Bridge Configuration Settings

Table 54-2 describes the hardware conference bridge configuration settings.

Table 54-2 Hardware Conference Bridge Configuration Settings

Field	Description
Conference Bridge Type	Choose Cisco Unified CallManager Conference Bridge Hardware . For a description of this type, refer to the “ Conference Bridge Types in Cisco Unified CallManager Administration ” section on page 24-4.
MAC Address	Enter a unique device MAC address in this required field. MAC addresses comprise 12 hexadecimal digits (0-9, A-F). Example 1231123245AB
Description	This field automatically generates from the MAC address that you provide.
Device Pool	Choose a device pool that has the highest priority within the Cisco Unified CallManager group that you are using or choose Default .
Location	Choose the appropriate location for this conference bridge. The location specifies the total bandwidth that is available for calls to and from this location. A location setting of <i>Hub_None</i> means that the locations feature does not keep track of the bandwidth that this conference bridge consumes.
Special Load Information	Enter any special load information or leave blank to use default.

Additional Information

See the “[Related Topics](#)” section on page 54-11.

Adding a Cisco IOS Conference Bridge Device

This section describes how to add a Cisco IOS conference device.

Before You Begin

Configure the device pools. See the “[Device Pool Configuration](#)” section on page 9-1.

Procedure

-
Step 1	Choose Media Resources > Conference Bridge .
Step 2	Click Add New . The Conference Bridge Configuration window displays.
Step 3	Enter the appropriate settings as described in Table 54-3 .
Step 4	Click Save . The window refreshes and displays the conference device that you just added.

- Step 5** To reset the conference bridge device and apply your changes, click **Reset**.
The Device Reset window displays.
- Step 6** Click **Reset**.

Additional Information

See the [“Related Topics”](#) section on page 54-11.

Cisco IOS Conference Bridge Configuration Settings

Table 54-3 describes the Cisco IOS conference bridge configuration settings.

Table 54-3 Cisco IOS Conference Bridge Configuration Settings

Field	Description
Conference Bridge Type	Choose Cisco IOS Conference Bridge or Cisco IOS Enhanced Conference Bridge . For a description of these types, refer to the “Conference Bridge Types in Cisco Unified CallManager Administration” section on page 24-4.
Conference Bridge Name	Enter the same name that exists in the gateway Command Line Interface (CLI).
Description	This field automatically generates from the conference bridge name that you provide.
Device Pool	Choose a device pool or choose Default .
Location	Choose the appropriate location for this conference bridge. The location specifies the total bandwidth that is available for calls to and from this location. A location setting of <i>Hub_None</i> means that the locations feature does not keep track of the bandwidth that this conference bridge consumes.

Additional Information

See the [“Related Topics”](#) section on page 54-11.

Adding a Cisco Video Conference Bridge Device

This section describes how to add a Cisco video conference bridge device.

Before You Begin

Configure the device pools. See the [“Device Pool Configuration”](#) section on page 9-1.

Procedure

-
- Step 1** Choose **Media Resources > Conference Bridge**.
- Step 2** Click **Add New**.
The Conference Bridge Configuration window displays.
- Step 3** Enter the appropriate settings as described in [Table 54-4](#).
- Step 4** Click **Save**.
The window refreshes and displays the conference device that you just added.
- Step 5** To reset the conference bridge device and apply your changes, click **Reset**.
The Device Reset window displays.
- Step 6** Click **Reset**.
-

Additional Information

See the [“Related Topics”](#) section on page 54-11.

Cisco Video Conference Bridge Configuration Settings

[Table 54-4](#) describes the Cisco video conference bridge configuration settings.

Table 54-4 Cisco Video Conference Bridge Configuration Settings

Field	Description
Conference Bridge Type	Choose Cisco Video Conference Bridge (IPVC-35xx) . For a description of this type, refer to the “Conference Bridge Types in Cisco Unified CallManager Administration” section on page 24-4.
MAC Address	Enter a unique device MAC address in this required field. MAC addresses comprise 12 hexadecimal digits (0-9, A-F). Example 1231123245AB
Description	This field automatically generates from the conference bridge name that you provide.
Device Pool	Choose a device pool or choose Default .
Location	Choose the appropriate location for this conference bridge. The location specifies the total bandwidth that is available for calls to and from this location. A location setting of <i>Hub_None</i> means that the locations feature does not keep track of the bandwidth that this conference bridge consumes.

Table 54-4 Cisco Video Conference Bridge Configuration Settings (continued)

Field	Description
Product-Specific Configuration	
Model-specific configuration fields that the device manufacturer defines	The device manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the “?” information icon under the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, refer to the documentation for the specific device that you are configuring or contact the manufacturer.

Additional Information

See the [“Related Topics”](#) section on page 54-11.

Adding a Cisco Unified CallManager Conference Bridge (WS-SVC-CMM) Device

This section describes how to add a Cisco Unified CallManager Conference Bridge (WS-SVC-CMM) device.

Before You Begin

Configure the device pools. See the [“Device Pool Configuration”](#) section on page 9-1.

Procedure

-
- Step 1** Choose **Media Resources > Conference Bridge**.
- Step 2** Click **Add New**.
- The Conference Bridge Configuration window displays.
- Step 3** Enter the appropriate settings as described in [Table 54-5](#).
- Step 4** Click **Save**.
- The window refreshes and displays the conference device that you just added.
- Step 5** To reset the conference bridge device and apply your changes, click **Reset**.
- A message displays that states that this action resets the conference bridge device.
- Step 6** Click **Reset**.
-

Additional Information

See the [“Related Topics”](#) section on page 54-11.

Cisco Unified CallManager Conference Bridge (WS-SVC-CMM) Configuration Settings

Table 54-5 describes the Cisco Unified CallManager Conference Bridge (WS-SVC-CMM) configuration settings.

Table 54-5 Cisco Unified CallManager Conference Bridge (WS-SVC-CMM) Configuration Settings

Field	Description
Conference Bridge Type	Choose Cisco Unified CallManager Conference Bridge (WS-SVC-CMM) . For a description of this type, refer to the “ Conference Bridge Types in Cisco Unified CallManager Administration ” section on page 24-4.
Description	Enter a description (up to 50 characters) or leave blank to generate automatically from the MAC address that you provide.
MAC Address	Enter a unique device MAC address in this required field. MAC addresses comprise 12 hexadecimal digits (0-9, A-F). Example 1231123245AB
Subunit	From the drop-down list box, choose the value for the daughter card for a given slot on the Communication Media Module card.
Device Pool	Choose a device pool or choose Default .
Location	Choose the appropriate location for this conference bridge. The location specifies the total bandwidth that is available for calls to and from this location. A location setting of <i>Hub_None</i> means that the locations feature does not keep track of the bandwidth that this conference bridge consumes.
Maximum Capacity	Choose the maximum number of streams for a given service on a daughter card. Possible values include 32, 64, 96, and 128 streams. Ensure that each daughter card has as many ports as the value that you choose.
Product-Specific Configuration	
Model-specific configuration fields that the device manufacturer defines	To view field descriptions and help for product-specific configuration items, click the “?” information icon under the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, refer to the documentation for the specific device that you are configuring or contact the manufacturer.

Additional Information

See the “[Related Topics](#)” section on page 54-11.

Updating a Conference Device

This section describes how to update a conference device.

Before You Begin

Make sure that the following prerequisites are met before you proceed with the steps:

- Configure the servers. See the [“Server Configuration” section on page 2-1](#).
- Configure the device pools. See the [“Device Pool Configuration” section on page 9-1](#).
- Configure the Conference device. See the applicable sections on adding conference devices.



Note Software conference bridges automatically get created when the Cisco Unified CallManager server gets created. See the [“Understanding Software Conference Bridge Configuration” section on page 54-3](#).

- For software conference bridges, activate the Cisco IP Voice Media Streaming Application service. Refer to the *Cisco Unified CallManager Serviceability Administration Guide*.

Procedure

-
- Step 1** Locate the conference bridge by using the procedure in the [“Finding a Conference Bridge” section on page 54-2](#).
- Step 2** Click the conference bridge that you want to update.
- Step 3** Update the appropriate settings as described in [Table 54-1](#), [Table 54-2](#), [Table 54-3](#), [Table 54-4](#), or [Table 54-5](#).
- Step 4** When you have completed your changes, click **Save**.
-

Additional Information

See the [“Related Topics” section on page 54-11](#).

Deleting a Conference Device

This section describes how to delete a Conference Device. Cisco Unified CallManager Conference Bridge Software cannot be deleted. See the [“Understanding Software Conference Bridge Configuration” section on page 54-3](#).

Before You Begin

Cisco Unified CallManager allows you to delete devices that may be associated with things such as media resource groups. To find out what dependencies the conference device may have, choose the **Dependency Records** link from the drop-down list box and click **Go** from the Conference Bridge Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#).

Procedure

-
- Step 1** Locate the conference bridge by using the procedure in the [“Finding a Conference Bridge” section on page 54-2](#).
- Step 2** Click the conference bridge that you want to delete.
- Step 3** Click **Delete Selected**.
- A message displays the following warning:
- You are about to permanently delete this Conference Bridge. This action cannot be undone. Continue?
- Step 4** To delete the conference device, click **OK**.
-

Additional Information

See the [“Related Topics” section on page 54-11](#).

Where to Find More Information

- *Cisco Unified Videoconferencing 3511 MCU and Cisco Unified Videoconferencing 3540 MCU Module Administrator Guide*
- *Cisco Unified CallManager System Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*

Related Topics

- [Finding a Conference Bridge, page 54-2](#)
- [Understanding Software Conference Bridge Configuration, page 54-3](#)
- [Software Conference Bridge Configuration Settings, page 54-3](#)
- [Adding a Hardware Conference Device, page 54-4](#)
- [Hardware Conference Bridge Configuration Settings, page 54-5](#)
- [Adding a Cisco IOS Conference Bridge Device, page 54-5](#)
- [Cisco IOS Conference Bridge Configuration Settings, page 54-6](#)
- [Adding a Cisco Video Conference Bridge Device, page 54-6](#)
- [Cisco Video Conference Bridge Configuration Settings, page 54-7](#)
- [Adding a Cisco Unified CallManager Conference Bridge \(WS-SVC-CMM\) Device, page 54-8](#)
- [Cisco Unified CallManager Conference Bridge \(WS-SVC-CMM\) Configuration Settings, page 54-9](#)
- [Updating a Conference Device, page 54-10](#)
- [Deleting a Conference Device, page 54-10](#)
- [Configuring a Meet-Me Number/Pattern, page 50-2](#)
- [Meet-Me Number/Pattern Configuration Settings, page 50-3](#)
- [Deleting a Meet-Me Number/Pattern, page 50-4](#)
- [Where to Find More Information, page 54-11](#)

- [Conference Bridges](#), *Cisco Unified CallManager System Guide*
- [Conference Bridge Types in Cisco Unified CallManager Administration](#), *Cisco Unified CallManager System Guide*



Media Termination Point Configuration

A Media Termination Point software device allows Cisco Unified CallManager to relay calls that are routed through SIP or H.323 endpoints or gateways. A media termination point device can be allocated because of DTMF or RSVP requirements. When a media termination point is allocated for RSVP, it can be inserted between any type of endpoint device, including SIP or H.323 devices.

Media termination point, a Cisco software application, installs on a server during the software installation process. You must activate and start the Cisco IP Voice Media Streaming App service on the server on which you configure the media termination point device. For information on activating and starting services, refer to the *Cisco Unified CallManager Serviceability Administration Guide*.

Each media termination point device that is defined in the database registers with the Media Resource Manager (MRM). The MRM keeps track of the total available media termination point devices in the system and of which devices have available resources.

During resource reservation, the MRM determines the number of resources and identifies the media resource type (in this case, the media termination point) and the location of the registered media termination point device. The MRM updates its share resource table with the registration information and propagates the registered information to the other Cisco Unified CallManagers within the cluster.

The media termination point and transcoder can register with the same Cisco Unified CallManager. See the [“Transcoder Configuration” section on page 59-1](#) for more information.

Each media termination point receives a list of Cisco Unified CallManagers, in priority order, to which it should attempt to register. Each media termination point can register with only one Cisco Unified CallManager at a time.



Note

Depending on the capabilities of the SIP end-point, Cisco Unified CallManager may require an RFC 2833 DTMF-compliant media termination point device to make SIP calls. For RSVP calls, the Media Resource Group List (MRGL) that is associated with the endpoint device needs to include the media termination point devices that support RSVP.

Use the following topics to add, update, and delete media termination points:

- [Finding a Media Termination Point, page 55-2](#)
- [Configuring a Media Termination Point, page 55-3](#)
- [Deleting a Media Termination Point, page 55-4](#)
- [Related Topics, page 55-5](#)

Finding a Media Termination Point

Because you might have several media termination points in your network, Cisco Unified CallManager lets you locate specific media termination points on the basis of specific criteria. Use the following procedure to locate media termination points.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your media termination point search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your media termination point search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Media Resources > Media Termination Point**.

The Find and List Media Termination Points window displays. Use the two drop-down list boxes to search for a media termination point.

Step 2 From the first Find Media Termination Points where drop-down list box, choose one of the following criteria:

- Name
- Description
- Device Pool

From the second Find Media Termination Points where drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is not empty
- is empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Tip

To find all media termination points that are registered in the database, click **Find** without entering any search text.

A list of discovered media termination points displays by

- Media Termination Point icon
- Media Termination Point name
- Description
- Device Pool
- Status
- IP Address

**Note**

You can delete multiple media termination points from the Find and List Media Termination Points window by checking the check boxes next to the appropriate media termination points and clicking **Delete Selected**. You can delete all media termination points in the window by clicking **Select All** and click **Delete Selected**.

- Step 4** Click the Media Termination Point icon or name, the Description, or the associated Device Pool from the list of records that match your search criteria.

The window displays the media termination point that you choose.

Additional Information

See the [“Related Topics” section on page 55-5](#).

Configuring a Media Termination Point

This section describes how to add, copy, or update a Media Termination Point.

**Note**

To perform this procedure, you must activate the Cisco IP Voice Media Streaming App service by using Cisco Unified CallManager Serviceability. For information about activating services, refer to the *Cisco Unified CallManager Serviceability Administration Guide*.

Before You Begin

Make sure that the following prerequisites are met before you proceed with the steps:

- Ensure servers are configured.
- Ensure device pools are configured.

**Note**

You can have only one Media Termination Point device for each Cisco Unified CallManager server. When a Cisco Unified CallManager Server is added, a media termination point device automatically gets created for the server but is not available for use until the Cisco IP Voice Media Streaming App service gets activated.

Procedure

- Step 1** Perform one of the following tasks:

- To add a Media Termination Point, choose **Media Resources > Media Termination Point**. The Find and List Media Termination Point window displays. Click **Add New**.
- To copy a Media Termination Point, choose **Media Resources > Media Termination Point**. The Find and List Media Termination Point window displays. Click the Copy icon next to the media termination point that you want to copy.
- To update a Media Termination Point, locate the media termination point by using the procedure in the [“Finding a Media Termination Point” section on page 55-2](#).

- Step 2** Enter the appropriate settings as described in [Table 55-1](#).
- Step 3** Click **Save**.

Additional Information

See the [“Related Topics”](#) section on page 55-5.

Cisco IOS Media Termination Point Configuration Settings

[Table 55-1](#) describes Cisco IOS media termination point configuration settings.

Table 55-1 Cisco IOS Media Termination Point Configuration Settings

Field	Description
Media Termination Point Type	Choose Cisco IOS Enhanced Software Media Termination Point . For specific information on this media termination point type, refer to “Media Termination Points” in the <i>Cisco Unified CallManager System Guide</i> .
Media Termination Point Name	Enter a name for the media termination point, up to 15 alphanumeric characters. Tip Ensure that you enter the same media termination point name that exists in the gateway Command Line Interface (CLI).
Description	Enter any description for the media termination point.
Device Pool	Choose a device pool that has the highest priority within the Cisco Unified CallManager group that you are using or choose Default .

Additional Information

See the [“Related Topics”](#) section on page 55-5.

Deleting a Media Termination Point

This section describes how to delete a Media Termination Point.

Before You Begin

Before deleting a media termination point that is currently in use and is the last device in the Media Resource Group, you should perform either or both of the following tasks:

- Assign a different media termination point to the media resource groups that are using the media termination point that you want to delete. See the [“Deleting a Media Resource Group”](#) section on page 60-5 section.
- Delete the media resource groups that are using the media termination point that you want to delete. See the [“Deleting a Media Resource Group”](#) section on page 60-5.

Procedure

-
- Step 1** Locate the media termination point by using the procedure in the [“Finding a Media Termination Point” section on page 55-2](#).
- Step 2** Click the media termination point that you want to delete.
- Step 3** Click **Delete Selected**.
- A message displays the following warning:
- You are about to permanently delete this Media Termination Point. This action cannot be undone. Continue?
- Step 4** To delete the media termination point, click **OK**.
- If this is the last device in the Media Resource Group, the Media Resource Group will remain as an empty group.
- Step 5** Click **OK**.
-

Additional Information

See the [“Related Topics” section on page 55-5](#).

Related Topics

- [Finding a Media Termination Point, page 55-2](#)
- [Configuring a Media Termination Point, page 55-3](#)
- [Deleting a Media Termination Point, page 55-4](#)
- [Related Topics, page 55-5](#)
- [Transcoders, page 25-1](#)
- [Media Termination Points, Cisco Unified CallManager System Guide](#)
- [Resource Reservation Protocol, Cisco Unified CallManager System Guide](#)



Music On Hold Audio Source Configuration

The integrated Music On Hold feature provides the ability to place on-net and off-net users on hold with music streamed from a streaming source. This feature includes the following actions:

- End user hold
- Network hold, which includes transfer hold, conference hold, and park hold

Music On Hold configuration comprises configuration of Music On Hold audio sources and Music On Hold servers.

For more information on how to use the Music On Hold Audio Source Configuration window, refer to the [Music On Hold](#) chapter in the *Cisco Unified CallManager Features and Services Guide*.



Music On Hold Fixed Audio Source Configuration

The integrated Music On Hold feature provides the ability to place on-net and off-net users on hold with music streamed from a streaming source. This feature includes the following actions:

- End user hold
- Network hold, which includes transfer hold, conference hold, and park hold

Music On Hold configuration comprises configuration of Music On Hold audio sources and Music On Hold servers. You can also enable a Music On Hold fixed audio source, and this audio source can allow multicasting.

For more information on how to use the Fixed MOH Audio Source Configuration window, refer to the [Music On Hold](#) chapter in the *Cisco Unified CallManager Features and Services Guide*.



Music On Hold Server Configuration

The Cisco Unified CallManager Music On Hold feature uses the MOH server, a software application that provides music on hold audio sources and connects a music on hold audio source to a number of streams.

For more information on how to use the Music On Hold Server Configuration window, refer to the [Music On Hold](#) chapter in the *Cisco Unified CallManager Features and Services Guide*.



Transcoder Configuration

The Media Resource Manager (MRM) has responsibility for resource registration and resource reservation of transcoders within a Cisco Unified CallManager cluster. Cisco Unified CallManager simultaneously supports registration of both the Media Termination Point (MTP) and Transcoder and concurrent MTP and transcoder functionality within a single call.

The Cisco Unified CallManager invokes a transcoder on behalf of endpoint devices when the two devices are using different codecs and would normally not be able to communicate. When inserted into a call, the transcoder converts the data streams between the two disparate codecs to enable communications between them.

A transcoder control process gets created for each transcoder device that is defined in the database. Each transcoder registers with the MRM when it initializes. The MRM keeps track of the transcoder resources and advertises their availability throughout the cluster.

Use the following topics to configure transcoders:

- [Finding a Transcoder, page 59-1](#)
- [Configuring a Transcoder, page 59-3](#)
- [Resetting a Transcoder, page 59-3](#)
- [Deleting a Transcoder, page 59-4](#)
- [Transcoder Configuration Settings, page 59-5](#)

Finding a Transcoder

Because you might have several transcoders in your network, Cisco Unified CallManager lets you locate specific transcoders on the basis of specific criteria. Use the following procedure to locate transcoders.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your transcoder search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your transcoder search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Media Resources > Transcoder**.

The Find and List Transcoders window displays. Use the two drop-down list boxes to search for a transcoder.

Step 2 From the first Find Transcoders where drop-down list box, choose one of the following criteria:

- Name
- Description
- Device Pool



Note The criterion that you choose in this drop-down list box specifies how the list of transcoders that your search generates will be sorted. For example, if you choose Device Pool, the Device Pool column will display as the left column of the results list.

From the second Find Transcoders where drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Tip To find all transcoders that are registered in the database, click **Find** without entering any search text.

A list of discovered transcoders displays by

- Transcoder icon
- Transcoder name
- Description
- Device Pool
- Status
- IP Address



Note You can delete multiple transcoders from the Find and List Transcoders window by checking the check boxes next to the appropriate transcoders and clicking **Delete Selected**. You can delete all transcoders in the window by clicking **Select All** and then clicking **Delete Selected**.

- Step 4** From the list of records, click the Transcoder icon or name, the Description, or the associated Device Pool that matches your search criteria.
- The window displays the transcoder that you choose.
-

Additional Information

See the [“Related Topics” section on page 59-6](#).

Configuring a Transcoder

This section describes how to configure a transcoder.

Procedure

- Step 1** Choose **Media Resources > Transcoder**.
- The Find and List Transcoders window displays.
- Step 2** Perform one of the following tasks:
- To copy an existing transcoder, locate the appropriate transcoder as described in the [“Finding a Transcoder” section on page 59-1](#), click the **Copy** button next to the transcoder that you want to copy, and continue with [Step 3](#).
 - To add a new transcoder, click the **Add New** button and continue with [Step 3](#).
 - To update an existing transcoder, locate the appropriate transcoder as described in the [“Finding a Transcoder” section on page 59-1](#) and continue with [Step 3](#).
- Step 3** Enter the appropriate settings as described in [Table 59-1](#).
- Step 4** Click **Save**.
- The window refreshes and shows specific information, including the status, for the transcoder that you just configured.
-

Additional Information

See the [“Related Topics” section on page 59-6](#).

Resetting a Transcoder

This section describes how to reset a Transcoder.

Procedure

- Step 1** Choose **Media Resources > Transcoder**.
- Step 2** From the Transcoders list, choose the transcoder that you want to reset.
- The window refreshes and displays the transcoder that you chose.

- Step 3** Click **Reset**.
The Reset dialog box displays.
- Step 4** Click **Reset** again.
-

Additional Information

See the [“Related Topics”](#) section on page 59-6.

Deleting a Transcoder

This section describes how to delete a transcoder.

Before You Begin

You cannot delete a transcoder that is assigned to a Media Resource Group. To find out which media resource groups are using the transcoder, from the Transcoder Configuration window, choose **Dependency Records** from the Related Links drop-down list box and click **Go**. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records”](#) section on page A-2. If you try to delete a transcoder that is in use, Cisco Unified CallManager displays an error message. Before deleting a transcoder that is currently in use, you must remove the transcoder from the media resource group(s) to which it is assigned.

Procedure

-
- Step 1** Locate the transcoder by using the procedure in the [“Finding a Transcoder”](#) section on page 59-1.
- Step 2** From the list of matching records, choose the transcoder that you want to delete.
The window refreshes and displays the transcoder that you chose.
- Step 3** Click **Delete**.
A message displays that states that you are about to permanently delete this transcoder and that you cannot undo this action.
- Step 4** If you want to continue, click **OK** or to cancel the deletion, click **Cancel**.
After the window refreshes, the transcoder that you deleted no longer appears in the transcoder list.
-

Additional Information

See the [“Related Topics”](#) section on page 59-6.

Transcoder Configuration Settings

Table 59-1 describes the transcoder configuration settings. For related procedures, see the “[Related Topics](#)” section on page 59-6.

Table 59-1 Transcoder Configuration Settings

Field	Description
Transcoder Type	Choose the appropriate transcoder type: Cisco Media Termination Point Hardware , Cisco IOS Media Termination Point , Cisco IOS Enhanced Media Termination Point , or Cisco Media Termination Point (WS-SVC-CMM) . For specific information on these transcoder types, refer to “ Transcoders ” in the <i>Cisco Unified CallManager System Guide</i> .
Device Name	This field displays if you chose Cisco IOS Media Termination Point or Cisco IOS Enhanced Media Termination Point as the transcoder type. Enter the same transcoding name that you entered in the gateway Command Line Interface (CLI).
Transcoder Name	For Cisco Media Termination Point (WS-SVC-CMM) transcoders, the system fills in this value based on the MAC address that you provide.
Description	Enter a description (up to 50 characters) or leave blank to generate automatically from the MAC address or device name that you provide.
MAC Address	For Cisco media termination point hardware or Cisco media termination point (WS-SVC-CMM), enter a MAC address, which must be 12 characters.
Subunit	For Cisco media termination point (WS-SVC-CMM) transcoders, choose a subunit from the drop-down list box.
Device Pool	Choose a device pool. For more detailed information on the chosen device pool, click View Details .
Special Load Information	Enter any special load information into the Special Load Information field or leave blank to use default. Valid characters include letters, numbers, dashes, dots (periods), and underscores.
Maximum Capacity	For Cisco media termination point (WS-SVC-CMM) transcoders, choose a maximum capacity from the drop-down list box.
Product-Specific Configuration	
Model-specific configuration fields defined by the device manufacturer	The device manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the “?” information icon below the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, refer to the documentation for the specific device that you are configuring or contact the manufacturer.

Related Topics

- [Finding a Transcoder, page 59-1](#)
- [Configuring a Transcoder, page 59-3](#)
- [Resetting a Transcoder, page 59-3](#)
- [Deleting a Transcoder, page 59-4](#)
- [Transcoder Configuration Settings, page 59-5](#)
- [Conference Bridge Configuration, page 54-1](#)
- [Media Termination Point Configuration, page 55-1](#)
- [Transcoders, *Cisco Unified CallManager System Guide*](#)
- [Transcoder Types in Cisco Unified CallManager Administration, *Cisco Unified CallManager System Guide*](#)



Media Resource Group Configuration

Media resource management comprises working with media resource groups and media resource group lists. Media resource management provides a mechanism for managing media resources, so all Cisco Unified CallManagers within a cluster can share them. Media resources provide conferencing, transcoding, media termination, annunciator, and music on hold services.

You can associate a Media Resource Group, a logical grouping of media servers, with a geographical location or with a site as desired. You can also form Media Resource Groups to control the usage of servers or the type of service (unicast or multicast) that is desired.

You can group devices of the following types into a single Media Resource Group:

- Conference Bridge (CFB)
- Media Termination Point (MTP)
- Music On Hold Server (MOH)
- Transcoder (XCODE)
- Annunciator (ANN)

Use the following topics to configure Media Resource Groups:

- [Finding a Media Resource Group, page 60-1](#)
- [Configuring a Media Resource Group, page 60-3](#)
- [Media Resource Group Configuration Settings, page 60-4](#)
- [Deleting a Media Resource Group, page 60-5](#)
- [Understanding Media Resources, *Cisco Unified CallManager System Guide*](#)
- [Media Resource Group and Media Resource Group List Configuration Checklist, *Cisco Unified CallManager System Guide*](#)

Finding a Media Resource Group

Because you might have several media resource groups in your network, Cisco Unified CallManager lets you locate specific media resource groups on the basis of specific criteria. Use the following procedure to locate media resource groups.

**Note**

During your work in a browser session, Cisco Unified CallManager Administration retains your media resource group search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your media resource group search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Media Resources > Media Resource Group**.

The Find and List Media Resource Group window displays. Use the two drop-down list boxes to search for a media resource group.

Step 2 From the first Find Media Resource Groups where drop-down list box, choose one of the following criteria:

- Name
- Description

**Note**

The criterion that you choose in this drop-down list box specifies how the list of media resource groups that your search generates will be sorted. For example, if you choose Description, the Description column will display as the left column of the results list.

From the second Find Media Resource Groups where drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.

**Tip**

To find all media resource groups that are registered in the database, click **Find** without entering any search text.

A list of discovered media resource groups displays by

- Media Resource Group name
- Description
- Multicast

**Note**

You can delete multiple media resource groups from the Find and List Media Resource Group window by checking the check boxes next to the appropriate media resource groups and clicking **Delete Selected**. You can delete all media resource groups in the window by clicking **Select All** and then clicking **Delete Selected**.

- Step 4** From the list of records, click the Media Resource Group icon or name, the Description, or the Multicast setting that matches your search criteria.

The window displays the media resource group that you choose.

Additional Information

See the [“Related Topics” section on page 60-6](#).

Configuring a Media Resource Group

Perform the following procedure to add, update, or copy a Media Resource Group.

**Note**

You cannot delete a media resource, such as a conference bridge, that is part of a Media Resource Group unless you first remove the resource from the Media Resource Group or you delete the Media Resource Group that contains the media resource.

Procedure

- Step 1** Choose **Media Resources > Media Resource Group**.

The Find and List Media Resource Group window displays.

- Step 2** Perform one of the followings tasks:

- To copy an media resource group, locate the appropriate media resource group as described in [“Finding a Media Resource Group” section on page 60-1](#). From the Search Results list, click the **Copy** icon that corresponds to the media resource group that you want to copy, and continue with [Step 3](#).
- To add a new media resource group, click the **Add New** button. The Media Resource Group Configuration window displays. Continue with [Step 3](#).
- To update an existing media resource group, locate the appropriate media resource group as described in [“Finding a Media Resource Group” section on page 60-1](#), and continue with [Step 3](#).

- Step 3** Enter the appropriate settings as described in [Table 60-1](#).

- Step 4** Click **Save**.

If you are copying a media resource group, you should change at least the media resource group name.

If you are adding a media resource group, the Status changes from *Ready* to *Insert completed*. The list of Media Resource Groups now includes the new Media Resource Group.

If you are updating an existing media resource group, the Status changes from *Ready* to *Update completed*.

To reset all devices in a Media Resource Group (both available and selected resources), click the **Reset Devices** button.



Note Resetting devices resets all devices that are associated with this Media Resource Group. Cisco Unified CallManager may drop active calls on affected gateways.

Additional Information

See the [“Related Topics” section on page 60-6](#).

Media Resource Group Configuration Settings

[Table 60-1](#) describes the configuration settings that are used for configuring Media Resource Groups. For more information about related procedures, see the [“Related Topics” section on page 60-6](#).

Table 60-1 Media Resource Group Configuration Settings

Field	Description
Media Resource Group Name	Enter a unique name in this required field for the Cisco Unified CallManager to identify the Media Resource Group. This name can comprise up to 50 characters. Valid characters include letters, numbers, spaces, dashes, dots (periods), and underscores.
Description	Enter a description for the Media Resource Group. This description can comprise up to 50 characters. Ensure Description does not contain double quotes (“”), less than (<), greater than (>), or the percent sign (%).
Devices for this Group	This area comprises two panes that are used to define the media resources for a Media Resource Group: Available Media Resources and Selected Media Resources.
Available Media Resources	This pane lists the media resources that can be chosen for a Media Resource Group. The list includes the following media resource types: • Conference Bridges (CFB) • Media Termination Points (MTP) • Music On Hold Servers (MOH) • Transcoders (XCODE) • Annunciator (ANN) Music On Hold servers that are configured for multicast are labeled as <i>(MOH)[Multicast]</i>. To add a media resource for this Media Resource Group, choose one from the list and click the down arrow. After a media resource is added, its name moves to the Selected Media Resources pane.

Table 60-1 Media Resource Group Configuration Settings (continued)

Field	Description
Selected Media Resources	This pane lists the media resources that were chosen for a Media Resource Group. For any Media Resource Group, you must choose at least one media resource. To delete (unselect) a media resource, choose its name in the list and click the up arrow.
Use Multicast for MOH Audio	To use multicast for Music On Hold Audio, check this check box. To do so, make sure that at least one of the Selected Media Resources is a multicast MOH server. Note The system administrator has responsibility for configuring or creating multicast audio sources.

Deleting a Media Resource Group

Perform the following procedure to delete an existing Media Resource Group.

Before You Begin

You cannot delete a Media Resource Group that is assigned to a Media Resource Group List. To find out which media resource groups lists are using the media resource group, in the Media Resource Group Configuration window, from the Related Links drop-down list box, choose **Dependency Records** and click **Go**. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#). If you try to delete a media resource group that is in use, Cisco Unified CallManager displays an error message. Before deleting a media resource group that is currently in use, you must perform either or both of the following tasks:

- Assign a different media resource group list to any media resource groups that are using the media resource group that you want to delete. See the [“Configuring a Media Resource Group List” section on page 61-2](#).
- Delete the media resource group lists that are using the media resource group that you want to delete. See the [“Deleting a Media Resource Group List” section on page 61-4](#).

Procedure

-
Step 1	Locate the media resource group by using the procedure in the “Finding a Media Resource Group” section on page 60-1 .
Step 2	From list of matching records, choose the media resource group that you want to delete.
Step 3	Click the Delete button. A message displays that states that you are about to permanently delete this media resource group and that you cannot undo this action.
Step 4	If you want to continue, click OK or to cancel the deletion, click Cancel . The chosen Media Resource Group no longer appears in the Media Resource Groups list.
-

Additional Information

See the [“Related Topics”](#) section on page 60-6.

Related Topics

- [Finding a Media Resource Group, page 60-1](#)
- [Configuring a Media Resource Group, page 60-3](#)
- [Media Resource Group Configuration Settings, page 60-4](#)
- [Deleting a Media Resource Group, page 60-5](#)
- [Accessing Dependency Records, page A-2](#)
- [Understanding Media Resources, *Cisco Unified CallManager System Guide*](#)
- [Media Resource Group and Media Resource Group List Configuration Checklist, *Cisco Unified CallManager System Guide*](#)

Media Resource Group List

- [Media Resource Group List Configuration, page 61-1](#)
- [Configuring a Media Resource Group List, page 61-2](#)
- [Deleting a Media Resource Group List, page 61-4](#)



Media Resource Group List Configuration

Media resource management comprises working with media resource groups and media resource group lists. Media resource management provides a mechanism for managing media resources, so all Cisco Unified CallManagers within a cluster can share them. Media resources provide conferencing, transcoding, media termination, annunciator, and music on hold services.

A Media Resource Group List provides a prioritized grouping of Media Resource Groups. An application selects the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that is defined in a Media Resource Group List.

Use the following topics to configure Media Resource Group Lists:

- [Finding a Media Resource Group List, page 61-1](#)
- [Configuring a Media Resource Group List, page 61-2](#)
- [Media Resource Group List Configuration Settings, page 61-3](#)
- [Deleting a Media Resource Group List, page 61-4](#)

Finding a Media Resource Group List

Because you might have several media resource group lists in your network, Cisco Unified CallManager lets you locate specific media resource group lists on the basis of specific criteria. Use the following procedure to locate media resource group lists.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your media resource group list search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your media resource group list search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Media Resources > Media Resource Group List**.

The Find and List Media Resource Group Lists window displays. Use the drop-down list box to search for a media resource group list.

- Step 2** From the Find Media Resource Group Lists where Name drop-down list box, choose the following criterion:
- begins with
 - contains
 - ends with
 - is exactly
 - is empty
 - is not empty
- Step 3** Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Tip To find all media resource group lists that are registered in the database, click **Find** without entering any search text.

A list of discovered media resource group lists displays by

- Media Resource Group List name



Note You can delete multiple media resource group lists from the Find and List Media Resource Group Lists window by checking the check boxes next to the appropriate media resource group lists and clicking **Delete Selected**. You can delete all media resource group lists in the window by clicking **Select All** and then clicking **Delete Selected**.

- Step 4** From the list of records, click the Media Resource Group List icon or name that matches your search criteria.

The window displays the media resource group list that you choose.

Additional Information

See the [“Related Topics” section on page 61-5](#).

Configuring a Media Resource Group List

Perform the following procedure to add, update, or copy a Media Resource Group List.



Note You cannot delete a Media Resource Group that is assigned to a Media Resource Group List unless you first remove the Media Resource Group from the Media Resource Group List(s) to which it is assigned or you delete the Media Resource Group List.

Procedure

- Step 1** Choose **Media Resources > Media Resource Group List**.
The Find and List Media Resource Group Lists window displays.

Step 2 Perform one of the followings tasks:

- To copy an media resource group list, locate the appropriate media resource group list as described in [“Finding a Media Resource Group List” section on page 61-1](#). From the Search Results list, click the **Copy** icon that corresponds to the media resource group list that you want to copy, and continue with [Step 3](#).
- To add a new media resource group list, click the **Add New** button. The Media Resource Group List Configuration window displays. Continue with [Step 3](#).
- To update an existing media resource group list, locate the appropriate media resource group list as described in [“Finding a Media Resource Group List” section on page 61-1](#), and continue with [Step 3](#).

Step 3 Enter the appropriate settings as described in [Table 61-1](#).

Step 4 Click **Save**.

If you are adding a new media resource group list, the Status changes to from *Ready* to *Insert completed*. The Media Resource Group Lists list now includes the new Media Resource Group List.

If you are copying a media resource group, you should change at least the media resource group name.

To reset all devices in a Media Resource Group List (both available and selected Media Resource Groups), click the **Reset Devices** button.



Note Resetting devices resets all devices that are associated with this Media Resource Group List. Cisco Unified CallManager may drop active calls on affected gateways.

Additional Information

See the [“Related Topics” section on page 61-5](#).

Media Resource Group List Configuration Settings

[Table 61-1](#) describes the configuration settings that are used for configuring Media Resource Group Lists. For more information about related procedures, see the [“Related Topics” section on page 61-5](#)

Table 61-1 Media Resource Group List Configuration Settings

Field	Description
Media Resource Group List Name	Enter a unique name in this required field for the Cisco Unified CallManager to identify the Media Resource Group List. This name can comprise up to 50 characters. Valid characters include letters, numbers, spaces, dashes, dots (periods), and underscores.

Table 61-1 Media Resource Group List Configuration Settings (continued)

Field	Description
Available Media Resource Groups	This window lists the media resource groups that can be chosen for a Media Resource Group List. The list includes only previously defined media resource groups. To add a media resource group for this Media Resource Group List, choose one from the list and click the down arrow that is located between the two panes. After a media resource group is added, its name moves to the Selected Media Resource Groups pane.
Selected Media Resource Groups	This pane lists the media resource groups that were chosen for a Media Resource Group List. For any Media Resource Group List, you must choose at least one media resource group. To delete (unselect) a media resource group, choose its name in the list and click the up arrow that is located between the two panes. Because media resource groups are listed in order of priority (highest to lowest), you must use the up and down arrows that are located to the right of this pane to reorder the Media Resource Group priority. To do so, choose a Media Resource Group in the list and use the up or down arrow to change its priority.

Deleting a Media Resource Group List

Perform the following procedure to delete an existing Media Resource Group List.



Note

You cannot delete a Media Resource Group List that is assigned to a device pool(s) or to a device(s). You must first modify the device pool(s) or device(s) to which a Media Resource Group List is assigned.

Procedure

- Step 1** Locate the media resource group list by using the procedure in the [“Finding a Media Resource Group List”](#) section on page 61-1.
- Step 2** From list of matching records, choose the media resource group list that you want to delete.
- Step 3** Click the **Delete** button.
A message displays that states that you are about to permanently delete this media resource group list and that you cannot undo this action.
- Step 4** If you want to continue, click **OK** or to cancel the deletion, click **Cancel**.
The chosen Media Resource Group List no longer appears in the Media Resource Groups List list.

Additional Information

See the [“Related Topics”](#) section on page 61-5.

Related Topics

- [Finding a Media Resource Group List, page 61-1](#)
- [Configuring a Media Resource Group List, page 61-2](#)
- [Media Resource Group List Configuration Settings, page 61-3](#)
- [Deleting a Media Resource Group List, page 61-4](#)
- [Media Resource Group Configuration, page 60-1](#)
- [Understanding Media Resources, *Cisco Unified CallManager System Guide*](#)
- [Media Resource Group and Media Resource Group List Configuration Checklist, *Cisco Unified CallManager System Guide*](#)



PART 5

Voice Mail Configuration





Cisco Voice-Mail Port Configuration

The optional Cisco Unity software, available as part of Cisco Unified Communications Solutions, provides voice-messaging capability for users when they are unavailable to answer calls. This section describes the procedures that are required for adding and configuring, updating, and deleting Cisco voice-mail ports by choosing Voice Mail from the Feature menu of the Cisco Unified CallManager window and choosing the submenu options.

For more information about configuring Cisco Unity, refer to the *Cisco Unified CallManager 4.0 Integration Guide for Cisco Unity 4.0*.

You can add and delete ports that are associated with a Cisco Unity voice-mail server to the Cisco Unified CallManager database without using the Cisco Voice Mail Port Wizard.

This section describes the following procedure:

- [Finding a Cisco Voice-Mail Port, page 62-1](#)
- [Configuring Cisco Voice-Mail Ports, page 62-3](#)
- [Cisco Voice-Mail Port Configuration Settings, page 62-4](#)
- [Deleting a Cisco Voice-Mail Port, page 62-6](#)

Finding a Cisco Voice-Mail Port

Because you will typically have a number of Cisco voice-mail ports in your network, Cisco Unified CallManager lets you locate specific Cisco voice-mail ports on the basis of specific criteria. Use the following procedure to locate Cisco voice-mail ports.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your Cisco voice-mail port search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your Cisco voice-mail port search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Voice Mail >Cisco Voice Mail Port**.

The Find and List Voice Mail Ports window displays. Use the two drop-down list boxes to search for a Cisco voice-mail port.

Step 2 From the first Find voice mail ports where drop-down list box, choose one of the following criteria:

- Device Name
- Description
- Directory Number
- Calling Search Space
- Device Pool



Note The criterion that you choose in this drop-down list box specifies how the list of Cisco voice-mail ports that your search generates will be sorted. For example, if you choose Device Pool, the Device Pool column will display as the left column of the results list.

From the second Find voice mail ports where drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Tip To find all Cisco voice-mail ports that are registered in the database, click **Find** without entering any search text.

A list of discovered Cisco voice-mail ports displays by

- Voice Mail Port icon
- Device Name
- Description
- Device Pool
- Status
- IP Address



Note You can delete multiple Cisco voice-mail ports from the Find and List Voice Mail Ports window by checking the check boxes next to the appropriate Cisco voice-mail ports and clicking **Delete Selected**. You can delete all Cisco voice-mail ports in the window by clicking the Select All button and clicking **Delete Selected**.

Step 4 From the list of records, click the Voice Mail Port icon, Device Name, Description, or associated Device Pool that matches your search criteria.

The window displays the Cisco voice-mail port that you choose.

Additional Information

See the [“Related Topics”](#) section on page 62-7.

Configuring Cisco Voice-Mail Ports

To connect a Cisco Unity voice-messaging system to Cisco Unified CallManager, you must add Cisco voice-mail ports to the Cisco Unified CallManager database.

**Tip**

You can also use the Cisco Voice Mail Port Wizard to add a new Cisco voice-mail server and ports or to add multiple ports to an existing server rather than the procedure that is described here. See [“Cisco Voice Mail Port Wizard”](#) section on page 63-1 for more information.

Perform this procedure to add individual Cisco voice-mail ports to the Cisco Unified CallManager database, or update or copy an existing voice-mail port.

Procedure

Step 1 Choose **Voice Mail > Cisco Voice Mail Port**.

The Find and List Voice Mail Ports window displays.

Step 2 Perform one of the followings tasks:

- To copy Cisco voice-mail port and its settings, locate the appropriate Cisco voice-mail port as described in [“Finding a Cisco Voice-Mail Port”](#) section on page 62-1. From the Search Results list, click the **Copy** icon that corresponds to the voice mail port that you want to copy, and continue with [Step 3](#).
- To add a new voice-mail port, click the **Add New** button. The Voice Mail Port Configuration window displays. Continue with [Step 3](#).
- To update an existing Cisco voice-mail port, locate the appropriate voice-mail port as described in [“Finding a Cisco Voice-Mail Port”](#) section on page 62-1. Click the voice mail port you want to update and continue with [Step 3](#).

Step 3 Enter the appropriate settings as described in [Table 62-1](#).

Step 4 Click **Save**.

If you are copying the basic settings of an existing Cisco voice mail port to apply to another Cisco voice-mail port, you must change the Port Name and Directory Number fields.

Additional Information

See the [“Related Topics”](#) section on page 62-7.

Cisco Voice-Mail Port Configuration Settings

Table 62-1 describes the Cisco voice-mail port configuration settings. For more information about related procedures, see the “[Related Topics](#)” section on page 62-7.

Table 62-1 Cisco Voice Mail Port Configuration Settings

Field	Description
Device Information	
Port Name	Enter a name to identify the Cisco voice-mail port. You must add a device for each port on Cisco voice-messaging system. If 24 ports exist, you must define 24 devices. The name must have no more than nine characters. Note For Cisco Unity, this name must match the name in the Unity Telephony Integration Manager (UTIM) configuration files, such as CiscoUM-VI1 or Cisco UM-VI2.
Description	Enter the purpose of the device.
Device Pool	Choose the default value or a specific device pool.
Calling Search Space	From the drop-down list box, choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that were called from this device. Choose the name of the calling search space that allows calls to the subscriber phones and to any network devices. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the Max List Box Items enterprise parameter specifies, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Calling Search Space window. Enter a partial calling search space name in the List items where Name contains field. Click the desired calling search space name in the list of calling search spaces that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when performing automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.
Location	Choose the default value None. The location specifies the total bandwidth that is available for calls to and from this device. A location setting of <i>None</i> means that the locations feature does not keep track of the bandwidth that is device consumes.

Table 62-1 Cisco Voice Mail Port Configuration Settings (continued)

Field	Description
SCCP Phone Security Profile	From the drop-down list box, choose a security profile based on the device security mode that you want to apply to the port. Cisco voice mail ports do not support Certificate Authority Proxy Function (CAPF), even though the security profile contains settings for CAPF; Cisco Unified CallManager ignores these settings after you apply the profile to the port. For more information on security profiles, refer to the <i>Cisco Unified CallManager Security Guide</i>.
Directory Number Information	
Directory Number	Enter the number that is associated with this voice-mail port. Make sure that this field is unique in combination with the Partition field.
Partition	Choose the partition to which the directory number belongs. Choose <None> if partitions are not used. If you choose a partition, you must choose a calling search space that includes that partition. You can configure the number of partitions that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more partitions exist than the Max List Box Items enterprise parameter specifies, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Partition window. Enter a partial partition name in the List items where Name contains field. Click the desired partition name in the list of partitions that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.
Calling Search Space	From the drop-down list box, 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. If you choose a partition, you must choose a calling search space that includes that partition. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the Max List Box Items enterprise parameter specifies, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Calling Search Space window. Enter a partial calling search space name in the List items where Name contains field. Click the desired calling search space name in the list of calling search spaces that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.

Table 62-1 Cisco Voice Mail Port Configuration Settings (continued)

Field	Description
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.
Internal Caller ID Display	This field indicates text that displays on the called party phone when a call is placed from this line.
Internal Caller ID Display (ASCII format)	This field indicates text that appears on the called party phone, in ASCII format, when a call is placed from this line.
External Number Mask	Specify the mask that is used to format caller ID information for external (outbound) calls. The mask can contain up to 50 characters. Enter the literal digits that you want to display in the caller ID information and use Xs to represent the directory number of the device. When Automated Alternate Routing (AAR) routes calls due to insufficient bandwidth, Cisco Unified CallManager uses the value in this field to place the call if sufficient bandwidth is not available. Example DN 1000 (external mask 9728131000) calls DN 1001 (external mask 2144131001). If insufficient bandwidth blocks the call, Cisco Unified CallManager uses the AAR prefix digits along with 2144131001 to place the call to 1001.

Deleting a Cisco Voice-Mail Port

To delete a single Cisco voice-mail port from Cisco Unified CallManager, follow these procedures.

Before You Begin

When you delete a Cisco voice-mail port that a directory number uses, the number remains in the Cisco Unified CallManager database. To determine which directory numbers are using the voice-mail port, in the Voice Mail Port Configuration window, choose **Dependency Records** from the Related Links drop-down list box and click **Go**. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#).

When you delete a voice-mail port that is in use, Cisco Unified CallManager displays a message. Before deleting a voice-mail port that is currently in use, you can assign a different voice-mail port to any directory number that is using the voice-mail port that you want to delete. See the [“Configuring a Directory Number” section on page 49-2](#).

After you delete the voice-mail port, you can delete the directory number that was using the voice-mail port. See the [“Deleting Unassigned Directory Numbers” section on page 51-3](#).

**Tip**

Instead of using the procedure that is described here, you can use the Cisco Voice Mail Port Wizard to delete ports from an existing server. See [“Cisco Voice Mail Port Wizard” section on page 63-1](#) for more information.

Procedure

-
- Step 1** Find the Cisco voice-mail port by using the procedure in the [“Finding a Cisco Voice-Mail Port” section on page 62-1](#).
- Step 2** Click the Cisco voice-mail port that you want to delete.
- Step 3** Click **Delete**.
-

Additional Information

See the [“Related Topics” section on page 62-7](#).

Related Topics

- [Finding a Cisco Voice-Mail Port, page 62-1](#)
- [Configuring Cisco Voice-Mail Ports, page 62-3](#)
- [Cisco Voice-Mail Port Configuration Settings, page 62-4](#)
- [Deleting a Cisco Voice-Mail Port, page 62-6](#)
- [Cisco Voice Mail Port Wizard, page 63-1](#)
- [Cisco Unity Configuration Checklist](#), *Cisco Unified CallManager System Guide*



Cisco Voice Mail Port Wizard

The optional Cisco Unity software, available as part of Cisco Unified Communications Solutions, provides voice-messaging capability for users when they are unavailable to answer calls. This section describes the procedures that are required for adding and configuring Cisco voice-mail ports in Cisco Unified CallManager for voice-messaging systems.

For more information about configuring Cisco Unity, refer to the *Cisco Unified CallManager 4.0 Integration Guide*.

For more information on voice-messaging connectivity to Cisco Unified CallManager, refer to “[Voice Mail Connectivity to Cisco Unified CallManager](#)” in the *Cisco Unified CallManager System Guide*.

The Cisco Voice Mail Port Wizard tool allows Cisco Unified CallManager administrators to quickly add and delete ports that are associated with a Cisco voice-mail server to the Cisco Unified CallManager database. This The following sections describes the procedures.

Adding a New Cisco Voice-Mail Server and Ports

To use the Cisco Voice Mail Port Wizard to add a new Cisco voice-mail server and ports to the Cisco Unified CallManager database, perform the following steps.

Before You Begin

The Cisco Voice Mail Port Wizard requires a range of consecutive directory numbers for the voice-mail ports. Make sure the voice-mail pilot number and subsequent numbers are available.

Procedure

-
- Step 1** Choose **Voice Mail > Cisco Voice Mail Port Wizard**.
- If no Cisco voice-mail ports exist, enter the name of the Cisco voice-mail server to add and continue with [Step 5](#). Otherwise, continue with [Step 2](#).
- Step 2** Choose **Create a new Cisco Voice Mail server and add ports to it**.
- Step 3** Click **Next**.
- Step 4** Enter the name of the Cisco voice-mail server.



Note

For Cisco Unity, this name must match the name in the Unity Telephony Integration Manager (UTIM) configuration file (the default specifies CiscoUM-VI). The wizard automatically appends the *<port number>* suffix when it adds the ports.

- Step 5** Click **Next**.
The Cisco Voice Mail Ports window displays.
- Step 6** From the drop-down list box, choose the number of ports to add.
- Step 7** Click **Next**.
The Cisco Voice Mail Device Information window displays.
- Step 8** Enter the appropriate configuration settings, as described in [Table 63-1](#). The wizard applies these configuration settings to all the new ports.

Table 63-1 Voice Mail Port Wizard Device Information Configuration Settings

Field	Description
Description	Enter the purpose of device.
Device Pool	Choose the default value Default or any defined device pool.
Calling Search Space	From the drop-down list box, 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. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the Max List Box Items enterprise parameter specifies, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Calling Search Space window. Enter a partial calling search space name in the List items where Name contains field. Click the desired calling search space name in the list of calling search spaces that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.
Location	Choose the default value None or any defined location. The location specifies the total bandwidth that is available for calls to and from this device. A location setting of <i>None</i> means that the locations feature does not keep track of the bandwidth that is consumed by this device.
SCCP Phone Security Profile	From the drop-down list box, choose a security profile based on the device security mode that you want to apply to the port. Cisco voice mail ports do not support Certificate Authority Proxy Function (CAPF), even though the security profile contains settings for CAPF; Cisco Unified CallManager ignores these settings after you apply the profile to the port. For more information on security profiles, refer to the <i>Cisco Unified CallManager Security Guide</i>.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.

Step 9 Click **Next**.

The Cisco Voice Mail Directory Numbers window displays.

Step 10 Enter the directory number settings for the new Cisco voice-mail server as described in [Table 63-2](#).

Table 63-2 **Voice Mail Port Wizard Directory Number Configuration Settings**

Field	Description
Beginning Directory Number	Enter the number that people call to access the Cisco voice-mail server. Each new port receives the next available directory number.
Partition	Choose the partition to which this set of directory numbers belong. Choose None if partitions are not used. If you choose a partition, you must choose a calling search space that includes that partition. You can configure the number of partitions that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more partitions exist than the Max List Box Items enterprise parameter specifies, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Partition window. Enter a partial partition name in the List items where Name contains field. Click the desired partition name in the list of partitions that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.
Calling Search Space	From the drop-down list box, 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. If you choose a partition, you must choose a calling search space that includes that partition. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the Max List Box Items enterprise parameter specifies, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Calling Search Space window. Enter a partial calling search space name in the List items where Name contains field. Click the desired calling search space name in the list of calling search spaces that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of <i>None</i> specifies that no rerouting of blocked calls will be attempted.
Internal Caller ID Display	This field indicates text that displays on the calling party phone when a call is placed to this line.
Internal Caller ID Display (ASCII format)	This field indicates text that displays on the calling party phone, in ASCII format, when a call is placed to this line.

Table 63-2 **Voice Mail Port Wizard Directory Number Configuration Settings (continued)**

Field	Description
External Number Mask	Specify the mask that is used to format caller ID information for external (outbound) calls. The mask can contain up to 50 characters. Enter the literal digits that you want to display in the caller ID information and use Xs to represent the directory number of the device.

Step 11 Click **Next**.

A window that asks whether you want to add these directory numbers to a line group displays.

Step 12 Choose one of the options that display:

- If you choose to add directory numbers to a new line group, skip to [Step 13](#).
- If you choose to add directory numbers to an existing line group, skip to [Step 15](#).
- If you choose to add directory numbers to a line group later, skip to [Step 17](#).

Step 13 Choose the “Yes. Add directory numbers to a **new** Line Group” option and click **Next**.

Step 14 In the Line Group window that displays, enter the name of the new line group and click **Next**.

The Ready to Add Cisco Voice Mail Ports summary window displays. This summary window lists the settings that you configured in the previous windows. The Cisco Voice Mail Port Wizard automatically assigns the correct values for each port.

Skip to [Step 18](#).

Step 15 Choose the “Yes. Add directory numbers to an **existing** Line Group” option and click **Next**.

Step 16 In the Line Group window that displays, choose a line group from the Line Group Name drop-down list box and click **Next**.

The Ready to Add Cisco Voice Mail Ports summary window displays. This summary window lists the settings that you configured in the previous windows. The Cisco Voice Mail Port Wizard automatically assigns the correct values for each port.

Skip to [Step 18](#).

Step 17 Choose the “No. I will add them later” option and click **Next**.

The Ready to Add Cisco Voice Mail Ports summary window displays. This summary window lists the settings that you configured in the previous windows. The Cisco Voice Mail Port Wizard automatically assigns the correct values for each port.

Step 18 If this information is correct, click **Finish** to add the new ports.

If the information shown is not correct, click the **Back** button to edit the information or **Cancel** to quit without adding any ports.

Step 19 After the Cisco Voice Mail Port Wizard finishes adding the new voice-mail ports that you specified, the Cisco Voice Mail Port Wizard Results window displays.

The window directs you to the other steps that you need to complete before you can start using these new voice-mail ports.

Next Steps

Make sure that you set up the message-waiting indicator (MWI) device. For more information, refer to the [“Cisco Unity Configuration Checklist”](#) section in the *Cisco Unified CallManager System Guide*.

Additional Topics

See the [“Related Topics”](#) section on page 63-6.

Adding Ports to an Existing Cisco Voice-Mail Server

To use the Cisco Voice Mail Port Wizard to add ports to an existing Cisco voice-mail server, perform the following steps.

Before You Begin

The Cisco Voice Mail Port Wizard requires a range of consecutive directory numbers for the voice-mail ports. Make sure that the voice-mail pilot number and subsequent numbers are available.

The voice-mail pilot number designates the number that people call to access the Cisco voice-mail server.

Procedure

-
Step 1	Choose Voice Mail > Cisco Voice Mail Port Wizard .
Step 2	Choose Add ports to an existing Cisco Voice Mail server .
Step 3	Click Next . The Cisco Voice Mail Server window displays.
Step 4	From the drop-down list box, choose the name of an existing Cisco voice-mail server (pilot number) and click Next . The Cisco Voice Mail Ports window displays and identifies the number of ports that are currently configured.
Step 5	From the drop-down list box, choose the number of ports to add and click Next . The Cisco Voice Mail Directory Numbers window displays the configuration information for the Cisco voice-mail server to which you added the ports. The Cisco Voice Mail Port Wizard automatically selects consecutive directory numbers following the last port and uses the same Partition, Calling Search Space, Display, AAR Group, and External Number Mask settings as the Cisco voice-mail pilot directory number. You can enter a different range of directory numbers in the New Directory Numbers field.
Step 6	If you need to change the number of ports, click the Back button.
Step 7	Click Next . The Ready to Add Cisco Voice Mail Ports summary window displays. This summary window lists the settings that you configured in the previous windows. The Cisco Voice Mail Port Wizard automatically assigns the correct values for each port.
Step 8	If this information is correct, click Finish to add the new ports. If the information shown is not correct, click the Back button to edit the information or click Cancel to quit without adding any ports.
-

Additional Topics

See the [“Related Topics”](#) section on page 63-6.

Deleting Ports from an Existing Cisco Voice-Mail Server

To delete ports from an existing Cisco voice-mail server, perform the following steps to use the Cisco Voice Mail Port Wizard.

Procedure

-
- Step 1** Choose **Voice Mail > Cisco Voice Mail Port Wizard**.
- Step 2** Choose **Delete ports from an existing Cisco Voice Mail server** and click **Next**.
The Cisco Voice Mail Server window displays.
- Step 3** From the drop-down list box, choose the name of an existing Cisco voice-mail server (pilot number) and click **Next**.
The Cisco Voice Mail Ports window, which indicates the number of ports that are currently configured, displays.
- Step 4** From the drop-down list box, choose the number of ports to delete and click **Next**.
The Ready to Delete Cisco Voice Mail Ports summary window displays.
The summary window provides information about the ports to be deleted. The Cisco Voice Mail Port Wizard automatically updates the port numbers and directory numbers so they are consecutive.
- Step 5** If this information is correct, click **Finish** to delete the selected ports.
If the information shown is not correct, click the **Back** button to edit the information or to quit without deleting any ports, click **Cancel**.
-

Additional Topics

See the [“Related Topics”](#) section on page 63-6.

Related Topics

- [Cisco Voice Mail Port Wizard, page 63-1](#)
- [Adding a New Cisco Voice-Mail Server and Ports, page 63-1](#)
- [Adding Ports to an Existing Cisco Voice-Mail Server, page 63-5](#)
- [Deleting Ports from an Existing Cisco Voice-Mail Server, page 63-6](#)
- [Message Waiting Configuration, page 64-1](#)
- [Cisco Unity Configuration Checklist, Cisco Unified CallManager System Guide](#)



Message Waiting Configuration

The Message Waiting Configuration window allows you to define a message waiting on or message waiting off directory number that a directory-connected based voice-messaging system uses to determine whether to set or clear a message waiting indication for a particular Cisco IP Phone.

The following topics provide information on message waiting configuration:

- [Finding a Message Waiting Number, page 64-1](#)
- [Configuring Message Waiting, page 64-3](#)
- [Message Waiting Configuration Settings, page 64-3](#)
- [Voice Mail Connectivity to Cisco Unified CallManager, Cisco Unified CallManager System Guide](#)
- [Cisco Unity Configuration Checklist, Cisco Unified CallManager System Guide](#)

Finding a Message Waiting Number

Because you might have several message-waiting numbers in your network, Cisco Unified CallManager lets you locate specific message-waiting numbers on the basis of specific criteria. Use the following procedure to locate message-waiting numbers.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your message-waiting number search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your message-waiting number search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Voice Mail > Message Waiting**.

The Find and List Message Waiting Numbers window displays. Use the three drop-down list boxes to search for a message-waiting number.

Step 2 From the first Find numbers where drop-down list box, choose one of the following criteria:

- Directory Number
- Partition
- Calling Search Space
- Description

**Note**

The criterion that you choose in this drop-down list box specifies how the list of message-waiting numbers that your search generates will be sorted. For example, if you choose Partition, the Partition column will display as the left column of the results list.

From the second Find numbers where drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is empty
- is not empty

From the Message Waiting Indicator is drop-down list box, choose one of the following criteria:

- Both
- On
- Off

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.

**Tip**

To find all message-waiting numbers that are registered in the database, click **Find** without entering any search text.

A list of discovered message-waiting numbers displays by

- Message Waiting Indicator icon (green if on, red if off)
- Directory Number
- Partition
- Calling Search Space
- Description

**Note**

You can delete multiple message-waiting numbers from the Find and List Message Waiting Numbers window by checking the check boxes next to the appropriate message-waiting numbers and clicking **Delete Selected**. You can delete all message-waiting numbers in the window by checking the check box in the Matching records title bar and clicking **Delete Selected**.

Step 4 From the list of records, click the MWI icon, directory number, associated partition, or calling search space that matches your search criteria.

The window displays the message-waiting number that you choose.

Additional Information

See the [“Related Topics” section on page 64-5](#).

Configuring Message Waiting

To configure message waiting for use with voice-messaging systems, use the following procedure.

Procedure

Step 1 Choose **Voice Mail > Message Waiting**.

Step 2 Click the **Add New**.

The Message Waiting Number Configuration window displays.

Step 3 Enter the appropriate settings as described in [Table 64-1](#).



Note The voice-messaging system only uses the message-waiting on/off directory number to turn on the message-waiting indicator. Because Cisco Unified CallManager does not use the Message Waiting on/off number for receiving calls, the Display, Forward All, Forward Busy, and Forward No Answer fields do not get used.

Step 4 To add this device to the system, click **Save**.

Additional Information

See the [“Related Topics”](#) section on page 64-5.

Message Waiting Configuration Settings

[Table 64-1](#) describes the Message Waiting configuration settings.

Table 64-1 Message Waiting Configuration Settings

Field Name	Description
Message Waiting Number	Enter the Cisco Message Waiting directory number. Make sure that this number is not used within the Cisco Unified CallManager auto-registration range.
Description	Enter up to 30 alphanumeric characters for a description of the message-waiting directory number.
Message Waiting Indicator	Click On or Off .

Table 64-1 **Message Waiting Configuration Settings (continued)**

Field Name	Description
Partition	If partitions are being used, choose the appropriate partition from the drop-down list box. If you do not want to restrict access to the message-waiting device directory number, choose <None> for the partition. You can configure the number of partitions that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more partitions exist than the Max List Box Items enterprise parameter specifies, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Partition window. Enter a partial partition name in the List items where Name contains field. Click the desired partition name in the list of partitions that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters. Note Make sure that the combination of message- waiting device directory number and partition is unique within the Cisco Unified CallManager cluster.
Calling Search Space	If partitions and calling search spaces are used, from the drop-down list box, choose a calling search space that includes the partitions of the DNs on all phones whose lamps you want to turn on (the partition that is defined for a phone DN must be in a calling search space that the MWI device uses). If partitions and calling search spaces are used, from the drop-down list box, choose a calling search space that includes the partitions of the DNs on all phones whose lamps you want to turn on (the partition that is defined for a phone DN must be in a calling search space that the MWI device uses). You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the Max List Box Items enterprise parameter specifies, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Calling Search Space window. Enter a partial calling search space name in the List items where Name contains field. Click the desired calling search space name in the list of calling search spaces that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.

Additional Information

See the [“Related Topics”](#) section on page 64-5.

Related Topics

- [Finding a Message Waiting Number, page 64-1](#)
- [Configuring Message Waiting, page 64-3](#)
- [Message Waiting Configuration Settings, page 64-3](#)
- [Voice Mail Connectivity to Cisco Unified CallManager](#), *Cisco Unified CallManager System Guide*
- [Cisco Unity Configuration Checklist](#), *Cisco Unified CallManager System Guide*
- [Voice-Mail Profile Configuration, page 66-1](#)
- [Directory Number Configuration Settings, page 49-6](#)



Cisco Voice-Mail Pilot Configuration

The voice mail-pilot number designates the directory number that you dial to access your voice messages. Cisco Unified CallManager automatically dials the voice-messaging number when you press the Messages button on your phone. Each pilot number can belong to a different voice-messaging system.

The following topics provide information on voice-mail pilot configuration:

- [Finding a Cisco Voice-Mail Pilot, page 65-1](#)
- [Configuring the Voice-Mail Pilot Number, page 65-3](#)
- [Voice-Mail Pilot Configuration Settings, page 65-3](#)
- [Deleting a Voice-Mail Pilot Number, page 65-4](#)
- [Voice Mail Connectivity to Cisco Unified CallManager, *Cisco Unified CallManager System Guide*](#)
- [Cisco Unity Configuration Checklist, *Cisco Unified CallManager System Guide*](#)

Finding a Cisco Voice-Mail Pilot

Because you may have several Cisco voice-mail pilots in your network, Cisco Unified CallManager lets you locate specific Cisco voice-mail pilots on the basis of specific criteria. Use the following procedure to locate Cisco voice-mail pilots.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your Cisco voice-mail pilot search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your Cisco voice-mail pilot search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Voice Mail > Voice Mail Pilot**.

The Find and List Voice Mail Pilots window displays. Use the two drop-down list boxes to search for a Cisco voice-mail pilot.

Step 2 From the first Find voice mail pilots where drop-down list box, choose one of the following criteria:

- Voice Mail Pilot Number
- Description
- Calling Search Space



Note The criterion that you choose in this drop-down list box specifies how the list of Cisco voice-mail pilots that your search generates will be sorted. For example, if you choose Calling Search Space, the Calling Search Space column will display as the left column of the results list.

From the second Find voice mail pilots where drop-down list box, choose one of the following criteria:

- begins with
- contains
- is exactly
- ends with
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Tip To find all Cisco voice-mail pilots that are registered in the database, click **Find** without entering any search text.

A list of discovered Cisco voice-mail pilots displays by

- Description
- Pilot Number
- Calling Search Space



Note You can delete multiple Cisco voice-mail pilots from the Find and List Voice Mail Pilots window by checking the check boxes next to the appropriate Cisco voice-mail pilots and clicking **Delete Selected**. You can delete all Cisco voice-mail pilots in the window by checking the check box in the Matching records title bar and clicking **Delete Selected**.

Step 4 From the list of records, click the Voice Mail Pilot icon, Device Name, Description, or associated Device Pool that matches your search criteria.

The window displays the Cisco voice-mail pilot that you choose.

Additional Information

See the [“Related Topics”](#) section on page 65-4.

Configuring the Voice-Mail Pilot Number

To configure the voice-mail pilot number, perform these procedures.

Procedure

-
- Step 1** Choose **Voice Mail > Voice Mail Pilot**.
- Step 2** Click the **Add New** link.
- Step 3** Configure the appropriate settings as described in [Table 65-1](#).
- Step 4** To add the new voice-mail pilot number or to update the settings for an existing voice-mail pilot number, click **Save**.
-

Additional Information

See the “[Related Topics](#)” section on page 65-4.

Voice-Mail Pilot Configuration Settings

[Table 65-1](#) describes the voice-mail pilot configuration settings.

Table 65-1 *Voice-Mail Pilot Configuration Settings*

Field	Description
Voice Mail Pilot Number	Enter a number to identify the voice mail pilot number.
Calling Search Space	From the drop-down list box, 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 pilot number. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the Max List Box Items enterprise parameter specifies, the ellipsis button (...) displays next to the drop-down list box. Click the (...) button to display the Select Calling Search Space window. Enter a partial calling search space name in the List items where Name contains field. Click the desired calling search space name in the list of calling search spaces that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.
Description	Enter the description of the pilot number.
Make this the default Voice Mail Pilot for the system	Check the check box to make this pilot number the default Voice Mail Pilot for the system. Note If you check the Default box, this voice mail pilot number replaces your current default pilot number.

Additional Information

See the [“Related Topics”](#) section on page 65-4.

Deleting a Voice-Mail Pilot Number

To delete the voice-mail pilot number, perform these procedures. You cannot delete the default or the *No Voice Mail* profile numbers.

Before You Begin

You cannot delete voice-mail pilot numbers that a voice-mail profile uses. To find out which voice-mail profiles are using the voice-mail pilot, in the Voice Mail Pilot Configuration window, choose **Dependency Records** from the Related Links drop-down list box and click **Go**. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records”](#) section on page A-2. If you try to delete a voice-mail pilot that is in use, Cisco Unified CallManager displays a message. Before deleting a voice-mail pilot that is currently in use, you must perform either or both of the following tasks:

- Assign a different voice-mail pilot to any voice-mail profiles that are using the voice-mail pilot that you want to delete. See the [“Configuring a Voice-Mail Profile”](#) section on page 66-2.
- Delete the voice-mail profiles that are using the voice-mail pilot that you want to delete. See the [“Deleting a Voice-Mail Profile”](#) section on page 66-3.

Procedure

Step 1 Choose **Voice Mail > Voice Mail Pilot**.

Step 2 Click the Cisco voice-mail pilot that you want to delete.

Step 3 Click **Delete**.

A confirmation window displays.



Note If you choose the default or the *No Voice Mail* pilot numbers, the Delete button does not display.

Step 4 To delete the voice-mail pilot, click **OK** or to cancel the deletion process, click **Cancel**.

If a voice-mail profile uses this voice-mail pilot number, a message displays and indicates the number of voice-mail profiles that use this voice-mail pilot number.

Additional Information

See the [“Related Topics”](#) section on page 65-4.

Related Topics

- [Finding a Cisco Voice-Mail Pilot, page 65-1](#)
- [Configuring the Voice-Mail Pilot Number, page 65-3](#)

- [Voice-Mail Pilot Configuration Settings, page 65-3](#)
- [Deleting a Voice-Mail Pilot Number, page 65-4](#)
- [Voice Mail Connectivity to Cisco Unified CallManager](#), *Cisco Unified CallManager System Guide*
- [Cisco Unity Configuration Checklist](#), *Cisco Unified CallManager System Guide*
- [Message Waiting Configuration, page 64-1](#)
- [Voice-Mail Profile Configuration, page 66-1](#)



Voice-Mail Profile Configuration

The Voice Mail Profile Configuration window of Cisco Unified CallManager Administration allows you to define any line-related voice-messaging information.



Note

A voice-mail profile gets assigned to a directory number, not a device.

The following topics provide information on voice-mail profiles:

- [Finding Voice-Mail Profiles, page 66-1](#)
- [Configuring a Voice-Mail Profile, page 66-2](#)
- [Voice-Mail Profile Configuration Settings, page 66-3](#)
- [Voice Mail Connectivity to Cisco Unified CallManager](#), *Cisco Unified CallManager System Guide*
- [Cisco Unity Configuration Checklist](#), *Cisco Unified CallManager System Guide*

Finding Voice-Mail Profiles

Because you may have several voice-mail profiles in your network, Cisco Unified CallManager lets you locate specific voice-mail profiles on the basis of specific criteria. Use the following procedure to locate voice-mail profiles.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your voice-mail profile search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your voice-mail profile search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Voice Mail > Voice Mail Profile**.

The Find and List Voice Mail Profiles window displays.

Step 2 From the drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with

- is exactly
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Note To find all voice-mail profiles that are registered in the database, click **Find** without entering any search text.

A list of discovered calling search spaces displays by

- Name
- Description
- Pilot/Calling Search Space

Step 4 From the list of records, click the voice-mail profile that matches your search criteria.
The window displays the voice-mail profile that you choose.

Step 5 To list all available voice-mail profiles, leave the criteria blank and click **Find**.

Additional Information

See the [“Related Topics” section on page 66-4](#).

Configuring a Voice-Mail Profile

To configure a voice-mail profile for a directory number, to copy a voice-mail profile or to update an existing voice-mail profile use the following procedure.

Procedure

Step 1 In the menu bar, choose **Voice Mail > Voice Mail Profile**.

The Find and List Voice Mail Profiles window displays.

Step 2 Perform one of the followings tasks:

- To copy a voice-mail profile, locate the appropriate voice-mail profile as described in [“Finding Voice-Mail Profiles” section on page 66-1](#). From the Search Results list, click the **Copy** icon that corresponds to the voice-mail profile that you want to copy and continue with [Step 3](#).
- To configure a voice-mail profile for a directory number, click the **Add New** button. The Voice Mail Profile Configuration window displays. Continue with [Step 3](#).
- To update an existing voice-mail profile, locate the appropriate voice-mail profile as described in [“Finding Voice-Mail Profiles” section on page 66-1](#) and continue with [Step 3](#).

Step 3 Configure the appropriate settings as described in [Table 66-1](#).

Step 4 Click **Save**.

If you are updating an existing voice-mail profile, click **Restart Devices** to restart all devices that are associated with the voice-mail profile.

Additional Information

See the [“Related Topics” section on page 66-4](#).

Voice-Mail Profile Configuration Settings

[Table 66-1](#) describes the voice-mail profile configuration settings. For more information about related procedures, see the [“Related Topics” section on page 66-4](#).

Table 66-1 Voice Mail Profile Configuration Settings

Field	Description
Voice Mail Profile Name	Enter a name to identify the voice-mail profile.
Description	Enter the description of the profile.
Voice Mail Pilot	Choose the appropriate voice-mail pilot number that is defined in the Voice Mail Pilot Configuration or Use Default .
Voice Mail Box Mask	Specify the mask that is used to format the voice mailbox number for auto-registered phones. When a call is forwarded to a voice-messaging system from a directory line on an auto-registered phone, Cisco Unified CallManager applies this mask to the number that is configured in the Voice Mail Box field for that directory line. For example, if you specify a mask of 972813XXXX, the voice mailbox number for directory number 7253 becomes 9728137253. If you do not enter a mask, the voice mailbox number matches the directory number (7253 in this example). By default, Cisco Unified CallManager sets the voice mailbox number to the same value as the directory number. You can change the voice mailbox number when configuring the directory number. See the “Directory Number Configuration Overview” section on page 49-1 for more information.
Make This the Default Voice Mail Profile for the System	Check the check box to make this profile name the default. Note If you check the Default check box, this voice-mail profile replaces your current default profile.

Deleting a Voice-Mail Profile

To delete a voice-mail profile, use the following procedure. You cannot delete the default profile or the No Voice Mail profile.

Before You Begin

You cannot delete a voice-mail profile that a directory number uses. To find out which directory numbers are using the voice-mail profiles, in the Voice Mail Profile Configuration window, choose **Dependency Records** from the Related Links drop-down list box and click **Go**. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#). If you try to delete a voice-mail profile that is in use, Cisco Unified CallManager displays a message. Before deleting a voice-mail profile that is currently in use, you must perform either or both of the following tasks:

- Assign a different voice-mail profile to any devices that are using the voice-mail profile that you want to delete.
- Delete the devices that are using the voice-mail profile that you want to delete.

Procedure

-
Step 1	To locate the voice-mail profile that you want to delete, follow the procedure on “Finding Voice-Mail Profiles” section on page 66-1 .
Step 2	Check the check box next to the voice-mail profiles that you want to delete. To select all the voice-mail profiles in the window, check the check box in the matching records title bar.
Step 3	Click Delete Selected .
-

Additional Information

See the [“Related Topics” section on page 66-4](#).

Related Topics

- [Finding Voice-Mail Profiles, page 66-1](#)
- [Configuring a Voice-Mail Profile, page 66-2](#)
- [Voice-Mail Profile Configuration Settings, page 66-3](#)
- [Voice Mail Connectivity to Cisco Unified CallManager, Cisco Unified CallManager System Guide](#)
- [Cisco Unity Configuration Checklist, Cisco Unified CallManager System Guide](#)



PART 6

Device Configuration





CTI Route Point Configuration

A computer telephony integration (CTI) route point designates a virtual device that can receive multiple, simultaneous calls for application-controlled redirection.

For first-party call control, you can optionally add a CTI port for each active voice line (the CTI application determines this). Applications that use CTI route points and CTI ports include Cisco SoftPhone, Cisco IP Auto Attendant, and Cisco IP Interactive Voice Response System. After you add a CTI route point to Cisco Unified CallManager Administration, information from the RIS Data Collector service displays in the CTI Route Point Configuration window. When available, the IP address of the device and the name of the Cisco Unified CallManager with which the device registered display.

For detailed instructions on how to configure CTI route points and CTI ports that are associated with these applications, refer to the documentation and online help that is included with these applications.

This section describes the following basic procedure:

- [Finding CTI Route Points, page 67-1](#)
- [Configuring a CTI Route Point, page 67-2](#)
- [CTI Route Point Configuration Settings, page 67-3](#)
- [Deleting a CTI Route Point, page 67-4](#)
- [Resetting a CTI Route Point, page 67-5](#)

Finding CTI Route Points

To find and list CTI route points, perform the following procedure.

Procedure

Step 1 Choose **Device > CTI Route Point**.

The Find and List Route Points window displays.

Step 2 Choose the search criteria to use. To list all items, do not enter any search text or use “Device Name is not empty” as the search criterion.

Step 3 Click **Find**.

The window refreshes to display a list of the CTI route points that match the specified search criteria.

Step 4 To view the next set of CTI route points, click **Next**.



Note

You can delete or reset multiple CTI route points from the Find and List Route Points window by checking the check boxes next to the appropriate CTI route points and clicking **Delete Selected** to delete the CTI route points or clicking **Reset Selected** to reset the CTI route points. You can choose all CTI route points in the window by clicking **Select All**.

Additional Information

See the [“Related Topics” section on page 67-5](#).

Configuring a CTI Route Point

To add or update a CTI route point, perform the following procedure.

Procedure

Step 1 Choose **Device > CTI Route Point**.

The Find and List Route Points window displays.

Step 2 Perform one of the followings tasks:

- To copy an CTI route point, locate the appropriate route point as described in [“Finding CTI Route Points” section on page 67-1](#). From the Search Results list, click the **Copy** icon that corresponds to the CTI route point that you want to copy, and continue with [Step 3](#).
- To add a new CTI route point, click the **Add New** button. The CTI Route Point Configuration window displays. Continue with [Step 3](#).
- To update a CTI route point, locate the appropriate CTI route point as described in [“Finding CTI Route Points” section on page 67-1](#), and continue with [Step 3](#).

Step 3 Enter the appropriate settings, as defined in [Table 67-1](#).

Step 4 Click **Save**.

For instructions on how to add and configure directory numbers, see the [“Configuring a Directory Number” section on page 49-2](#).

After you add a CTI route point to Cisco Unified CallManager Administration, information from the RIS Data Collector service displays in the CTI Route Point Configuration window. When available, the IP address of the device and the name of the Cisco Unified CallManager with which the device registered display.

Additional Information

See the [“Related Topics” section on page 67-5](#).

CTI Route Point Configuration Settings

Table 67-1 describes the CTI route point configuration settings. For more information about related procedures, see the “[Related Topics](#)” section on page 67-5.

Table 67-1 CTI Route Point Configuration Settings

Field	Description
Device Name	Enter unique identifier for this device, from 1 to 15 characters, including alphanumeric, dot, dash, or underscores.
Description	Enter a descriptive name for the CTI route point.
Device Pool	Choose the name of a Device Pool. The device pool specifies the collection of properties for this device including CallManager Group, Date/Time Group, Region, and Calling Search Space for auto-registration.
Calling Search Space	From the drop-down list box, choose a calling search space. The calling search space specifies the collection of partitions that are searched to determine how a collected (originating) number should be routed. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the Max List Box Items enterprise parameter specifies, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Calling Search Space window. Enter a partial calling search space name in the List items where Name contains field. Click the desired calling search space name in the list of calling search spaces that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.
Location	Choose the appropriate location for this route point. The location specifies the total bandwidth that is available for calls to and from this location. A location setting of <i>None</i> means that the locations feature does not keep track of the bandwidth that this route point consumes.
Media Resource Group List	Choose the appropriate Media Resource Group List. A Media Resource Group List comprises a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from the available media resources according to the priority order that is defined in a Media Resource Group List. If you choose <none>, Cisco Unified CallManager uses the Media Resource Group that is defined in the device pool. For more information, see the “Media Resource Management” section in the <i>Cisco Unified CallManager System Guide</i>.

Table 67-1 CTI Route Point Configuration Settings (continued)

Field	Description
Network Hold Audio Source	To specify the audio source that plays when the network initiates a hold action, click the drop-down arrow and choose an audio source from the list that displays. If you do not choose an audio source, Cisco Unified CallManager uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID. You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose Media Resources > Music On Hold Audio Source.
User Hold Audio Source	To specify the audio source that plays when an application initiates a hold action, click the drop-down arrow and choose an audio source from the list that displays. If you do not choose an audio source, Cisco Unified CallManager uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID. You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose Media Resources > Music On Hold Audio Source.

Deleting a CTI Route Point

To delete a CTI route point, perform the following procedure.

Before You Begin

Because you can delete a CTI route point that is assigned to one or more directory numbers, you should determine which directory numbers are using the CTI route point. To determine which directory numbers are using the CTI route point choose **Dependency Records** link from the Related Links drop-down list box in the CTI Route Point Configuration windowing and click **Go**. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#). If you try to delete a CTI route point that is in use, Cisco Unified CallManager displays a message.

If you delete a CTI Route Point that has a directory number assigned to it, you can find the directory number by using the Route Plan Report. You can also delete the directory number by using the Route Plan Report.

Procedure

Step 1 Choose **Device > CTI Route Point**.

The Find/List CTI Route Points window displays.

Step 2 Specify the search criteria that are needed to locate the CTI route point that you want to delete.

Step 3 Click **Find**.

The window refreshes to display a list of the CTI route points that match the specified search criteria.

- Step 4** Perform one of the following actions:
- Check the check boxes next to the CTI route points that you want to delete and click **Delete Selected**.
 - Delete all the CTI route points in the window by clicking **Select All** and click **Delete Selected**.
 - Choose the name of the CTI route point that you want to delete from the list to display its current settings and click **Delete**.
- Step 5** To permanently delete the CTI route point, click **OK**.
-

Additional Information

See the [“Related Topics” section on page 67-5](#).

Resetting a CTI Route Point

To reset a CTI route point, perform the following procedure.

Procedure

-
- Step 1** Choose **Device > CTI Route Point**.
- The Find and List CTI Route Points window displays.
- Step 2** Choose the search criteria to use.
- Step 3** Click **Find**.
- The window displays a list of CTI route points that match the search criteria.
- Step 4** Check the check boxes next to the CTI route points that you want to reset. To choose all CTI route points in the window, check the check box in the matching records title bar.
- Step 5** Click **Reset Selected**.
- The Reset Device dialog displays.
- Step 6** Click one of the following buttons:
- **Restart**—Restarts a device without shutting it down.
 - **Reset**—Shuts down a device and brings it back up.
 - **Close**—Closes the Reset Device dialog without performing any action.
-

Additional Information

See the [“Related Topics” section on page 67-5](#).

Related Topics

- [Configuring a CTI Route Point, page 67-2](#)
- [Finding CTI Route Points, page 67-1](#)

- [CTI Route Point Configuration Settings](#), page 67-3
- [Deleting a CTI Route Point](#), page 67-4
- [Resetting a CTI Route Point](#), page 67-5
- [Computer Telephony Integration](#), *Cisco Unified CallManager System Guide*



Gatekeeper Configuration

A gatekeeper device, also known as a Cisco Multimedia Conference Manager (MCM), supports the H.225 Registration, Admission, and Status Protocol (RAS) message set that is used for call admission control, bandwidth allocation, and dial pattern resolution (call routing). The gatekeeper provides these services for communications between Cisco Unified CallManager clusters and H.323 networks. You can configure multiple gatekeeper devices per Cisco Unified CallManager cluster. You can configure alternate gatekeepers for redundancy. Refer to MCM documentation for alternate gatekeeper configuration details.

Gatekeeper configuration comprises two components:

- Cisco Unified CallManager configuration. Each Cisco Unified CallManager cluster can register with one or more gatekeepers. This chapter describes how to configure the gatekeeper in Cisco Unified CallManager. You also need to configure trunk devices on the Trunk Configuration window. See the [“Trunk Configuration” section on page 71-1](#).
- Gatekeeper configuration on the router. This type of configuration applies to a Cisco IOS Multimedia Conference Manager (MCM) that acts as the gatekeeper. Recommended platforms for the gatekeeper include Cisco 2600, 3600, or 7200 routers with Cisco IOS Release 12.1(3)T or higher. Refer to the MCM documentation for information on configuring the gatekeeper. Alternate gatekeeper configuration occurs in the MCM only, so no configuration is necessary in Cisco Unified CallManager.

The following topics cover gatekeeper configuration in Cisco Unified CallManager Administration:

- [Finding a Gatekeeper, page 68-1](#)
- [Configuring a Gatekeeper, page 68-3](#)
- [Gatekeeper Configuration Settings, page 68-3](#)
- [Deleting a Gatekeeper, page 68-4](#)
- [Resetting a Gatekeeper, page 68-5](#)

Finding a Gatekeeper

Because you might have several gatekeepers in your network, Cisco Unified CallManager Administration lets you locate specific gatekeepers on the basis of specific criteria. Use the following procedure to locate gatekeepers.

**Note**

During your work in a browser session, Cisco Unified CallManager Administration retains your gatekeeper search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your gatekeeper search preferences until you modify your search or close the browser.

Procedure**Step 1** Choose **Device > Gatekeeper**.

The Find and List Gatekeeper window displays. Use the two drop-down list boxes to search for a gatekeeper.

Step 2 From the first Find gatekeepers where drop-down list box, choose one of the following criteria:

- Name
- Description

**Note**

The criterion that you choose in this drop-down list box specifies how the list of gatekeepers that your search generates will be sorted. For example, if you choose Description, the Description column will display as the left column of the results list.

From the second Find gatekeepers where drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is not empty
- is empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.**Tip**

To find all gatekeepers that are registered in the database, click **Find** without entering any search text.

A list of discovered gatekeepers displays by

- Gatekeeper name
- Description

**Note**

You can delete multiple gatekeepers from the Find and List Gatekeeper window by checking the check boxes next to the appropriate gatekeepers and clicking **Delete Selected**.

- Step 4** Click the Gatekeeper icon or name or the Description from the list of records that matches your search criteria.

The window displays the gatekeeper that you choose.

Additional Information

See the [“Related Topics” section on page 68-6](#).

Configuring a Gatekeeper

Perform the following procedure to add or update a gatekeeper.



Note

You can configure multiple gatekeeper devices per Cisco Unified CallManager cluster.

Procedure

- Step 1** Choose **Device > Gatekeeper**.

The Find and List Gatekeepers window displays.

- Step 2** Perform one of the followings tasks:

- To add a new gatekeeper, click the **Add New** button and continue with [Step 3](#).
- To update an existing gatekeeper, locate the appropriate gatekeeper as described in [“Finding a Gatekeeper” section on page 68-1](#) and continue with [Step 3](#).

- Step 3** Enter the appropriate settings as described in [Table 68-1](#).

- Step 4** Click **Save**.

Additional Information

See the [“Related Topics” section on page 68-6](#).

Gatekeeper Configuration Settings

[Table 68-1](#) describes the gatekeeper configuration settings. For related procedures, see the [“Related Topics” section on page 68-6](#).

Table 68-1 Gatekeeper Configuration Settings

Field	Description
Gatekeeper Information	
Host Name/IP Address	Enter the IP address or host name of the gatekeeper in this required field. You can register multiple gatekeepers per Cisco Unified CallManager cluster.

Table 68-1 Gatekeeper Configuration Settings (continued)

Field	Description
Description	Enter a descriptive name for the gatekeeper.
Registration Request Time to Live	Do not change this value unless a Cisco TAC engineer instructs you to do so. Enter the time in seconds. The default value specifies 60 seconds. The Registration Request Time to Live field indicates the time that the gatekeeper considers a registration request (RRQ) valid. The system must send a keepalive RRQ to the gatekeeper before the RRQ Time to Live expires. Cisco Unified CallManager sends an RRQ to the gatekeeper to register and subsequently to maintain a connection with the gatekeeper. The gatekeeper may confirm (RCF) or deny (RRJ) the request.
Registration Retry Timeout	Do not change this value unless a Cisco TAC engineer instructs you to do so. Enter the time in seconds. The default value specifies 300 seconds. The Registration Retry Timeout field indicates the time that Cisco Unified CallManager waits before retrying gatekeeper registration after a failed registration attempt.
Enable Device	This check box allows you to register this gatekeeper with Cisco Unified CallManager. By default, this check box remains checked. To unregister the gatekeeper from Cisco Unified CallManager gracefully, uncheck this check box. The gatekeeper unregisters within approximately 1 minute of updating this field.

Deleting a Gatekeeper

Perform the following steps to delete a gatekeeper.

Before You Begin

You cannot delete a gatekeeper that is assigned to one or more trunks. To find out which trunks are using the gatekeeper, click the **Dependency Records** link from the Gatekeeper Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#). If you try to delete a gatekeeper that is in use, Cisco Unified CallManager displays an error message. Before deleting a gatekeeper that is currently in use, you must perform either or both of the following tasks:

- Assign a different gatekeeper to any trunks that are using the gatekeeper that you want to delete. See the [“Configuring a Trunk” section on page 71-2](#).
- Delete the trunks that are using the gatekeeper that you want to delete. See the [“Deleting a Trunk” section on page 71-27](#).

Procedure

-
- Step 1** Locate the gatekeeper by using the procedure in the [“Finding a Gatekeeper” section on page 68-1](#).
- Step 2** From the list of matching records, choose the gatekeeper that you want to delete.
- Step 3** Click **Delete Selected**.
A confirmation dialog box displays.
- Step 4** To delete the gatekeeper, click **OK**.
-

Additional Information

See the [“Related Topics” section on page 68-6](#).

Resetting a Gatekeeper

Resetting a gatekeeper does not mean that the physical device is reset; instead, resetting forces the Cisco Unified CallManager to reset the logical connection to the gatekeeper and to reregister with the gatekeeper. During this time of reregistering and until successful registration, new calls that are made by using this trunk, which uses this gatekeeper, fail. Perform the following procedure to reset a gatekeeper.



Note

Resetting a gatekeeper does not cause all active calls that this gatekeeper controls to be dropped; however, new call attempts fail.

Procedure

-
- Step 1** Locate the gatekeeper by using the procedure in the [“Finding a Gatekeeper” section on page 68-1](#).
- Step 2** From the list of matching records, choose the gatekeeper that you want to reset.
- Step 3** If you changed any settings for the Gatekeeper Device, click **Reset**.
The Reset Device dialog displays.
- Step 4** Click one of the following choices:
- **Restart**—Restarts the chosen devices without shutting them down (reregisters the phones and trunks with Cisco Unified CallManager).
 - **Reset**—Shuts down, then restarts, the internal gatekeeper device. The Cisco Unified CallManager cluster unregisters (URQ) and then reregisters (RRQ) with the gatekeeper.
 - **Close**—Closes the Reset Device dialog without performing any action.
-

Additional Information

See the [“Related Topics” section on page 68-6](#).

Related Topics

- [Gatekeeper Configuration](#), page 68-1
- [Finding a Gatekeeper](#), page 68-1
- [Configuring a Gatekeeper](#), page 68-3
- [Gatekeeper Configuration Settings](#), page 68-3
- [Deleting a Gatekeeper](#), page 68-4
- [Resetting a Gatekeeper](#), page 68-5
- [Trunk Configuration](#), page 71-1
- [Gatekeepers and Trunks](#), *Cisco Unified CallManager System Guide*

Additional Cisco Documentation

- *Cisco Unified Communications Solution Reference Network Design*
- Cisco IOS Multimedia Conference Manager (Command Reference) documentation



Gateway Configuration

Cisco Unified Communications gateways enable Cisco Unified CallManager to communicate with non-IP telecommunications devices. Cisco Unified CallManager supports several gateway types as described in the *Cisco Unified CallManager System Guide*.

These sections provide information about using Cisco Unified CallManager for working with and configuring Cisco gateways.

- [Adding Gateways to Cisco Unified CallManager, page 69-1](#)
- [Gateway Configuration Settings, page 69-13](#)
- [Port Configuration Settings, page 69-59](#)
- [Finding Specific Gateways, page 69-66](#)
- [Modifying Gateways and Ports, page 69-74](#)
- [Understanding Cisco Unified CallManager Voice Gateways, Cisco Unified CallManager System Guide](#)

Adding Gateways to Cisco Unified CallManager

To enable Cisco Unified CallManager to manage IP telephony gateways in your network, you must first add each gateway to the Cisco Unified CallManager configuration database. The procedures, windows, and configuration settings for adding a gateway vary according to the gateway model that you are adding.

The following procedure describes how to add a new gateway in Cisco Unified CallManager.

Procedure

- Step 1** To display the Find and List Gateways window, choose **Device > Gateway**.
- Step 2** Click the **Add New** button. The Add a New Gateway window displays.
- Step 3** From the Gateway Type drop-down list box, choose the gateway type that you want to add. The Device Protocol field may automatically get populated depending on gateway type that you choose.
- Step 4** Click **Next**.

Step 5 In the following table, click the specific procedure for the gateway type that you are configuring. After you are in the correct procedure, start with the step where you enter the appropriate settings for that particular gateway type.

Table 69-1 Gateways

Type of Gateway	Procedure to Add
Cisco Voice Gateway 200 (VG200) VG224 Gateway Cisco IOS 269X, 26XX, 362X, 364X, 366X, 3725, 3745 Gateways Cisco 2801, 2811, 2821, 2851, 3825, 3845 Gateways Cisco Catalyst 4000 Access Gateway Module Cisco Catalyst 4224 Voice Gateway Switch Communication Media Module Cisco IAD2400	Adding a Cisco IOS MGCP Gateway, page 69-2
Cisco IOS 269X, 3725, 3745 Gateways	Adding a Cisco IOS SCCP Gateway, page 69-8
Cisco Catalyst 6000 E1 VoIP Gateway Cisco Catalyst 6000 T1 VoIP Gateway Cisco DT-24+ or DE-30+ Digital Access Trunk Gateway	Adding a Non-IOS MGCP Gateway, page 69-9
Other Cisco IOS Gateway that is configured in H.323 mode	Adding a Cisco IOS H.323 Gateway, page 69-10
Cisco Catalyst 6000 24 Port FXS Gateway	Adding an Analog Access Gateway and Ports, page 69-11
Cisco VG248 Gateway	Adding a Cisco VG248 Analog Phone Gateway, page 69-12

Adding a Cisco IOS MGCP Gateway

Use the following procedure to add and configure a Cisco IOS MGCP gateway to Cisco Unified CallManager. The following Cisco IOS gateways support MGCP:

- CiscoVG200 Voice Gateway
- VG224 Gateway
- Cisco IOS 362x, 364x, 366x Gateways
- Cisco IOS 3725 and 3745 Gateways
- Cisco IOS 26xx and 269x Gateways
- Cisco 2801, 2811, 2821, 2851, 3825, 3845 Gateways
- Cisco Catalyst 4000 Access Gateway Module

- Cisco Catalyst 4224 Voice Gateway Switch
- Communication Media Module
- Cisco IAD2400 gateways

**Note**

Like other IOS MGCP gateways, MRP/ASI gateways may work with a Cisco Unified CallManager group that contains three Cisco Unified CallManagers. ASI/MRP gateways testing occurs, however, with only one backup Cisco Unified CallManager.

Before You Begin

Before configuring a Cisco IOS MGCP gateway for use with Cisco Unified CallManager, you must configure the gateway by using the Cisco IOS command-line interface (CLI). For procedures and commands that are required to perform this configuration, refer to the configuration documentation that is supplied with the gateway.

Procedure

-
- Step 1** To display the Find and List Gateways window, choose **Device > Gateway**.
- Step 2** Click the **Add New** button. The Add a New Gateway window displays.
- Step 3** From the Gateway Type drop-down list box, choose one of the following MGCP gateways:
- Cisco VG200
 - VG224
 - Cisco 362X, 364X, 366X gateways
 - Cisco 3725 and 3745 gateways
 - Cisco 26XX and 269X gateways
 - Cisco 2801, 2811, 2821, 2851, 3825, 3845 Gateways
 - Cisco Catalyst 4000 Access Gateway Module
 - Cisco Catalyst 4224 Voice Gateway Switch
 - Communication Media Module
 - Cisco IAD2400 gateway

**Note**

The Cisco Catalyst 6000 gateways also support MGCP but are configured differently. See the [“Adding a Non-IOS MGCP Gateway”](#) section on page 69-9.

Cisco IOS MGCP gateways support different device protocols for interfacing to the PSTN or other non-IP devices, depending on the gateway model and the type of installed network modules and voice interface cards (VICs). A subsequent web window provides configuration for these interfaces.

- Step 4** Click **Next**.
- Step 5** If a Protocol drop-down list box displays, choose **MGCP** and click **Next**. Otherwise, skip to [Step 6](#).
- Step 6** The appropriate Gateway Configuration window displays.

Enter the appropriate settings and choose the type of network modules that are installed in each slot, as described in the [“MGCP Gateway Configuration Settings”](#) section on page 69-14, including any product-specific configuration settings.

Step 7 Click **Save**.

The Gateway Configuration window updates and displays drop-down list boxes with options for configuring the type of voice interface cards (VICs) in each subunit of each network module.

The available choices depend on the type of network modules that are configured in the Gateway Configuration window.

Step 8 From the drop-down list boxes, choose the type of VICs that are installed in each subunit and click **Save**.

The window updates to add links for configuring endpoint information and ports for the chosen type of VICs.

Step 9 Click an endpoint identifier (for example, 1/0/0) to configure device protocol information and add ports for the installed types of VICs.

For detailed instructions, see the following procedures:

- [Adding FXS Ports to an MGCP Gateway, page 69-4](#)
- [Adding FXO Ports to an MGCP Gateway, page 69-5](#)
- [Adding Digital Access T1 Ports to an MGCP Gateway, page 69-7](#)
- [Adding a Digital Access PRI Device to an MGCP Gateway, page 69-7](#)
- [Adding a BRI Port to an MGCP Gateway, page 69-8](#)

Step 10 To reset the gateway and apply the changes, click **Reset**.**Step 11** Continue configuring endpoint information and ports as needed.**Step 12** After you finish configuring the endpoint and adding ports, you need to add the MGCP gateway device to a route group/route list or assign a route pattern to the gateway, so calls can be routed to the gateway.

Note You need to add the MGCP gateway to a route pattern only for outbound calling.

Adding Ports to an MGCP Gateway

The device protocols and port types that can be configured on MGCP gateways vary by the type of installed voice interface cards. This section contains the following procedures:

- [Adding FXS Ports to an MGCP Gateway, page 69-4](#)
- [Adding FXO Ports to an MGCP Gateway, page 69-5](#)
- [Adding Digital Access T1 Ports to an MGCP Gateway, page 69-7](#)
- [Adding a Digital Access PRI Device to an MGCP Gateway, page 69-7](#)
- [Adding a BRI Port to an MGCP Gateway, page 69-8](#)

Adding FXS Ports to an MGCP Gateway

You can use Foreign Exchange Station (FXS) ports to connect to any POTS device. Use this procedure to configure FXS ports on an MGCP gateway.

Before You Begin

You must add an MGCP gateway before configuring ports. See the [“Adding a Cisco IOS MGCP Gateway”](#) section on page 69-2 for instructions.

Procedure

-
- Step 1** To display the Find and List Gateways window, choose **Device > Gateway** or skip to [Step 4](#) if you have already located the MGCP gateway to which you want to add FXS ports.
- Step 2** Enter the appropriate search criteria to locate the MGCP gateway to which you want to add FXS ports.
- Step 3** Click the name of the desired gateway to display its MGCP configuration settings and endpoint identifiers.
- Step 4** From the Gateway Configuration window, click the endpoint identifier for the FXS VIC that you want to configure.
- The window refreshes and displays the Gateway Configuration window.
- Step 5** Enter the appropriate **Gateway Information** and **Port Information** settings. See the following sections for details about these fields:
- [FXS/FXO Port Configuration Settings, page 69-16-](#)
 - [POTS Port Configuration Settings, page 69-60](#)
- Step 6** Click **Save**.
-
-  **Note** After you insert a POTS port, the window refreshes and displays the POTS port information at the bottom of the window. An **Add a new DN** link displays below the new port.
-
- Step 7** Click **Add a new DN** to add directory numbers to the POTS port or, if you configured another type of port, go to [Step 9](#).
-
-  **Note** See the [“Configuring a Directory Number”](#) section on page 49-2 and [“Directory Number Configuration Settings”](#) section on page 49-6 for information about adding and configuring DNs.
-
- Step 8** To return to the main MGCP gateway configuration window for the gateway to which you just added the ports, choose **Back to MGCP Configuration** in the Related Links drop-down list box and click **Go**.
- Step 9** To reset the gateway and apply the changes, click **Reset**.
- Step 10** Repeat [Step 4](#) through [Step 8](#) to add additional FXS ports.
-

Additional Information

See the [“Related Topics”](#) section on page 69-76.

Adding FXO Ports to an MGCP Gateway

You can use Foreign Exchange Office (FXO) ports for connecting to a central office or PBX. Use this procedure to add and configure FXO ports for loop start or ground start on an MGCP gateway.

**Note**

Cisco Unified CallManager assumes all loop-start trunks lack positive disconnect supervision. Configure trunks with positive disconnect supervision as ground start, so active calls can be maintained during a Cisco Unified CallManager server failover.

Before You Begin

You must add an MGCP gateway before configuring ports. See the [“Adding a Cisco IOS MGCP Gateway”](#) section on page 69-2 for instructions.

Procedure

-
- Step 1** To display the Find and List Gateways window, choose **Device > Gateway** or skip to [Step 4](#) if you have already located the MGCP gateway to which you want to add FXO ports.
- Step 2** Enter the appropriate search criteria to locate the MGCP gateway to which you want to add FXO ports and click **Find**. The search results window displays.
- Step 3** Click the name of the desired gateway to display its MGCP configuration settings and endpoint identifiers.
- Step 4** From the MGCP Configuration window, click the endpoint identifiers of the FXO port that you want to configure.
- Step 5** From the Port Type drop-down list box, choose either **Ground Start** or **Loop Start**.

**Note**

You must choose the same port type for both endpoint identifiers of the VIC-2FXO port. If you choose different port types, a message displays.

-
- Step 6** Enter the appropriate **Gateway Configuration** and **Port Information** settings as described in the following sections:
- [FXS/FXO Port Configuration Settings, page 69-16](#)
 - [Loop-Start Port Configuration Settings, page 69-62](#)
 - [Ground-Start Port Configuration Settings, page 69-63](#)
- Step 7** Click **Save**.
- Step 8** To return to the main MGCP gateway configuration window for the gateway to which you just added the ports, choose **Back to MGCP Configuration** in the Related Links drop-down list box and click **Go**.
- Step 9** To reset the gateway and apply the changes, click **Reset**.
- Step 10** To add more FXO ports, repeat [Step 4](#) through [Step 7](#).
-

Additional Information

See the [“Related Topics”](#) section on page 69-76.

Adding Digital Access T1 Ports to an MGCP Gateway

Use this procedure to add Digital Access T1 (T1-CAS) ports to an MGCP gateway.

-
- Step 1** To display the Find and List Gateways window, choose **Device > Gateway** or skip to [Step 4](#) if you have already located the MGCP gateway to which you want to add T1-CAS ports.
- Step 2** To locate the MGCP gateway to which you want to add a Digital Access T1 (T1-CAS) port, enter the appropriate search criteria.
- Step 3** To display its MGCP configuration settings and endpoint identifiers, click the name of the desired gateway.
- Step 4** From the Gateway Configuration window, click the endpoint identifier of the Digital Access T1 (T1-CAS) port that you want to configure.
- In the Device Protocol drop-down list box that displays, choose **Digital Access T1** and click **Next**.
- See the [“Port Configuration Settings” section on page 69-59](#) for the appropriate settings for the port type that you choose.
- Step 5** Enter the appropriate Gateway Configuration settings. See the [“Digital Access T1 Configuration Settings” section on page 69-40](#) for details.
- Step 6** Click **Save**.
- Step 7** To reset the gateway and apply the changes, click **Reset**.
-

Additional Information

See the [“Related Topics” section on page 69-76](#).

Adding a Digital Access PRI Device to an MGCP Gateway

-
- Step 1** To display the Find and List Gateways window, choose **Device > Gateway** or skip to [Step 4](#) if you have already located the MGCP gateway to which you want to add a port.
- Step 2** To locate the MGCP gateway to which you want to add a T1 PRI or E1 PRI port, enter the appropriate search criteria.
- Step 3** To display the configuration information for the selected gateway, click the name of the desired gateway in the list.
- Step 4** From the Gateway Configuration window, click the endpoint identifier of the T1 PRI or E1 PRI port that you want to configure.
- Step 5** Configure the T1 PRI or E1 PRI device protocol settings. See the [“Digital Access PRI Port Configuration Settings” section on page 69-20](#) for detailed field descriptions.
- Step 6** Click **Save**.
- Step 7** To reset the gateway and apply the changes, click **Reset**.
-

Additional Information

See the [“Related Topics” section on page 69-76](#).

Adding a BRI Port to an MGCP Gateway

The device protocols and port types that you can configure on MGCP gateways vary by the type of installed voice interface cards (VICs). This section contains the procedures for adding a BRI port to an MGCP gateway.

Procedure

-
Step 1	To display the Find/List Gateways window, choose Device > Gateway , or if you have already located the MGCP gateway to which you want to add a port, skip to Step 4 .
Step 2	To locate the MGCP gateway to which you want to add a BRI port, enter the appropriate search criteria.
Step 3	To display the configuration information for the chosen gateway, click the name of the desired gateway in the list.
Step 4	From the MGCP Configuration window, click the endpoint identifier of the BRI port that you want to configure.
Step 5	Configure the BRI device protocol settings. See the “ BRI Gateway Configuration Settings ” section on page 69-33 for detailed field descriptions.
Step 6	Click Save .
Step 7	To apply the changes, reset the gateway.
-

Additional Information

See the “[Related Topics](#)” section on [page 69-76](#).

Adding a Cisco IOS SCCP Gateway

Use the following procedure to add and configure a Cisco IOS SCCP gateway to Cisco Unified CallManager. The following Cisco IOS gateways support SCCP:

- Cisco IOS 269xGateways
- Cisco IOS 3725 and 3745 Gateways
- Cisco VG224 Gateway

Before You Begin

Configure a Cisco IOS SCCP gateway by adding the gateway first to Cisco Unified CallManager. Afterward, configure the gateway by using the Cisco IOS command-line interface (CLI). For procedures and commands that are required to perform this configuration, refer to the configuration documentation that is supplied with the gateway.

Procedure

-
Step 1	Choose Device > Gateway . The Find and List Gateway window displays.
Step 2	Click Add New . The Add a New Gateway window displays.

- Step 3** From the Gateway Type drop-down list box, choose one of the following SCCP gateways:
- Cisco IOS 269x Gateways
 - Cisco IOS 3725 and 3745 Gateways
- Step 4** From the Protocol drop-down list box, choose the SCCP protocol.
- Cisco IOS SCCP gateways support SCCP for interfacing to the PSTN or other non-IP devices, depending on the gateway model and the type of installed network modules and voice interface cards (VICs). A subsequent web window provides configuration for the interface.
- Step 5** Click **Next**.
- The Gateway Configuration window displays for this SCCP gateway.
- Step 6** Enter the appropriate settings and choose the type of network modules that are installed in each slot, as described in the [“Cisco IOS SCCP Gateway Configuration Settings” section on page 69-57](#), including any product-specific configuration settings.
- Step 7** Click **Save**.
- The Gateway Configuration window updates and displays drop-down list boxes with options for configuring the type of voice interface cards (VICs) in each subunit of each network module.
- The available choices depend on the type of network modules that are configured in the Gateway Configuration window.
- Step 8** From the drop-down list boxes, choose the type of VICs that are installed in each subunit and click **Save**.
- The window updates to add links for configuring endpoint information and ports for the chosen type of VICs.
- Step 9** Click an endpoint identifier (for example, 1/0/0) to configure device protocol information, add ports for the installed types of VICs and add FXS/BRI port to a SCCP gateway. See the [“Cisco Unified IP Phone Configuration” section on page 70-1](#) and the [“Phone Configuration Settings” section on page 70-6](#) for details of configuring the analog phones.
- Step 10** Reset the gateway to apply the changes.
- Step 11** Continue configuring endpoint information and ports as needed.

Adding a Non-IOS MGCP Gateway

Use the following procedure to add the following non-IOS Cisco MGCP gateways to Cisco Unified CallManager:

- Cisco DT-24+ Gateway
- Cisco DE-30+ Gateway
- Cisco Catalyst 6000 E1 VoIP Gateway
- Cisco Catalyst 6000 T1 VoIP Gateway

Procedure

-
- Step 1** To display the Find and List Gateways window, choose **Device > Gateway**.
- Step 2** Click the **Add New** button.
- The Add a New Gateway window displays.

- Step 3** From the Gateway Type drop-down list box, choose one of the following digital gateways and click **Next**:
- Cisco DT-24+ Gateway
 - Cisco DE-30+ Gateway
 - Cisco Catalyst 6000 E1 VoIP Gateway
 - Cisco Catalyst 6000 T1 VoIP Gateway
- Step 4** From the drop-down list box, choose the appropriate device protocol for the type of interfaces that you are configuring on the gateway. The available choices vary according to gateway model:
- Cisco DT-24+ Gateway or Cisco Catalyst 6000 T1 VoIP Gateway—Choose either Digital Access PRI or Digital Access T1.
 - Cisco DE-30+ Gateway or Cisco Catalyst 6000 E1 VoIP Gateway—The Digital Access PRI device protocol automatically gets chosen, and the Gateway Configuration window displays. Skip to [Step 6](#).
- Step 5** Click **Next**.
- The Gateway Configuration window displays.
- Step 6** Enter the appropriate settings, depending on whether you are configuring a Digital Access PRI interface or a Digital Access T1 interface as described in following sections:
- [Digital Access PRI Port Configuration Settings, page 69-20](#)
 - [Digital Access T1 Configuration Settings, page 69-40](#)
- Step 7** Click **Save**.
- Step 8** If you are configuring a Digital Access T1 interface on a DT-24+ or Catalyst 6000 T1 VoIP Gateway, in the Ports pane that displays on the left side of the window, click **Add a New Port** link to configure ports.
- See the [“Adding Digital Access T1 Ports to an MGCP Gateway” section on page 69-7](#).
- Step 9** To reset the gateway and apply the changes, click **Reset**.
-

Additional Information

See the [“Related Topics” section on page 69-76](#).

Adding a Cisco IOS H.323 Gateway

Follow these procedures to add a Cisco IOS H.323 gateway to Cisco Unified CallManager.

Before You Begin

Before configuring a Cisco IOS H.323 gateway for use with Cisco Unified CallManager, you must configure the gateway by using the Cisco IOS command-line interface (CLI). Compared to MGCP gateways, H.323 gateways require more configuration on the gateway because the gateway must maintain the dial plan and route pattern. For procedures and commands that are required to perform this configuration, refer to the configuration documentation that is supplied with the gateway.

Procedure

-
- Step 1** To display the Find and List Gateways window, choose **Device > Gateway**.
- Step 2** Click the **Add New** button.
The Add a New Gateway window displays.
- Step 3** From the Gateway Type drop-down list box, choose **H.323 Gateway**.
- Step 4** Click **Next**.
- Step 5** Enter the appropriate settings as described in “[H.323 Gateway Configuration Settings](#)” section on [page 69-44](#).
- Step 6** Click **Save**.
- Step 7** To reset the gateway and apply the changes, click **Reset**.
-

Additional Information

See the “[Related Topics](#)” section on [page 69-76](#).

Adding an Analog Access Gateway and Ports

Use the procedure in this section to add and configure ports for the following non-IOS Cisco analog access gateways:

- Cisco Catalyst 6000 24 Port FXS Gateway

Procedure

-
- Step 1** To display the Find and List Gateways window, choose **Device > Gateway**.
- Step 2** Click the **Add New** button.
The Add a New Gateway window displays.
- Step 3** From the Gateway type drop-down list box, choose a supported analog gateway:
- Cisco Catalyst 6000 24 Port FXS Gateway
- Step 4** Click **Next**.
The Gateway Configuration window displays.
- Step 5** Enter the appropriate settings, as described in the “[Analog Access Gateway Configuration Settings](#)” section on [page 69-53](#).
- Step 6** Click **Save**.
- Step 7** To add a port to this gateway, click the **Add a New Port** link in the Ports pane that displays on the left side of the window.
The Port Configuration window displays.
- Step 8** From the drop-down list box, choose **POTS** as the port type and click **Next**.

- Step 9** Enter the appropriate port configuration settings as described in the [“POTS Port Configuration Settings” section on page 69-60](#).
- Step 10** Click **Save**.
- If you have inserted POTS ports, the window refreshes and displays the POTS port in the list on the left side of the window. An **Add DN** link displays to the right of the new port.
- Step 11** To add a directory numbers to a POTS port, click **Add DN**.
- For information about adding and configuring directory numbers, see the [“Configuring a Directory Number” section on page 49-2](#) and the [“Directory Number Configuration Settings” section on page 49-6](#).
- Step 12** After you finish adding POTS ports and configuring directory numbers for the POTS ports, you can return to the Gateway Configuration window. In the Related Links drop-down list box, choose Configure Device and click **Go**.
- Step 13** To apply the changes, click **Reset**.
-

Additional Information

See the [“Related Topics” section on page 69-76](#).

Adding a Cisco VG248 Analog Phone Gateway

The Cisco VG248 Analog Phone Gateway, a standalone, rack-mounted, 48-FXS port product, allows on-premise analog telephones, fax machines, modems, voice-messaging systems, and speakerphones to register with one Cisco Unified CallManager cluster.

The Cisco VG248 connects to a Cisco Unified CallManager by using the Skinny Client Control Protocol to allow for enhanced features.

Cisco Unified CallManager recognizes the Cisco VG248 as a gateway device, called a “Cisco VG248 Gateway.” Additionally, Cisco Unified CallManager treats each of the 48 ports as an individual device, similar to a Cisco Unified IP Phone, called a “Cisco VGC Phone.”

Use the following procedure to add a Cisco VG248 Gateway and to add and configure ports to the gateway.

Procedure

-
- Step 1** To display the Find and List Gateways window, choose **Device > Gateway**.
- Step 2** Click the **Add New** button.
- The Add a New Gateway window displays.
- Step 3** From the Gateway type drop-down list box, choose **Cisco VG248 Gateway**.
- Step 4** Click **Next**.
- The Gateway Configuration window displays.
- Step 5** Enter the appropriate settings, as described in the [“Cisco VG248 Gateway Configuration Settings” section on page 69-56](#).
- Step 6** From the Configured Slots, VICs and Endpoints drop-down list box, choose 48_PORTS.

- Step 7** Click **Save**.
- The ports 0 through 48 display in the Configured Slots, VICs, and Endpoints area.
- Step 8** Click a port.
- The Phone Configuration window displays and lists the phone model as Cisco VGCPPhone. From the Gateway Configuration window, the MAC address automatically displays.
- Step 9** Enter the appropriate settings, as described in the [“Phone Configuration Settings” section on page 70-6](#).
- Step 10** Click **Save**.
- Step 11** To configure a directory number for the port, click the **Add a New DN** link that displays in the Association Information area on the left side of the window.
- The Directory Number Configuration window displays. For information about adding and configuring directory numbers, see the [“Configuring a Directory Number” section on page 49-2](#).
- Step 12** To configure more ports for the gateway, from the Related Link drop-down list box, choose the **Back to Gateway** link and click **Go**.
- The Gateway Configuration window displays. To configure the phone settings and directory numbers for additional ports, repeat steps 8 through 11.
- When you configure port 1, the **Create all Ports like Port 1** button displays on the Gateway Configuration window. This button allows you to configure ports 2 through 48 with the same parameters and settings as port 1, regardless of whether the ports are already configured.
- Step 13** To apply the changes, click **Reset**.
-

Additional Information

See the [“Related Topics” section on page 69-76](#).

Gateway Configuration Settings

See the following sections for tables that list detailed descriptions for all gateway configuration fields:

- [MGCP Gateway Configuration Settings, page 69-14](#)
- [FXS/FXO Port Configuration Settings, page 69-16](#)
- [Digital Access PRI Port Configuration Settings, page 69-20](#)
- [BRI Gateway Configuration Settings, page 69-33](#)
- [Digital Access T1 Configuration Settings, page 69-40](#)
- [H.323 Gateway Configuration Settings, page 69-44](#)
- [Analog Access Gateway Configuration Settings, page 69-53](#)
- [Cisco VG248 Gateway Configuration Settings, page 69-56](#)
- [Cisco IOS SCCP Gateway Configuration Settings, page 69-57](#)

For detailed information about port configuration settings, see the [“Port Configuration Settings” section on page 69-59](#).

MGCP Gateway Configuration Settings

Table 69-2 provides detailed descriptions for MGCP gateway configuration settings.

Table 69-2 **MGCP Gateway Configuration Settings**

Field	Description
Gateway Details	
Domain Name	Enter a name of up to 50 characters that identifies the Cisco MGCP gateway. Use the Domain Name Service (DNS) host name if it is configured to resolve correctly; otherwise, use the host name as defined on the Cisco MGCP gateway. If you are using the host name as it is configured on the IOS gateway, the name that you enter here must match exactly. For example, if the hostname is configured on the gateway to resolve to vg200-1 and the IP domain name is not configured, enter the hostname in this field (in this case, vg200-1). If the hostname is configured on the gateway as vg200-1 and the IP domain name is configured on the gateway as cisco.com, enter vg200-1.cisco.com in this field.
Description	Enter a description that clarifies the purpose of the device.
Cisco Unified CallManager Group	From the drop-down list box, choose a Cisco Unified CallManager redundancy group. A Cisco Unified CallManager redundancy group includes a prioritized list of up to three Cisco Unified CallManagers. The first Cisco Unified CallManager in the list serves as the primary Cisco Unified CallManager. If the primary Cisco Unified CallManager is not available or fails, the gateway attempts to connect with the next Cisco Unified CallManager in the list and so on.

Table 69-2 MGCP Gateway Configuration Settings (continued)

Field	Description
Configured Slots, VICs, and Endpoints	
Note	You must specify the beginning port number for some VICs. For example, if the VIC in Subunit 0 begins at 0 and has two ports (0 and 1), the VIC in Subunit 1 must begin at a port number greater than 1 and have two ports (2 and 3 or 4 and 5).
Note	The correct number of slots displays for each model of MGCP gateway. (The VG200 gateway has only one slot.)
Note	To begin configuring ports on a module, select the module first, then click Save .
Module in Slot 0 Module in Slot 1 Module in Slot 2 Module in Slot 3 (and so on)	For each available slot on the chosen MGCP gateway, choose the type of module that is installed; for example: • NM-1V—Has one voice interface card (VIC) in Subunit 0 for FXS or FXO. When you use the VIC-2BRI-S/T-TE card with a NM-1V module, you can make two calls because the second BRI port is shut down. • NM-2V—Has two VICs, one in Subunit 0 and one in Subunit 1 for either FXS or FXO. When you use the VIC-2BRI-S/T-TE card with a NM-2V module, you can make four calls. If another VIC is in the second slot of the NM-2V, the second port on the VIC-2BRI-S/T-TE gets shut down. • NM-HDV—Has one VIC in Subunit 0 for either T1-CAS or T1-PRI, or E1-PRI. • NM-HDA—Has three VICs, one in Subunit 0, one in Subunit 1, and one in Subunit 2. • VWIC-SLOT—Has a slot for any of the following modules: VIC (FXS, FXO, or BRI), T1-CAS, T1-PRI, or E1-PRI. • AIM-VOICE-30—Has two VICs, one in Subunit 0 and one in Subunit 1 for T1-CAS, T1-PRI, or E1-PRI. • WS-X6600-24FXS—Has 24 FXS ports. • WS-X6600-6T1—Has six ports for T1 PRI or CAS. • WS-X6600-6E1—Has six ports for E1 PRI. • WS-SVC-CMM-MS—Has two port adapters, one for a T1 interface and one for an E1 interface for Europe and other countries. • None—Has no network modules installed.

Table 69-2 *MGCP Gateway Configuration Settings (continued)*

Field	Description
Product-Specific Configuration	
Model-specific configuration fields defined by the gateway manufacturer	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the “?” information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, refer to the documentation for the specific gateway that you are configuring or contact the manufacturer.

Additional Information

See the “[Related Topics](#)” section on page 69-76.

FXS/FXO Port Configuration Settings

[Table 69-3](#) provides detailed descriptions for FXS/FXO port configuration settings.

**Note**

For the VG200 gateway, not all switch emulation types support the network side. How you configure the gateway switch type determines whether you may or may not be able to set network side.

Table 69-3 *FXS/FXO Port Configuration Settings*

Field	Description
Device Information	
Description	Cisco Unified CallManager generates a string that uniquely identifies the analog MGCP description. For example: AALN/S0/SU1/1@domain.com You can edit this field.
Device Pool	From the drop-down list box, choose the appropriate device pool. The device pool specifies a collection of properties for this device including CallManager Group, Date/Time Group, Region, and Calling Search Space for auto registration of devices.
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that is defined in a Media Resource Group List.

Table 69-3 **FXS/FXO Port Configuration Settings (continued)**

Field	Description
Packet Capture Mode (for Cisco IOS MGCP gateways only)	Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, refer to the <i>Cisco Unified CallManager Security Guide</i> .
Packet Capture Duration (for Cisco IOS MGCP gateways only)	Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, refer to the <i>Cisco Unified CallManager Security Guide</i> .
Calling Search Space	From the drop-down list box, choose the appropriate calling search space. A calling search space comprises a collection of route partitions that are searched to determine how a collected (originating) number should be routed. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the Max List Box Items enterprise parameter specifies, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Calling Search Space window. Enter a partial calling search space name in the List items where Name contains field. Click the desired calling search space name in the list of calling search spaces that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and enter a value for Max List Box Items in the CCMAAdmin Parameters pane.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.
Location	Choose the appropriate location for this device. The location specifies the total bandwidth that is available for calls to and from this location. A location setting of None means that the locations feature does not keep track of the bandwidth that this device consumes.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.

Table 69-3 *FXS/FXO Port Configuration Settings (continued)*

Field	Description
Network Locale	From the drop-down list box, choose the locale that is associated with the gateway. The network locale identifies a set of detailed information to support the hardware in a specific location. The network locale contains a definition of the tones and cadences that the device uses in a specific geographic area. Note Choose only a network locale that is already installed and that the associated devices support. The list contains all available network locales for this setting, but not all are necessarily installed. If the device is associated with a network locale that it does not support in the firmware, the device will fail to come up.
Transmit UTF-8 for Calling Party Name	This device uses the user locale setting of the device's device pool to determine whether to send Unicode and whether to translate received Unicode information. For the sending device, if you check this check box and the user locale setting in the device's device pool matches the terminating phone's user locale, the device sends Unicode. If the user locale settings do not match, the device sends ASCII. The receiving device translates incoming Unicode characters based on the user locale setting of the sending device's device pool. If the user locale setting matches the terminating phone's user locale, the phone displays the characters. Note The phone may display junk characters if the two ends of the trunk configure user locales that do not belong to the same language group.
Multilevel Precedence and Preemption (MLPP) Information	
MLPP Domain	From the drop-down list box, choose an MLPP domain to associate with this device. If you leave the value <i><None></i>, this device inherits its MLPP domain from the value set for the device's device pool. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value set for the MLPP Domain Identifier enterprise parameter.

Table 69-3 **FXS/FXO Port Configuration Settings (continued)**

Field	Description
MLPP Indication	This setting is not available on all devices. If available, this setting specifies whether a device that can play precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options: • Default—This device inherits its MLPP indication setting from its device pool. • Off—This device does not handle nor process indication of an MLPP precedence call. • On—This device does handle and process indication of an MLPP precedence call. Note Do not configure a device with the following combination of settings: MLPP Indication is set to <i>Off or Default</i> (when default is <i>Off</i>) while MLPP Preemption is set to <i>Forceful</i>.
MLPP Preemption	This setting is not available on all devices. If available, this setting specifies whether a device that can preempt calls in progress will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options: • Default—This device inherits its MLPP preemption setting from its device pool. • Disabled—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher-precedence calls. • Forceful—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. Note Do not configure a device with the following combination of settings: MLPP Indication is set to <i>Off or Default</i> (when default is <i>Off</i>) while MLPP Preemption is set to <i>Forceful</i>.
Port Information (POTS)	
Port Direction	Choose the direction of calls that are passing through this port: • Inbound—Use for incoming calls only. • Outbound—Use for outgoing calls. • Bothways—Use for inbound and outbound calls (default).
Prefix DN (for FXS ports)	Enter the prefix digits that are appended to the digits that this trunk receives on incoming calls. Cisco Unified CallManager adds prefix digits after first truncating the number in accordance with the Num Digits setting.

Table 69-3 *FXS/FXO Port Configuration Settings (continued)*

Field	Description
Num Digits (for FXS ports)	Enter the number of significant digits to collect, from 0 to 32. Cisco Unified CallManager counts significant digits from the right (last digit) of the number called. Use this field for the processing of incoming calls and to indicate the number of digits starting from the last digit of the called number that is used to route calls coming into the PRI span. See Prefix DN.
Expected Digits (for FXS ports)	Enter the number of digits that are expected on the inbound side of the trunk. For this rarely used field, leave zero as the default value if you are unsure.
SMDI Port Number (0-4096)	Use this field for analog access ports that connect to a voice-messaging system. Set the SMDI Port Number equal to the actual port number on the voice-messaging system to which the analog access port connects. Note Voice-mail logical ports typically must match physical ports for the voice-messaging system to operate correctly.
Unattended Port	Check this check box to indicate an unattended port on this device.
Product-Specific Configuration	
Model-specific configuration fields defined by the gateway manufacturer	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the “?” information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, refer to the documentation for the specific gateway that you are configuring or contact the manufacturer.

Additional Information

See the [“Related Topics”](#) section on page 69-76.

Digital Access PRI Port Configuration Settings

[Table 69-4](#) provides detailed descriptions for Digital Access PRI port configuration settings.

**Note**

To determine whether your gateway supports the QSIG protocol, refer to the gateway product documentation. For information on QSIG support with Cisco Unified CallManager, refer to the [“Q.Signaling \(QSIG\)”](#) section on page 40-6.

Table 69-4 Digital Access PRI Port Configuration Settings

Field	Description
Device Information	
Endpoint Name	For MGCP gateways, this display-only field contains a string that is generated by Cisco Unified CallManager that uniquely identifies the MGCP endpoint. For example: S1/DS1-0@VG200-2 S1 indicates slot 1, DS1-0 designates the digital interface, and @VG200-2 designates the MGCP domain name.
MAC Address	Enter MAC address of the gateway. The MAC address uniquely identifies the hardware device. You must enter a 12-hexadecimal character value.
Description	Enter a description that clarifies the purpose of the device.
Device Pool	From the drop-down list box, choose the appropriate device pool. The device pool specifies a collection of properties for this device including CallManager Group, Date/Time Group, Region, and Calling Search Space for auto-registration of devices.
Call Classification	This parameter determines whether an incoming call that is using this gateway is considered off the network (OffNet) or on the network (OnNet). When the Call Classification field is configured as Use System Default, the setting of the Cisco Unified CallManager clusterwide service parameter, Call Classification, determines whether the gateway is OnNet or OffNet. This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively.
Network Locale	From the drop-down list box, choose the locale that is associated with the gateway. The network locale identifies a set of detailed information to support the hardware in a specific location. The network locale contains a definition of the tones and cadences that are used by the device in a specific geographic area. Note Choose only a network locale that is already installed and supported by the associated devices. The list contains all available network locales for this setting, but not all are necessarily installed. If the device is associated with a network locale that it does not support in the firmware, the device will fail to come up.
Packet Capture Mode (for Cisco IOS MGCP gateways only)	Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, refer to the <i>Cisco Unified CallManager Security Guide</i>.

Table 69-4 **Digital Access PRI Port Configuration Settings (continued)**

Field	Description
Packet Capture Duration (for Cisco IOS MGCP gateways only)	Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, refer to the <i>Cisco Unified CallManager Security Guide</i> .
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, among the available media resources according to the priority order that is defined in a Media Resource List.
Location	Choose the appropriate location for this device. The location specifies the total bandwidth that is available for calls to and from this location. A location setting of None means that the locations feature does not keep track of the bandwidth that is consumed by this device.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.
Load Information	Enter the appropriate firmware load information for the gateway. The value that you enter here overrides the default firmware load for this gateway type.
Transmit UTF-8 for Calling Party Name	This device uses the user locale setting of the device's device pool to determine whether to send Unicode and whether to translate received Unicode information. For the sending device, if you check this check box and the user locale setting in the device's device pool matches the terminating phone's user locale, the device sends Unicode. If the user locale settings do not match, the device sends ASCII. The receiving device translates incoming Unicode characters based on the user locale setting of the device pool to which the sending device belongs. If the user locale setting matches the terminating phone user locale, the phone displays the characters. Note The phone may display junk characters if the two ends of the trunk configure user locales that do not belong to the same language group.
V150 (subset)	Check this box to enable v150 (subset) modem relay support on the gateways. IP-STE's currently use this feature to support end-to-end secure calls to an ISDN-STE. (Applies only to T1 PRI and T1 CAS.) The default value specifies unchecked.

Table 69-4 **Digital Access PRI Port Configuration Settings (continued)**

Field	Description
Multilevel Precedence and Preemption (MLPP) Information	
MLPP Domain	From the drop-down list box, choose an MLPP domain to associate with this device. If you leave the value <None>, this device inherits its MLPP domain from the value that is set for the device's device pool. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value that is set for the MLPP Domain Identifier enterprise parameter.
MLPP Indication	This setting is not available on all devices. If available, this setting specifies whether a device that can play precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options: • Default—This device inherits its MLPP indication setting from its device pool. • Off—This device does not handle nor process indication of an MLPP precedence call. • On—This device does handle and process indication of an MLPP precedence call. Note Do not configure a device with the following combination of settings: MLPP Indication is set to <i>Off</i> or <i>Default</i> (when default is <i>Off</i>) while MLPP Preemption is set to <i>Forceful</i>.
MLPP Preemption	This setting is not available on all devices. If available, this setting specifies whether a device that can preempt calls in progress will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options: • Default—This device inherits its MLPP preemption setting from its device pool. • Disabled—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. • Forceful—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. Note Do not configure a device with the following combination of settings: MLPP Indication is set to <i>Off</i> or <i>Default</i> (when default is <i>Off</i>) while MLPP Preemption is set to <i>Forceful</i>.

Table 69-4 *Digital Access PRI Port Configuration Settings (continued)*

Field	Description
Interface Information	
PRI Protocol Type	Choose the communications protocol for the span. T1 PRI spans provide several options, depending on the carrier or switch; for example: • PRI 4ESS—AT&T Interexchange carrier • PRI 5E8 Custom—Cisco Unified IP Phone • PRI 5E9—AT&T family local exchange switch or carrier • PRI DMS—MCI family local exchange switch or carrier; Canadian local exchange carrier • PRI ETSI SC—European local exchange carrier on T1; also, Japanese, Taiwan, Korean, and Hong Kong local exchange. • PRI NI2—AT&T family local exchange switch or carrier • PRI NTT—Japanese NTT exchange switch • PRI ISO QSIG T1—PBX T1 tie trunk using ISO QSIG • PRI ISO QSIG E1—PBX E1 tie trunk using ISO QSIG Determine the switch to which you are connecting and the preferred protocol; for example: • Nortel Meridian—DMS, 5E8 Custom • Lucent Definity—4ESS or 5E8 • Madge (Teleos) box—5E8 Teleos • Intecom PBX—5E8 Intecom
Protocol Side	Choose the appropriate protocol side. This setting specifies whether the gateway connects to a Central Office/Network device or to a User device. Make sure that the two ends of the PRI connection use opposite settings. For example, if you connect to a PBX and the PBX uses User as its protocol side, choose Network for this device. Typically, use User for this option for central office connections.
Channel Selection Order	Choose the order in which channels or ports are enabled from first (lowest number port) to last (highest number port), or from last to first. Valid entries include TOP_DOWN (first to last) or BOTTOM_UP (last to first). If you are not sure which port order to use, choose TOP_DOWN.

Table 69-4 Digital Access PRI Port Configuration Settings (continued)

Field	Description
Channel IE Type	Choose one of the following values to specify whether channel selection is presented as a channel map or a slot map: • Timeslot Number—B-channel usage always indicates actual timeslot map format (such as 1-15 and 17-31 for E1). • Slotmap—B-channel usage always indicates a slot map format. • Use Number When 1B—Channel usage indicates a channel map for one B-channel but indicates a slot map if more than one B-channel exists. • Continuous Number—Configures a continuous range of slot numbers (1-30) as the E1 logical channel number instead of the noncontinuous actual timeslot number (1-15 and 17-31).
PCM Type	Specify the digital encoding format. Choose one of the following formats: • a-law: Use for Europe and the rest of the world. • mu-law: Use for North America, Hong Kong, Taiwan, and Japan.
Delay for first restart (1/8 sec ticks)	Enter the rate at which the spans are brought in service. The delay occurs when many PRI spans are enabled on a system and the Inhibit Restarts at PRI Initialization check box is unchecked. For example, set the first five cards to 0 and set the next five cards to 16. (Wait 2 seconds before bringing them in service.)
Delay between restarts (1/8 sec ticks)	Enter the time between restarts. The delay occurs when a PRI RESTART gets sent if the Inhibit Restarts check box is unchecked.
Inhibit restarts at PRI initialization	A RESTART or SERVICE message confirms the status of the ports on a PRI span. If RESTART or SERVICE messages are not sent, Cisco Unified CallManager assumes the ports are in service. When the D-Channel successfully connects with another PRI D-Channel, it sends a RESTART or SERVICE message when this check box is unchecked.
Enable status poll	Check the check box to enable the Cisco Unified CallManager advanced service parameter, Change B-Channel Maintenance Status. This service parameter allows you to take individual B-channels out of service for an MGCP T1/E1 PRI gateway in real time. Uncheck this check box to disable the service parameter "Change B-Channel Maintenance Status." Note Default leaves this field unchecked.
Unattended Port	Check this check box to indicate an unattended port on this device.

Table 69-4 Digital Access PRI Port Configuration Settings (continued)

Field	Description
Call Routing Information - Inbound Calls	
Significant Digits	Choose the number of significant digits to collect, from 0 to 32 or All. Cisco Unified CallManager counts significant digits from the right (last digit) of the number that is called. If you choose <i>All</i>, the Cisco Unified CallManager does not truncate the inbound number. EXAMPLE Digits received are 123456. Significant digits setting is 4. Digits translated are 3456. Use for the processing of incoming calls and to indicate the number of digits, starting from the last digit of the called number, that are used to route calls that are coming into the PRI span. See Prefix DN.
Calling Search Space	From the drop-down list box, choose the appropriate calling search space. A calling search space designates a collection of route partitions that are searched to determine how a collected (originating) number should be routed. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the Max List Box Items enterprise parameter specifies, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Calling Search Space window. Enter a partial calling search space name in the List items where Name contains field. Click the desired calling search space name in the list of calling search spaces that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when automated alternate routing (AAR) is performed. The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.
Prefix DN	Enter the prefix digits that are appended to the digits that this trunk receives on incoming calls. The Cisco Unified CallManager adds prefix digits after first truncating the number in accordance with the Num Digits setting.

Table 69-4 Digital Access PRI Port Configuration Settings (continued)

Field	Description
Call Routing Information - Outbound Calls	
Calling Party Presentation	Choose whether you want the Cisco Unified CallManager to allow or restrict the display of the calling party phone number. Choose <i>Default</i> if you do not want to change calling line ID presentation. Choose <i>Allowed</i> if you want Cisco Unified CallManager to send “Calling Line ID Allowed” on outbound calls. Choose <i>Restricted</i> if you want Cisco Unified CallManager to send “Calling Line ID Restricted” on outbound calls. For more information about this field, see Table 17-6 in the “Calling Party Number Transformations Settings” section in the <i>Cisco Unified CallManager System Guide</i>.
Calling Party Selection	Any outbound call on a gateway can send directory number information. Choose which directory number is sent: • Originator—Send the directory number of the calling device. • First Redirect Number—Send the directory number of the redirecting device. • Last Redirect Number—Send the directory number of the last device to redirect the call. • First Redirect Number (External)—Send the directory number of the first redirecting device with the external phone mask applied. • Last Redirect Number (External)—Send the directory number of the last redirecting device with the external phone mask applied.

Table 69-4 **Digital Access PRI Port Configuration Settings (continued)**

Field	Description
Called party IE number type unknown	Choose the format for the number type in called party directory numbers. Cisco Unified CallManager sets the called directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified CallManager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the called directory number to be encoded to a non-national type numbering plan. Choose one of the following options: • Cisco Unified CallManager—Use when the Cisco Unified CallManager sets the directory number type. • Unknown—Use when the dialing plan is unknown. • National—Use when you are dialing within the dialing plan for your country. • International—Use when you are dialing outside the dialing plan for your country. • Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number.
Calling party IE number type unknown	Choose the format for the number type in calling party directory numbers. Cisco Unified CallManager sets the calling directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified CallManager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the calling directory number to be encoded to a non-national type numbering plan. Choose one of the following options: • Cisco Unified CallManager—Use when the Cisco Unified CallManager sets the directory number type. • Unknown—Use when the dialing plan is unknown. • National—Use when you are dialing within the dialing plan for your country. • International—Use when you are dialing outside the dialing plan for your country. • Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number.

Table 69-4 **Digital Access PRI Port Configuration Settings (continued)**

Field	Description
Called Numbering Plan	Choose the format for the numbering plan in called party directory numbers. Cisco Unified CallManager sets the called DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified CallManager does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of the following options: • Cisco Unified CallManager—Use when the Cisco Unified CallManager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—Use when the dialing plan is unknown.
Calling Numbering Plan	Choose the format for the numbering plan in calling party directory numbers. Cisco Unified CallManager sets the calling DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified CallManager does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of the following options: • Cisco Unified CallManager—Use when the Cisco Unified CallManager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—Use when the dialing plan is unknown.

Table 69-4 *Digital Access PRI Port Configuration Settings (continued)*

Field	Description
Number of digits to strip	Choose the number of digits to strip on outbound calls, from 0 to 32. For example, when 8889725551234 is dialed, and the number of digits to strip is 3, Cisco Unified CallManager strips 888 from the outbound number.
Caller ID DN	Enter the pattern that you want to use for calling line ID, from 0 to 24 digits. For example, in North America: 555XXXX = Variable calling line ID, where X equals an extension number. The CO appends the number with the area code if you do not specify it. 5555000 = Fixed calling line ID, where you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it.
SMDI Base Port	Enter the first SMDI port number of the T1 span. If you set this parameter to a nonzero value and this gateway belongs to an unknown type of route list, route group, or route list, hunting does not continue past this span.
PRI Protocol Type Specific Information	
Display IE Delivery	Check the check box to enable delivery of the display information element (IE) in SETUP and NOTIFY messages (for DMS protocol) for the calling and connected party name delivery service.
Redirecting Number IE Delivery— Outbound	Check this check box to include the Redirecting Number IE in the outgoing SETUP message from the Cisco Unified CallManager to indicate the first redirecting number and the redirecting reason of the call when the call is forwarded. Uncheck the check box to exclude the first redirecting number and the redirecting reason from the outgoing SETUP message. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box.
Redirecting Number IE Delivery— Inbound	Check this check box to accept the Redirecting Number IE in the incoming SETUP message to the Cisco Unified CallManager. Uncheck the check box to exclude the Redirecting Number IE in the incoming SETUP message to the Cisco Unified CallManager. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box.

Table 69-4 Digital Access PRI Port Configuration Settings (continued)

Field	Description
Send Extra Leading Character in Display IE	Check this check box to include a special leading character byte (non ASCII, nondisplayable) in the DisplayIE field. Uncheck this check box to exclude this character byte from the Display IE field. This check box only applies to the DMS-100 protocol and the DMS-250 protocol. Default leaves this setting disabled (unchecked).
Setup non-ISDN Progress Indicator IE Enable	Default leaves this setting disabled (unchecked). Enable this setting only if users are not receiving ringback tones on outbound calls. When this setting is enabled, the Cisco Unified CallManager sends Q.931 Setup messages out digital (that is, non-H.323) gateways with the Progress Indicator field set to non-ISDN. This message notifies the destination device that the Cisco Unified CallManager gateway is non-ISDN and that the destination device should play in-band ringback. This problem usually associates with Cisco Unified CallManagers that connect to PBXs through digital gateways.
MCDN Channel Number Extension Bit Set to Zero	To set the channel number extension bit to zero, check the check box. To set the extension bit to 1, uncheck the check box. This setting only applies to the DMS-100 protocol
Send Calling Name in Facility IE	Check the check box to send the calling name in the Facility IE field. By default, the Cisco Unified CallManager leaves the check box unchecked. Set this feature for a private network that has a PRI interface that is enabled for ISDN calling name delivery. When this check box is checked, the calling party's name gets sent in the Facility IE of the SETUP or FACILITY message, so the name can display on the called party's device. Set this feature for PRI trunks in a private network only. Do not set this feature for PRI trunks that are connected to the PSTN. Note This field applies to the NI2 protocol only.
Interface Identifier Present	Check the check box to indicate that an interface identifier is present. By default, the Cisco Unified CallManager leaves the check box unchecked. This setting only applies to the DMS-100 protocol for digital access gateways in the Channel Identification information element (IE) of the SETUP, CALL PROCEEDING, ALERTING, and CONNECT messages.
Interface Identifier Value	Enter the value that was obtained from the PBX provider. This field applies to only the DMS-100 protocol. Valid values range from 0 through 255.

Table 69-4 Digital Access PRI Port Configuration Settings (continued)

Field	Description
Connected Line ID Presentation (QSIG Inbound Call)	Choose whether you want the Cisco Unified CallManager to allow or block the connected party's phone number from displaying on an inbound caller's phone. This field applies only to gateways that are using QSIG protocol. The gateway applies this setting for incoming calls only. Choose <i>Default</i> if you do not want to change the connected line ID presentation. Choose <i>Allowed</i> if you want Cisco Unified CallManager to send "Connected Line ID Allowed" to enable the connected party's number to display for the calling party. Choose <i>Restricted</i> if you want Cisco Unified CallManager to send "Connected Line ID Restricted" to block the connected party's number from displaying for the calling party. For more information about this field, see Table 17-9 in the "Connected Party Presentation and Restriction Settings" section in the <i>Cisco Unified CallManager System Guide</i>.
UUIE Configuration	
Passing Precedence Level Through UUIE	Check this check box to enable passing MLPP information through the PRI 4ESS UUIE field. This box is used for interworking with DRSN switch. The system makes this check box available only if the PRI Protocol Type value of PRI 4ESS is specified for this gateway. The default value specifies unchecked.
Security Access Level	Enter the value for the security access level. Valid values include 00 through 99. The system makes this field available only if the Passing Precedence Level Through UUIE check box is checked. The default value specifies 2.
Product-Specific Configuration	
Model-specific configuration fields that the gateway manufacturer defines	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the "?" information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, refer to the documentation for the specific gateway that you are configuring or contact the manufacturer.

Additional Information

See the ["Related Topics"](#) section on page 69-76.

BRI Gateway Configuration Settings

Table 69-5 provides detailed descriptions for BRI configuration settings.

Table 69-5 BRI Gateway Configuration Settings

Field	Description
Device Information	
End-Point Name (MGCP gateways)	For MGCP gateways, this display-only field contains a string that Cisco Unified CallManager generates that uniquely identifies the MGCP endpoint. For example: BRI/S1/SU0/P0@SC3640.cisco.com S1 indicates slot 1, SU0 indicates subunit 0, P0 indicates port 0, and @SC3640.cisco.com designates the MGCP domain name.
Description	Enter a description that clarifies the purpose of the device.
Device Pool	From the drop-down list box, choose the appropriate device pool. For this device, the device pool specifies a collection of properties that includes CallManager Group, Date/Time Group, Region, and Calling Search Space for auto-registration of devices.
Call Classification	This parameter determines whether an incoming call that is using this gateway is considered off the network (OffNet) or on the network (OnNet). When the Call Classification field is configured as Use System Default, the setting of the Cisco Unified CallManager clusterwide service parameter, Call Classification, determines whether the gateway is OnNet or OffNet. This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively.
Network Locale	From the drop-down list box, choose the locale that is associated with the gateway. The network locale identifies a set of detailed information to support the hardware in a specific location. The network locale contains a definition of the tones and cadences that devices use in a specific geographic area.
Packet Capture Mode (for Cisco IOS MGCP gateways only)	Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, refer to the <i>Cisco Unified CallManager Security Guide</i>.
Packet Capture Duration (for Cisco IOS MGCP gateways only)	Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, refer to the <i>Cisco Unified CallManager Security Guide</i>.

Table 69-5 BRI Gateway Configuration Settings (continued)

Field	Description
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that a Media Resource List defines.
Location	Choose the appropriate location for this device. The location specifies the total bandwidth that is available for calls to and from this location. A location setting of None means that the locations feature does not keep track of the bandwidth that this device consumes.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.
Interface Information	
BRI Protocol	Choose the communications protocol for the span. BRI-NET3
Protocol Side	Choose the appropriate protocol side. This setting specifies whether the gateway connects to a Central Office/Network device or to a User device. Note BRI supports only the User side.
Channel Selection Order	Choose the order in which channels or ports are enabled from first (lowest number port) to last (highest number port) or from last to first. Valid entries include TOP_DOWN (first to last) or BOTTOM_UP (last to first). If you are not sure which port order to use, choose TOP_DOWN.
PCM Type	Specify the digital encoding format. Choose one of the following formats: - a-law: Use for Europe and the rest of the world. - mu-law: Use for North America, Hong Kong, Taiwan, and Japan.
Delay for First Restart (1/8 sec ticks)	Enter the rate at which the spans are brought in service. The delay occurs when many BRI spans are enabled on a system and the Inhibit Restarts at BRI Initialization check box is unchecked. For example, set the first five cards to 0 and set the next five cards to 16. (Wait 2 seconds before bringing them in service.)
Delay Between Restarts (1/8 sec ticks)	Enter the time between restarts. The delay occurs when a BRI RESTART gets sent if the Inhibit Restarts check box is unchecked.

Table 69-5 BRI Gateway Configuration Settings (continued)

Field	Description
Inhibit Restarts at BRI Initialization	A RESTART message confirms the status of the ports on a BRI span. If RESTART messages are not sent, Cisco Unified CallManager assumes that the ports are in service. When the data link successfully connects with another BRI data link, it sends a RESTART message when this check box is unchecked.
Enable Status Poll	Check the check box to view the B-channel status in the debug window.
Establish Datalink on First Call	Cisco Unified CallManager establishes the data link to the gateway when the gateway registers with Cisco Unified CallManager. When you configure the gateway and switch to negotiate the TEI (terminal endpoint identifier) on the first call, you can check the check box to establish the data link on the first call. Note Default leaves the check box unchecked.
Call Routing Information - Inbound Calls	
Significant Digits	Choose the number of significant digits to collect, from 0 to 32 or All. Cisco Unified CallManager counts significant digits from the right (last digit) of the number called. If you choose <i>All</i>, the Cisco Unified CallManager does not truncate the inbound number. EXAMPLE Digits received are 123456. Significant digits setting is 4. Digits translated are 3456. Use for the processing of incoming calls and to indicate the number of digits, starting from the last digit of the called number, that are used to route calls that are coming into the BRI span. See Prefix DN.
Calling Search Space	Choose the appropriate calling search space. A calling search space designates a collection of route partitions that are searched to determine how a collected (originating) number should be routed.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when automated alternate routing (AAR) is performed. The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.
Prefix DN	Enter the prefix digits that are appended to the digits that this trunk receives on incoming calls. The Cisco Unified CallManager adds prefix digits after first truncating the number in accordance with the Num Digits setting.

Table 69-5 BRI Gateway Configuration Settings (continued)

Field	Description
Call Routing Information - Outbound Calls	
Calling Party Presentation	Choose whether you want the Cisco Unified CallManager to transmit or block caller ID. Choose <i>Default</i> if you do not want to change calling party presentation. Choose <i>Allowed</i> if you want Cisco Unified CallManager to send caller ID. Choose <i>Restricted</i> if you do not want Cisco Unified CallManager to send caller ID.
Calling Party Selection	Any outbound call on a gateway can send directory number information. Choose which directory number is sent: • Originator—Send the directory number of the calling device. • First Redirect Number—Send the directory number of the redirecting device. • Last Redirect Number—Send the directory number of the last device to redirect the call. • First Redirecting Party (External)—Send the directory number of the first redirecting device with the external phone mask applied. • Last Redirecting Party (External)—Send the directory number of the last redirecting device with the external phone mask applied.
Called party IE number type unknown	Choose the format for the number type in called party directory numbers. Cisco Unified CallManager sets the called directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified CallManager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the called directory number to be encoded to a non-national numbering plan type. Choose one of the following options: • CallManager—The Cisco Unified CallManager sets the directory number type. • International—Use when you are dialing outside the dialing plan for your country. • National—Use when you are dialing within the dialing plan for your country. • Unknown—The dialing plan is unknown. • Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number.

Table 69-5 BRI Gateway Configuration Settings (continued)

Field	Description
Calling party IE number type unknown	Choose the format for the number type in calling party directory numbers. Cisco Unified CallManager sets the calling directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified CallManager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the calling directory number to be encoded to a non-national numbering plan type. Choose one of the following options: • CallManager—The Cisco Unified CallManager sets the directory number type. • International—Use when you are dialing outside the dialing plan for your country. • National—Use when you are dialing within the dialing plan for your country. • Unknown—The dialing plan is unknown. • Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number.
Called Numbering Plan	Choose the format for the numbering plan in called party directory numbers. Cisco Unified CallManager sets the called DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified CallManager does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of the following options: • CallManager—The Cisco Unified CallManager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—The dialing plan is unknown. • Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number.

Table 69-5 BRI Gateway Configuration Settings (continued)

Field	Description
Calling Numbering Plan	Choose the format for the numbering plan in calling party directory numbers. Cisco Unified CallManager sets the calling DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified CallManager does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of the following options: • CallManager—The Cisco Unified CallManager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—The dialing plan is unknown. • Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number.
Number of digits to strip	Choose the number of digits to strip on outbound calls, from 0 to 32. For example, when 8889725551234 is dialed, and the number of digits to strip is 3, Cisco Unified CallManager strips 888 from the outbound number.
Caller ID DN	Enter the pattern that you want to use for caller ID, from 0 to 24 digits. For example, in North America: • 555XXXX = Variable caller ID, where X equals an extension number. The CO appends the number with the area code if you do not specify it. • 5555000 = Fixed caller ID, where you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it.

Table 69-5 BRI Gateway Configuration Settings (continued)

Field	Description
BRI Protocol Type Specific Information	
Redirecting Number IE Delivery— Outbound	Check this check box to include the Redirecting Number IE in the outgoing SETUP message from the Cisco Unified CallManager to indicate the first redirecting number and the redirecting reason of the call when the call is forwarded. Uncheck the check box to exclude the first redirecting number and the redirecting reason from the outgoing SETUP message. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box. Note Default leaves the check box checked.
Redirecting Number IE Delivery— Inbound	Check this check box to accept the Redirecting Number IE in the incoming SETUP message to the Cisco Unified CallManager. Uncheck the check box to exclude the Redirecting Number IE in the incoming SETUP message to the Cisco Unified CallManager. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box. Note Default leaves the check box checked.
Setup non-ISDN Progress Indicator IE Enable	Default leaves this setting disabled (unchecked). Enable this setting only if users are not receiving ringback tones on outbound calls. When this setting is enabled, the Cisco Unified CallManager sends Q.931 Setup messages out digital (that is, non-H.323) gateways with the Progress Indicator field set to non-ISDN. This message notifies the destination device that the Cisco Unified CallManager gateway is non-ISDN and that the destination device should play in-band ringback. This problem usually associates with Cisco Unified CallManagers that connect to PBXs through digital gateways.
Product-Specific Configuration	
Model-specific configuration fields that are defined by the gateway manufacturer	The model-specific fields under product-specific configuration define the gateway manufacturer. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the “?” information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, refer to the documentation for the specific gateway that you are configuring or contact the manufacturer.

Additional Information

See the “[Related Topics](#)” section on page 69-76.

Digital Access T1 Configuration Settings

Table 69-6 provides detailed descriptions for Digital Access T1 configuration settings.

Table 69-6 Digital Access T1 Configuration Settings

Field	Description
MAC Address (non-IOS gateway)	Enter MAC address of the gateway. The MAC address uniquely identifies the hardware device. You must enter a 12-hexadecimal character value.
Domain Name	For MGCP gateways, this display-only field contains a string that Cisco Unified CallManager generates that uniquely identifies the MGCP digital interface. For example: S1/DS1-0@VG200-2 S1 indicates slot 1, DS1-0 designates the digital interface, and @VG200-2 designates the MGCP domain name.
Note Enter either a MAC address or a domain name, whichever applies.	
Description	Enter a description that clarifies the purpose of the device.
Device Pool	From the drop-down list box, choose the appropriate device pool. The device pool specifies a collection of properties for this device including CallManager Group, Date/Time Group, Region, and Calling Search Space for auto-registration of devices.
Call Classification	This parameter determines whether an incoming call that is using this gateway is considered off the network (OffNet) or on the network (OnNet). When the Call Classification field is configured as Use System Default, the setting of the Cisco Unified CallManager clusterwide service parameter, Call Classification, determines whether the gateway is OnNet or OffNet. This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively.
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that is defined in a Media Resource List.
Packet Capture Mode (for Cisco IOS MGCP gateways only)	Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, refer to the <i>Cisco Unified CallManager Security Guide</i> .

Table 69-6 Digital Access T1 Configuration Settings (continued)

Field	Description
Packet Capture Duration (for Cisco IOS MGCP gateways only)	Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, refer to the <i>Cisco Unified CallManager Security Guide</i> .
Calling Search Space	From the drop-down list box, choose the appropriate calling search space. A calling search space designates a collection of route partitions that are searched to determine how a collected (originating) number should be routed. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the Max List Box Items enterprise parameter specifies, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Calling Search Space window. Enter a partial calling search space name in the List items where Name contains field. Click the desired calling search space name in the list of calling search spaces that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when automated alternate routing (AAR) is performed. The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.
Location	Choose the appropriate location for this device. The location specifies the total bandwidth that is available for calls to and from this location. A location setting of None means that the locations feature does not keep track of the bandwidth that this device consumes.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.
MLPP Domain	From the drop-down list box, choose an MLPP domain to associate with this device. If you leave the value <None>, this device inherits its MLPP domain from the value that was set for the device's device pool. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value that was set for the MLPP Domain Identifier enterprise parameter.

Table 69-6 Digital Access T1 Configuration Settings (continued)

Field	Description
MLPP Indication	This setting is not available on all devices. If available, this setting specifies whether a device that play precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options: • Default—This device inherits its MLPP indication setting from its device pool. • Off—This device does not handle nor process indication of an MLPP precedence call. • On—This device does handle and process indication of an MLPP precedence call. Note Do not configure a device with the following combination of settings: MLPP Indication is set to <i>Off</i> or <i>Default</i> (when default is <i>Off</i>) while MLPP Preemption is set to <i>Forceful</i>.
MLPP Preemption	This setting is not available on all devices. If available, this setting specifies whether a device that is capable of preempting calls in progress will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options: • Default—This device inherits its MLPP preemption setting from its device pool. • Disabled—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. • Forceful—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. Note Do not configure a device with the following combination of settings: MLPP Indication is set to <i>Off</i> or <i>Default</i> (when default is <i>Off</i>) while MLPP Preemption is set to <i>Forceful</i>.
Handle DTMF Precedence Signals	Check this box to enable this gateway to interpret special DTMF signals as MLPP precedence levels.
Load Information	Enter the appropriate firmware load information for the gateway. The values that you enter here override the default values for this gateway.
Port Selection Order	Choose the order in which channels or ports are allocated for outbound calls from first (lowest number port) to last (highest number port) or from last to first. Valid entries include Top Down (first to last) or Bottom Up (last to first). If you are not sure which port order to use, choose Top Down.

Table 69-6 Digital Access T1 Configuration Settings (continued)

Field	Description
Digit Sending	Choose one of the following digit-sending types for out-dialing: • DTMF—Dual-tone multifrequency. Normal touchtone dialing • MF—Multifrequency • PULSE—Pulse (rotary) dialing
Network Locale	From the drop-down list box, choose the locale that is associated with the gateway. The network locale identifies a set of detailed information to support the hardware in a specific location. The network locale contains a definition of the tones and cadences that the device uses in a specific geographic area. Note Choose only a network locale that is already installed and supported by the associated devices. The list contains all available network locales for this setting, but not all are necessarily installed. If the device is associated with a network locale that it does not support in the firmware, the device will fail to come up.
SMDI Base Port	Enter the first SMDI port number of the T1 span. If you set this parameter to a nonzero value and this gateway belongs to an unknown type of route list, route group, or route list, hunting does not continue past this span.
V150 (subset)	Check this box to enable v150 (subset) modem relay support on the gateways. This feature is currently used by IP-STE to support end-to-end secure calls to an ISDN-STE. (Applies only to T1 PRI and T1 CAS.) The default value specifies unchecked.
Product-Specific Configuration	
Model-specific configuration fields that the gateway manufacturer defines	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the “?” information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, refer to the documentation for the specific gateway that you are configuring or contact the manufacturer.

Additional Information

See the [“Related Topics”](#) section on page 69-76.

H.323 Gateway Configuration Settings

Table 69-7 lists configuration settings for H.323 gateways.

Table 69-7 H.323 Gateway Configuration Settings

Field	Description
Device Information	
Device Name	Enter a unique name that Cisco Unified CallManager uses to identify the device. Use either the IP address or the host name as the device name.
Description	Enter a description that clarifies the purpose of the device.
Device Pool	From the drop-down list box, choose the appropriate device pool. The device pool specifies a collection of properties for this device including CallManager Group, Date/Time Group, Region, and Calling Search Space for auto-registration of devices.
Call Classification	This parameter determines whether an incoming call that is using this gateway is considered off the network (OffNet) or on the network (OnNet). When the Call Classification field is configured as Use System Default, the setting of the Cisco Unified CallManager clusterwide service parameter, Call Classification, determines whether the gateway is OnNet or OffNet. This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively.
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, among the available media resources according to the priority order that a Media Resource Group List defines.
Packet Capture Mode	Configure this field only when you need to troubleshoot encrypted signaling information for the H.323 gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, refer to the <i>Cisco Unified CallManager Security Guide</i> .
Packet Capture Duration	Configure this field only when you need to troubleshoot encrypted signaling information for the H.323 gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, refer to the <i>Cisco Unified CallManager Security Guide</i> .
Location	Choose the appropriate location for this device. The location specifies the total bandwidth that is available for calls to and from this location. A location setting of None means that the locations feature does not keep track of the bandwidth that this device consumes.

Table 69-7 H.323 Gateway Configuration Settings (continued)

Field	Description
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.
Tunneled Protocol	Choose the QSIG option if you want to use H.323 gateways to transport (tunnel) non-H.323 protocol information in H.323 signaling messages from Cisco Unified CallManager to other Annex M.1-compliant H.323 PINXs. QSIG tunneling supports the following features: Call Completion, Call Diversion, Call Transfer, Identification Services, Message Waiting Indication, and Path Replacement. Note Refer to the <i>Cisco Unified CallManager Compatibility Matrix</i> for information about Annex M.1 feature compatibility with third-party vendor(s).
Signaling Port	This field applies only to H.323 devices. The value designates the H.225 signaling port that this device uses. Default value specifies 1720. Valid values range from 1 to 65535.
Media Termination Point Required	If you want a Media Termination Point to implement features that H.323 does not support (such as hold and transfer), check the check box. Use this check box only for H.323 clients and H.323 devices that do not support the H.245 Empty Capabilities Set message. If you check this check box to require an MTP and this device becomes the endpoint of a video call, the call will be audio only.
Retry Video Call as Audio	This check box applies only to video endpoints that receive a call. By default, the system checks this check box to specify that this device should immediately retry a video call as an audio call (if it cannot connect as a video call) prior to sending the call to call control for rerouting. If you uncheck this check box, a video call that fails to connect as video does not try to establish as an audio call. The call then fails to call control. Call control reroutes the call within the route/hunt list. If Automatic Alternate Routing (AAR) is configured and enabled, call control also reroutes the call between route/hunt lists.

Table 69-7 H.323 Gateway Configuration Settings (continued)

Field	Description
Wait for Far End H.245 Terminal Capability Set	This field applies only to H.323 devices. By default, system checks this check box to specify that Cisco Unified CallManager needs to receive the far-end H.245 Terminal Capability Set before it sends its H.245 Terminal Capability Set. Unchecking this check box specifies that Cisco Unified CallManager should initiate capabilities exchange. Note Uncheck this check box to allow calls through H.320 gateways for ISDN calls to and from other H.323 and H.320 endpoints.
Path Replacement Support	This check box displays if you choose the QSIG option from the Tunneled Protocol drop-down list box. This setting works with QSIG tunneling (Annex M.1) to ensure that non-H.323 information gets sent on the leg of the call that uses path replacement. Note The default setting leaves the check box unchecked. When you choose the QSIG Tunneled Protocol option, the system automatically checks the check box.
Transmit UTF-8 for Calling Party Name	This device uses the user locale setting of the device's device pool to determine whether to send unicode and whether to translate received unicode information. For the sending device, if you check this check box and the user locale setting in the device's device pool matches the terminating phone's user locale, the device sends unicode. If the user locale settings do not match, the device sends ASCII. The receiving device translates incoming unicode characters based on the user locale setting of the sending device's device pool. If the user locale setting matches the terminating phone's user locale, the phone displays the characters. Note The phone may display junk characters if the two ends of the trunk configure user locales that do not belong to the same language group.

Table 69-7 H.323 Gateway Configuration Settings (continued)

Field	Description
SRTP Allowed	Check the SRTP Allowed check box if you want Cisco Unified CallManager to allow secure and nonsecure calls over the gateway. If you do not check this check box, Cisco Unified CallManager prevents SRTP negotiation with the gateway and uses RTP.  Caution If you check this check box, Cisco strongly recommends that you configure IPSec, so you do not expose keys and other security-related information during call negotiations. If you do not configure IPSec correctly, signaling between Cisco Unified CallManager and the gateway is nonsecure. For more information on encryption for gateways, refer to the <i>Cisco Unified CallManager Security Guide</i>.
Multilevel Precedence and Preemption (MLPP) Information	
MLPP Domain	From the drop-down list box, choose an MLPP domain to associate with this device. If you leave the value <None>, this device inherits its MLPP domain from the value that was set for the device's device pool. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value that was set for the MLPP Domain Identifier enterprise parameter.
MLPP Indication	This device type does not have this setting.
MLPP Preemption	This device type does not have this setting.
Call Routing Information - Inbound Calls	
Significant Digits	Significant digits represent the number of final digits that are retained on inbound calls. Use for the processing of incoming calls and to indicate the number of digits that are used to route calls coming into the device. Choose the number of significant digits to collect, from 0 to 32. Cisco Unified CallManager counts significant digits from the right (last digit) of the number called.

Table 69-7 H.323 Gateway Configuration Settings (continued)

Field	Description
Calling Search Space	From the drop-down list box, choose the appropriate calling search space. A calling search space specifies the collection of Route Partitions that are searched to determine how a collected (originating) number should be routed. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the Max List Box Items enterprise parameter specifies, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Calling Search Space window. Enter a partial calling search space name in the List items where Name contains field. Click the desired calling search space name in the list of calling search spaces that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.
Prefix DN	Enter the prefix digits that are appended to the called party number on incoming calls. Cisco Unified CallManager adds prefix digits after first truncating the number in accordance with the Significant Digits setting.
Redirecting Number IE Delivery—Inbound	Check this check box to accept the Redirecting Number IE in the incoming SETUP message to the Cisco Unified CallManager. Uncheck the check box to exclude the Redirecting Number IE in the incoming SETUP message to the Cisco Unified CallManager. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box.

Table 69-7 H.323 Gateway Configuration Settings (continued)

Field	Description
Enable Inbound FastStart	Check this check box to enable the H.323 FastStart call connections on incoming calls. By default, the check box remains unchecked for the H.323 gateway. For intercluster calls, you must check the Enable Inbound FastStart check box on Cisco Unified CallManager servers in other clusters for the outbound FastStart feature to work. Note If you updated Cisco CallManager 3.3(2) servers in other clusters with support patch B, do not enable inbound FastStart because 3.3(2)spB does not support the inbound FastStart feature over intercluster trunks.
Call Routing Information - Outbound Calls	
Calling Party Selection	Any outbound call on a gateway can send directory number information. Choose which directory number is sent: • Originator—Send the directory number of the calling device. • First Redirect Number—Send the directory number of the redirecting device. • Last Redirect Number—Send the directory number of the last device to redirect the call. • First Redirect Number (External)—Send the directory number of the first redirecting device with the external phone mask applied. • Last Redirect Number (External)—Send the directory number of the last redirecting device with the external phone mask applied.
Calling Party Presentation	Choose whether you want the Cisco Unified CallManager to allow or restrict the display of the calling party phone number. Choose <i>Default</i> if you do not want to change calling line ID presentation. Choose <i>Allowed</i> if you want Cisco Unified CallManager to send “Calling Line ID Allowed” on outbound calls. Choose <i>Restricted</i> if you want Cisco Unified CallManager to send “Calling Line ID Restricted” on outbound calls. For more information about this field, see Table 17-6 in the “Calling Party Number Transformations Settings” section in the <i>Cisco Unified CallManager System Guide</i>.

Table 69-7 **H.323 Gateway Configuration Settings (continued)**

Field	Description
Called party IE Number Type Unknown	Choose the format for the number type in called party directory numbers. Cisco Unified CallManager sets the called directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified CallManager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the called directory number to be encoded to a non-national type numbering plan. Choose one of the following options: • Cisco Unified CallManager—Use when the Cisco Unified CallManager sets the directory number type. • Unknown—This option specifies that the dialing plan is unknown. • National—Use when you are dialing within the dialing plan for your country. • International—Use when you are dialing outside the dialing plan for your country. • Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number.

Table 69-7 H.323 Gateway Configuration Settings (continued)

Field	Description
Calling party IE Number Type Unknown	Choose the format for the number type in calling party directory numbers. Cisco Unified CallManager sets the calling directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified CallManager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the calling directory number to be encoded to a non-national type numbering plan. Choose one of the following options: • Cisco Unified CallManager—Use when the Cisco Unified CallManager sets the directory number type. • Unknown—This option specifies that the dialing plan is unknown. • National—Use when you are dialing within the dialing plan for your country. • International—Use when you are dialing outside the dialing plan for your country. • Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number.
Called Numbering Plan	Choose the format for the numbering plan in called party directory numbers. Cisco Unified CallManager sets the called DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified CallManager does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of the following options: • Cisco Unified CallManager—Use when the Cisco Unified CallManager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—This option specifies that the dialing plan is unknown.

Table 69-7 H.323 Gateway Configuration Settings (continued)

Field	Description
Calling Numbering Plan	Choose the format for the numbering plan in calling party directory numbers. Cisco Unified CallManager sets the calling DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified CallManager does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of the following options: • Cisco Unified CallManager—Use when the Cisco Unified CallManager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—This option specifies that the dialing plan is unknown.
Caller ID DN	Enter the pattern that you want to use for calling line ID, from 0 to 24 digits. For example, in North America: • 555XXXX = Variable calling line ID, where X equals an extension number. The CO appends the number with the area code if you do not specify it. • 5555000 = Fixed calling line ID. Use when you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it.
Display IE Delivery	Check the check box to enable delivery of the display IE in SETUP, CONNECT, and NOTIFY messages for the calling and called party name delivery service.
Redirecting Number IE Delivery—Outbound	Check this check box to include the Redirecting Number IE in the outgoing SETUP message from the Cisco Unified CallManager to indicate the first redirecting number and the redirecting reason of the call when the call is forwarded. Uncheck the check box to exclude the first redirecting number and the redirecting reason from the outgoing SETUP message. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box.

Table 69-7 H.323 Gateway Configuration Settings (continued)

Field	Description
Enable Outbound FastStart	Check this check box to enable the H.323 FastStart feature on outgoing calls. By default, the check box remains unchecked for the H.323 gateway or trunk. Note When you check the Enable Outbound FastStart check box, you must set the Media Termination Point Required, Media Resource Group Lists, and Codec for Outbound FastStart.
Codec For Outbound FastStart	Use the drop-down list box to choose the codec for use with the H.323 device for an outbound FastStart call: • G711 u-law 64K (default) • G711 a-law 64K • G723 • G729 • G729AnnexA • G729AnnexB • G729AnnexA-AnnexB Note When you check the Enable Outbound FastStart check box, you must choose the codec for supporting outbound FastStart calls. You may need to click Save prior to choosing the Codec For Outbound FastStart.

Additional Information

See the [“Related Topics”](#) section on page 69-76.

Analog Access Gateway Configuration Settings

[Table 69-8](#) lists configuration settings for Analog Access gateways (Cisco Catalyst 6000 24 port FXS Gateway).

Table 69-8 Analog Access Gateway Configuration Settings

Field	Description
Device Information	
MAC Address	Enter MAC address of the gateway. The MAC address uniquely identifies the hardware device. You must enter a 12-hexadecimal character value.
Description	Enter the purpose of the device.

Table 69-8 **Analog Access Gateway Configuration Settings (continued)**

Field	Description
Device Pool	From the drop-down list box, choose the appropriate device pool. The device pool specifies a collection of properties for this device including CallManager Group, Date/Time Group, Region, and Calling Search Space for auto-registration of devices.
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that a Media Resource Group List defines.
Calling Search Space	From the drop-down list box, choose the appropriate calling search space. The calling search space specifies a collection of partitions that are searched to determine how a collected (originating) number should be routed. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the Max List Box Items enterprise parameter specifies, the ellipsis button (...) displays next to the drop-down list box. Click the ... button to display the Select Calling Search Space window. Enter a partial calling search space name in the List items where Name contains field. Click the desired calling search space name in the list of calling search spaces that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.
Location	Choose the appropriate location for this device. The location specifies the total bandwidth that is available for calls to and from this location. A location setting of None means that the locations feature does not keep track of the bandwidth that this device consumes.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.

Table 69-8 **Analog Access Gateway Configuration Settings (continued)**

Field	Description
Network Locale	From the drop-down list box, choose the locale that is associated with the gateway. The network locale identifies a set of detailed information to support the hardware in a specific location. The network locale contains a definition of the tones and cadences that the device uses in a specific geographic area. Note Choose only a network locale that is already installed and supported by the associated devices. The list contains all available network locales for this setting, but not all are necessarily installed. If the device is associated with a network locale that it does not support in the firmware, the device will fail to come up.
Port Selection Order	Choose the order in which ports are chosen. If you are not sure which port order to use, choose Top Down: • Top Down—Selects ports in descending order, from port 1 to port 8. • Bottom Up—Selects ports in ascending order, from port 8 to port 1.
Load Information	Enter the appropriate firmware load information for the gateway. The value that you enter here overrides the default firmware load for this gateway type.
Transmit UTF-8 for Calling Party Name	This device uses the user locale setting of the device's device pool to determine whether to send unicode and whether to translate received unicode information. For the sending device, if you check this check box and the user locale setting in the device's device pool matches the terminating phone's user locale, the device sends unicode. If the user locale settings do not match, the device sends ASCII. The receiving device translates incoming unicode characters based on the user locale setting of the sending device's device pool. If the user locale setting matches the terminating phone's user locale, the phone displays the characters. Note The phone may display junk characters if the two ends of the trunk configure user locales that do not belong to the same language group.
Multilevel Precedence and Preemption (MLPP) Information	
MLPP Domain	From the drop-down list box, choose an MLPP domain to associate with this device. If you leave the value <None>, this device inherits its MLPP domain from the value that was set for the device's device pool. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value that was set for the MLPP Domain Identifier enterprise parameter.
MLPP Indication	This device type does not have this setting.
MLPP Preemption	This setting does not have this device type.

Table 69-8 **Analog Access Gateway Configuration Settings (continued)**

Field	Description
Product-Specific Configuration	
Model-specific configuration fields that the gateway manufacturer defines	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the “?” information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, refer to the documentation for the specific gateway that you are configuring or contact the manufacturer.

Additional Information

See the [“Related Topics”](#) section on page 69-76.

Cisco VG248 Gateway Configuration Settings

[Table 69-9](#) lists configuration settings for the Cisco VG248 Gateways.

Table 69-9 **Cisco VG248 Gateway Configuration Settings**

Field	Description
MAC Address (Last 10 Characters)	Enter the last 10 digits of the Media Access Control (MAC) address for the Cisco VG248. Only one MAC address exists for the Cisco VG248 Analog Phone Gateway, but Cisco Unified CallManager requires unique MAC addresses for all devices. When only 10 digits of the MAC address are entered, Cisco Unified CallManager can use the MAC address for the gateway and append additional information to it to create the MAC addresses for the VGC phones. The conversion of the MAC address for each device occurs by adding the two-digit port number to the end of the MAC address (to the right of the number) and adding VGC at the beginning of the MAC address. EXAMPLE MAC Address for the Cisco VG248 is 0039A44218 the MAC address for registered port 12 in Cisco Unified CallManager is VGC0039A4421812
Description	Cisco Unified CallManager automatically provides this information by adding VGCGW immediately in front of the MAC address.
Load Information	Enter the firmware version for the Cisco VG248 that is being configured; otherwise, leave blank to use the default.

Table 69-9 Cisco VG248 Gateway Configuration Settings (continued)

Field	Description
Configured Slots, VICs and Endpoints	
Note To begin configuring ports on a module, select the module first, then click Save .	
48_PORTS	From the list of endpoint identifiers, choose one of the ports to configure the VGC_Phone ports.

Additional Information

See the [“Related Topics”](#) section on page 69-76.

Cisco IOS SCCP Gateway Configuration Settings

[Table 69-10](#) lists configuration settings for the Cisco IOS SCCP gateways.

Table 69-10 Cisco IOS SCCP Gateway Configuration Settings

Field	Description
MAC Address (last 10 Characters)	Enter the last 10 digits of the Media Access Control (MAC) address for the gateway. Use the MAC address of the interface that the <i>sccp local</i> IOS command specifies on the gateway. Valid characters include the digits 0 through 9 and the uppercase characters A through F. The conversion of the MAC address for each device occurs by adding the three-digit mapping of the slot/subunit/port to the end of the MAC address (to the right of the number). EXAMPLE MAC Address for the gateway is 0006D7E5C7 The MAC address in Cisco Unified CallManager is 0006D7E5C7281 where 281 is the three-digit mapping of the slot/subunit/port. The values 2,8 and 1 can be hex digits and each do not necessarily correspond to slot, subunit and port values. The system inserts the following two-character strings before the MAC address to indicate the phone device types: • BR—BRI phone • AN—Analog phone The system also inserts SKIGW for the gateway name.
Description	Cisco Unified CallManager automatically provides this information by adding SKIGW immediately in front of the MAC address. You can override the description.

Table 69-10 Cisco IOS SCCP Gateway Configuration Settings (continued)

Field	Description
Cisco Unified CallManager Group	From the drop-down list box, choose a Cisco Unified CallManager redundancy group. A Cisco Unified CallManager redundancy group includes a prioritized list of up to three Cisco Unified CallManagers. The first Cisco Unified CallManager in the list serves as the primary Cisco Unified CallManager. If the primary Cisco Unified CallManager is not available or fails, the gateway attempts to connect with the next Cisco Unified CallManager in the list, and so on.
Configured Slots, VICS and Endpoints	
Note	You must specify the beginning port number for some VICs. For example, if the VIC in Subunit 0 begins at 0 and has two ports (0 and 1); then, the VIC in Subunit 1 must begin at a port number greater than 1 and have two ports (2 and 3 or 4 and 5).
Note	The correct number of slots displays for each model of SCCP gateway.
Note	To begin configuring ports on a module, select the module first, then click Save .
Module in Slot 0 Module in Slot 1 Module in Slot 2 Module in Slot 3 (and so on)	For each available slot on the chosen SCCP gateway, choose the type of module that is installed. The following modules are supported. Network Modules (with VIC slots): - NM-2V—Has two VICs, one in Subunit 0 and one in Subunit 1 for FXS-SCCP. - NM-HD-2V—Has two VIC slots, one in Subunit 0 and one in Subunit 1 for FXS-SCCP or for BRI-NT/TE-SCCP. - NM-HD-2VE—Has two VIC slots, one in Subunit 0 and one in Subunit 1 for FXS-SCCP or for BRI-NT/TE-SCCP Network Modules (no VIC slots): - NM-HDA-4FXS—Has 4 FXS directly without VIC and can be extended by up to two expansion modules EM-HDA-8FXS to support 16 FXS ports. - EM-HDA-8FXS—Expansion module for the NM-HDA-4FXS Voice Interface Cards: - VIC-2FXS - VIC-4FXS - VIC2-2FXS - VIC2-2BRI-NT/TE

Table 69-10 Cisco IOS SCCP Gateway Configuration Settings (continued)

Field	Description
	At the slot level, there are four options. - NM-2V—Two subunits with option VIC-2FXS-SCCP - NM-HD-2V—Two subunits with options VIC-4FXS-SCCP, VIC2-2FXS-SCCP, VIC2-2BRI-NT/TE-SCCP - NM-HD-2VE—Two subunits with options VIC-4FXS-SCCP, VIC2-2FXS-SCCP, VIC2-2BRI-NT/TE-SCCP - NM-HDA—Three subunits with options NM-HDA-4FXS-SCCP, EM-8FXS-EM0-SCCP, EM-8FXS-EM1-SCCP In NM-HDA, these options do not represent true VICs. The VIC2-2BRI-NT/TE represents the only VIC for BRI SCCP phones. VG224 GW differs from all others. The following option supports only one slot: - ANALOG—One subunit option 24FXS-SCCP (supports 24 FXS ports) The option None means there is no network modules installed.
Product Specific Configuration	
Model-specific configuration fields defined by the gateway manufacturer	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the “?” information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, refer to the documentation for the specific gateway that you are configuring or contact the manufacturer.

Additional Information

See the [“Related Topics”](#) section on page 69-76.

Port Configuration Settings

See the following sections for tables that list detailed descriptions for all port type configuration fields:

- [POTS Port Configuration Settings, page 69-60](#)
- [Loop-Start Port Configuration Settings, page 69-62](#)
- [Ground-Start Port Configuration Settings, page 69-63](#)
- [E & M Port Configuration Settings, page 69-63](#)

For detailed information about gateway configuration settings, see the [Gateway Configuration Settings, page 69-13](#).

POTS Port Configuration Settings

Table 69-11 describes the POTS port configuration settings.

Table 69-11 POTS Port Configuration Settings

Field	Description
Port Selection	
Port Type	For POTS ports, this field displays <i>POTS</i> .
Beginning Port Number Ending Port Number	Choose whether you want to add and configure all available ports, a single port, or a range of ports by setting values for the Beginning Port Number and Ending Port Number fields: - To specify a range of ports, choose appropriate values for Beginning Port Number and Ending Port Number. - To create a single port, choose the same number in the Beginning Port Number and Ending Port Number fields. - To add all available ports, choose All Ports for both the Beginning Port Number and Ending Port Number fields.
Port Details	
Port Direction	Choose the direction of calls that pass through this port: - Inbound—Use for incoming calls only. - Outbound—Use for outgoing calls. - Bothways—Use for inbound and outbound calls (default).
Audio Signal Adjustment into IP Network	This field specifies the gain or loss that is applied to the received audio signal relative to the port application type. Note Improper gain setting may cause audio echo. Use caution when you are adjusting this setting.
Audio Signal Adjustment from IP Network	This field specifies the gain or loss that is applied to the transmitted audio signal relative to the port application type. Note Improper gain setting may cause audio echo. Use caution when you are adjusting this setting.
Prefix DN	Enter the prefix digits that are appended to the digits that this trunk receives on incoming calls. The Cisco Unified CallManager adds prefix digits after it truncates the number in accordance with the Num Digits setting.
Num Digits	Enter the number of significant digits to collect, from 0 to 32. Cisco Unified CallManager counts significant digits from the right (last digit) of the number that is called. Use this field for the processing of incoming calls and to indicate the number of digits starting from the last digit of the called number that are used to route calls that are coming into the PRI span. See Prefix DN.

Table 69-11 POTS Port Configuration Settings (continued)

Field	Description
Expected Digits	Enter the number of digits that are expected on the inbound side of the trunk. For this rarely used field, leave zero as the default value if you are unsure.
Call Restart Timer (1000-5000 ms)	Call Restart Timer (1000-5000 ms); ms indicates time in milliseconds.
Offhook Validation Timer (100-1000 ms)	Offhook Validation Timer (100-1000 ms); ms indicates time in milliseconds.
Onhook Validation Timer (100-1000 ms)	Onhook Validation Timer (100-1000 ms); ms indicates time in milliseconds.
Hookflash Timer (100-1500 ms)	Hookflash Timer (100-1500 ms); ms indicates time in milliseconds.
SMDI Port Number (0-4096)	Use this field for analog access ports that connect to a voice-messaging system. Set the SMDI Port Number equal to the actual port number on the voice-messaging system to which the analog access port connects. Note Voice-mail logical ports typically must match physical ports for the voice-messaging system to operate correctly.
Unattended Port	Check this check box to indicate an unattended port on this device.
Product-Specific Configuration	
Model-specific configuration fields that the gateway manufacturer defines	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the “?” information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, refer to the documentation for the specific gateway that you are configuring or contact the manufacturer.

Additional Information

See the [“Related Topics”](#) section on page 69-76.

Loop-Start Port Configuration Settings

Table 69-12 describes the loop-start port configuration settings.

Table 69-12 Loop-Start Port Configuration Settings

Field	Description
Port Type	From the Port Type drop-down list box, choose Loop Start .
Beginning Port Number Ending Port Number	Choose whether you want to add and configure all available ports, a single port, or a range of ports by setting values for the Port Number and End Port Number fields: - To specify a range of ports, choose appropriate values for Beginning Port Number and Ending Port Number. - To create a single port, choose the same number in the Beginning Port Number and Ending Port Number fields. - To add all available ports, choose All Ports for both the Beginning Port Number and Ending Port Number fields.
Port Direction	Choose the direction of calls that pass through this port: - Inbound—Use for incoming calls only. - Outbound—Use for outgoing calls. - Both Ways—Use for inbound and outbound calls.
Attendant DN	Enter the directory number to which you want incoming calls routed; for example, zero or a directory number for an attendant.
Unattended Port	Check this check box to indicate an unattended port on this device.
Product-Specific Configurations	
Model-specific configuration fields that the gateway manufacturer defines	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the “?” information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, refer to the documentation for the specific gateway that you are configuring or contact the manufacturer.

Additional Information

See the “[Related Topics](#)” section on page 69-76.

Ground-Start Port Configuration Settings

Table 69-13 describes the ground-start port configuration settings.

Table 69-13 *Ground-Start Port Configuration Settings*

Field	Description
Port Type	From the Port Type drop-down list box, choose Ground Start .
Beginning Port Number Ending Port Number	Choose whether you want to add and configure all available ports, a single port, or a range of ports by setting values for the Beginning Port Number and Ending Port Number fields: - To specify a range of ports, choose appropriate values for Beginning Port Number and Ending Port Number. - To create a single port, choose the same number in the Beginning Port Number and Ending Port Number fields. - To add all available ports, choose All Ports for both the Beginning Port Number and Ending Port Number fields.
Port Direction	Choose the direction of calls that pass through this port: - Inbound—Use for incoming calls only. - Outbound—Use for outgoing calls. - Both Ways—Use for inbound and outbound calls.
Attendant DN	Enter the number to which you want incoming calls to be routed; for example, zero or a directory number for an attendant.
Unattended Port	Check this check box to indicate an unattended port on this device.
Product-Specific Configuration	
Model-specific configuration fields that the gateway manufacturer defines	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the “?” information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, refer to the documentation for the specific gateway that you are configuring or contact the manufacturer.

Additional Information

See the “[Related Topics](#)” section on page 69-76.

E & M Port Configuration Settings

E & M (Ear and Mouth) ports allow connection for PBX trunk lines (tie lines). E & M designates a signaling technique for two-wire, four-wire, and six-wire telephone and trunk interfaces.

Table 69-14 describes the E & M port configuration settings.

Table 69-14 E & M Port Configuration Settings

Field	Description
Port Type	From the Port Type drop-down list box, choose EANDM .
Beginning Port Number Ending Port Number	Choose whether you want to add and configure all available ports, a single port, or a range of ports by setting values for the Beginning Port Number and Ending Port Number fields: - To specify a range of ports, choose appropriate values for Beginning Port Number and Ending Port Number. - To create a single port, choose the same number in the Beginning Port Number and Ending Port Number fields. - To add all available ports, choose All Ports for both the Beginning Port Number and Ending Port Number fields.
Port Details	
Port Direction	Choose the direction of calls that pass through this port: - Inbound—Use for incoming calls only. - Outbound—Use for outgoing calls. - Both Ways—Use for inbound and outbound calls.
Calling Party Selection	Any outbound call on a gateway can send directory number information. Choose which directory number is sent: - Originator—Send the directory number of the calling device. - First Redirect Number—Send the directory number of the redirecting device. - Last Redirect Number—Send the directory number of the last device to redirect the call. - First Redirect Number (External)—Send the directory number of the first redirecting device with the external phone mask applied. - Last Redirect Number (External)—Send the directory number of the last redirecting device with the external phone mask applied.
Caller ID Type	Choose the caller ID type: - ANI—Choose this type to use the Asynchronous Network Interface (ANI) caller ID type. - DNIS—Choose this type to use the Dialed Number Identification Service (DNIS) caller ID type.

Table 69-14 E & M Port Configuration Settings (continued)

Field	Description
Caller ID DN	Enter the pattern that you want to use for calling line ID, from 0 to 24 digits. For example, in North America: 555XXXX = Variable calling line ID, where X equals an extension number. The CO appends the number with the area code if you do not specify it. 5555000 = Fixed calling line ID, where you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it.
Prefix DN	Enter the prefix digits that are appended to the called party number on incoming calls. The Cisco Unified CallManager adds prefix digits after first truncating the number in accordance with the Num Digits setting.
Num Digits	Choose the number of significant digits to collect, from 0 to 32. Cisco Unified CallManager counts significant digits from the right (last digit) of the number that is called. Use this field if you check the Sig Digits check box. Use this field for the processing of incoming calls and to indicate the number of digits starting from the last digit of the called number that are used to route calls that are coming into the PRI span. See Prefix DN and Sig Digits.
Expected Digits	Enter the number of digits that are expected on the inbound side of the trunk. If you are unsure, leave zero as the default value for this rarely used field.
Product-Specific Configuration	
Model-specific configuration fields that the gateway manufacturer defines	The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the “?” information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, refer to the documentation for the specific gateway that you are configuring or contact the manufacturer.

Additional Information

See the [“Related Topics”](#) section on page 69-76.

Finding Specific Gateways

Because you might have hundreds of gateways in your network, Cisco Unified CallManager lets you use specific criteria to locate specific gateways. Use these sections to find specific gateways:

- [Searching by Device Name, page 69-66](#)
- [Searching by Description, page 69-67](#)
- [Searching by Directory Number/Route Pattern, page 69-68](#)
- [Searching by Calling Search Space, page 69-69](#)
- [Searching by Device Pool, page 69-70](#)
- [Searching by Route Group, page 69-71](#)
- [Searching by Device Type, page 69-72](#)



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your gateway search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your gateway search preferences until you modify your search or close the browser.

Searching by Device Name

Use this procedure if you know the device name of a specific gateway or if you want to get a listing of all gateways that are registered with Cisco Unified CallManager.

Procedure

-
- Step 1** Choose **Device > Gateway**.
- The Find and List Gateway window displays.
- Step 2** From the drop-down list box, choose **Name**; then, choose one of the following criteria:
- begins with
 - contains
 - ends with
 - is exactly
 - is not empty
 - is empty
- Step 3** Specify the appropriate search text, if applicable. You can also specify how many items per page to display and whether to hide or show endpoints.
- Step 4** Click **Find**.
- A list of discovered gateways displays by
- Device icon
 - Device Name
 - Description (if applicable)

- Device Pool (if applicable)
- Status
- IP Address

**Tip**

To search for directory numbers within the search results, click the **Search Within Results** check box and enter your search criteria as described in the previous step.

**Note**

You can delete or reset multiple gateways from the Find and List Gateways window by checking the check boxes next to the appropriate gateways and clicking **Delete Selected** to delete the gateways or clicking **Reset Selected** to reset the gateways. You can choose all the gateways in the window by checking the check box in the matching records title bar.

Additional Information

See the [“Related Topics” section on page 69-76](#).

Searching by Description

Use this procedure if you know any key words that are used in the Description field of a specific gateway that is registered with Cisco Unified CallManager.

Procedure

-
- Step 1** Choose **Device > Gateway**.
- The Find and List Gateways window displays.
- Step 2** From the drop-down list box, choose **Description**; then, choose one of the following criteria:
- begins with
 - contains
 - ends with
 - is exactly
 - is not empty
 - is empty
- Step 3** Specify the appropriate search text, if applicable. You can also specify how many items per page to display and whether to hide or show endpoints.
- Step 4** Click **Find**.
- A list of discovered gateways displays by
- Device icon
 - Device Name
 - Description (if applicable)
 - Device Pool

- Status
- IP Address

**Tip**

To search for directory numbers within the search results, click the **Search Within Results** check box and enter your search criteria as described in the previous step.

**Note**

You can delete or reset multiple gateways from the Find and List Gateways window by checking the check boxes next to the appropriate gateways and clicking **Delete Selected** to delete the gateways or clicking **Reset Selected** to reset the gateways. You can choose all the gateways in the window by checking the check box in the matching records title bar.

Additional Information

See the [“Related Topics”](#) section on page 69-76.

Searching by Directory Number/Route Pattern

Use this procedure to locate gateways that are assigned to a specific extension or range of extensions and that are registered with Cisco Unified CallManager.

Procedure

-
- Step 1** Choose **Device > Gateway**.
The Find and List Gateways window displays.
- Step 2** From the drop-down list box, choose **DN/Route Pattern**; then, choose one of the following criteria:
- begins with
 - contains
 - ends with
 - is exactly
 - is not empty
 - is empty
- Step 3** Specify the appropriate search text, if applicable. You can also specify how many items per page to display and whether to hide or show endpoints.
- Step 4** Click **Find**.
A list of discovered gateways displays by
- Device icon
 - Device Name
 - Description (if applicable)
 - Extension (Ext.)
 - Partition

- Status
- IP Address

**Tip**

To search for directory numbers within the search results, click the **Search Within Results** check box and enter your search criteria as described in the previous step.

**Note**

You can delete or reset multiple gateways from the Find and List Gateways window by checking the check boxes next to the appropriate gateways and clicking **Delete Selected** to delete the gateways or clicking **Reset Selected** to reset the gateways. You can choose all the gateways in the window by checking the check box in the matching records title bar.

Additional Information

See the [“Related Topics” section on page 69-76](#).

Searching by Calling Search Space

Use this procedure to locate gateways that are assigned to a calling search space and that are registered with Cisco Unified CallManager.

Procedure

Step 1 Choose **Device > Gateway**.

The Find and List Gateways window displays.

Step 2 From the drop-down list box, choose **Calling Search Space**; then, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is not empty
- is empty

Step 3 Specify the appropriate search text, if applicable. You can also specify how many items per page to display and whether to hide or show endpoints.

**Tip**

You can locate an existing calling search space by choosing one from the drop-down list box under the **Find** button. This action automatically inserts the name of the calling search space that you choose into the **Find** field.

Step 4 Click **Find**.

A list of discovered gateways displays by

- Device icon
- Device Name
- Description (if applicable)
- Calling Search Space
- Status
- IP Address

**Tip**

To search for directory numbers within the search results, click the **Search Within Results** check box and enter your search criteria as described in the previous step.

**Note**

You can delete or reset multiple gateways from the Find and List Gateways window by checking the check boxes next to the appropriate gateways and clicking **Delete Selected** to delete the gateways or clicking **Reset Selected** to reset the gateways. You can choose all the gateways in the window by checking the check box in the matching records title bar.

Additional Information

See the [“Related Topics”](#) section on page 69-76.

Searching by Device Pool

Use this procedure to locate gateways that are assigned to a specific device pool and that are registered with Cisco Unified CallManager.

Procedure**Step 1** Choose **Device > Gateway**.

The Find and List Gateways window displays.

Step 2 From the drop-down list box, choose **Device Pool**; then, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is not empty
- is empty

Step 3 Specify the appropriate search text, if applicable. You can also specify how many items per page to display and whether to hide or show endpoints.

**Tip**

You can locate an existing device pool by choosing one from the drop-down list box under the **Find** button. This action automatically inserts the name of the device pool that you choose into the **Find** field.

Step 4 Click **Find**.

A list of discovered gateways displays by

- Device icon
- Device Name
- Description (if applicable)
- Device Pool
- Status
- IP Address

**Tip**

To search for directory numbers within the search results, click the **Search Within Results** check box and enter your search criteria as described in the previous step.

**Note**

You can delete or reset multiple gateways from the Find and List Gateways window by checking the check boxes next to the appropriate gateways and clicking **Delete Selected** to delete the gateways or clicking **Reset Selected** to reset the gateways. You can choose all the gateways in the window by checking the check box in the matching records title bar.

Additional Information

See the [“Related Topics” section on page 69-76](#).

Searching by Route Group

Use this procedure to locate gateways that are assigned to a specific route group and that are registered with Cisco Unified CallManager.

Procedure**Step 1** Choose **Device > Gateway**.

The Find and List Gateways window displays.

Step 2 From the drop-down list box, choose **Route Group Name**; then, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly

- is not empty
- is empty

Step 3 Specify the appropriate search text, if applicable. You can also specify how many items per page to display and whether to hide or show endpoints.

**Tip**

You can locate an existing route group by choosing one from the drop-down list box under the **Find** button. This action automatically inserts the name of the route group that you choose into the **Find** field.

Step 4 Click **Find**.

A list of discovered gateways displays by

- Device icon
- Device Name (Port)
- Description (if applicable)
- Route Group (Priority)
- Status
- IP Address

**Tip**

To search for directory numbers within the search results, click the **Search Within Results** check box and enter your search criteria as described in the previous step.

**Note**

You can delete or reset multiple gateways from the Find and List Gateways window by checking the check boxes next to the appropriate gateways. Click **Delete Selected** to delete the gateways or click **Reset Selected** to reset the gateways. You can choose all the gateways in the window by checking the check box in the matching records title bar.

Additional Information

See the [“Related Topics”](#) section on page 69-76.

Searching by Device Type

Use this procedure if you know the device type of a specific gateway or if you want to get a listing of all gateways of a particular device type.

Procedure

Step 1 Choose **Device > Gateway**.

The Find and List Gateways window displays.

Step 2 From the drop-down list box, choose **Device Type**; then, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is not empty
- is empty

Step 3 Specify the appropriate search text, if applicable. You can also specify how many items per page to display and whether to hide or show endpoints.

**Tip**

You can locate an existing device type by choosing one from the drop-down list box under the **Find** button. This action automatically inserts the name of the device type that you choose into the **Find** field.

Step 4 Click **Find**.

A list of discovered gateways displays by

- Device icon
- Device Name
- Description (if applicable)
- Device Type
- Status
- IP Address

**Tip**

To search for directory numbers within the search results, click the **Search Within Results** check box and enter your search criteria as described in the previous step.

**Note**

You can delete or reset multiple gateways from the Find and List Gateways window by checking the check boxes next to the appropriate gateways and clicking **Delete Selected** to delete the gateways or clicking **Reset Selected** to reset the gateways. You can choose all the gateways in the window by checking the check box in the matching records title bar.

Additional Information

See the [“Related Topics”](#) section on page 69-76.

Modifying Gateways and Ports

Using Cisco Unified CallManager, you perform the following tasks identically regardless of the gateway type:

- [Using Dependency Records, page 69-74](#)
- [Deleting Gateways, page 69-74](#)
- [Resetting and Restarting Gateways, page 69-75](#)
- [Updating Gateways and Ports, page 69-76](#)

Using Dependency Records

Gateways and ports use a variety of configuration information such as partitions, device pools, and directory numbers. Before updating or deleting gateways or ports, you can find configuration information about that gateway and port by using the Dependency Records link. To access the link, choose **Dependency Records** from the Related Links drop-down list box and click **Go**. For more information about this link, see the “[Dependency Records](#)” appendix.

Deleting Gateways

Complete the following steps to delete a gateway from Cisco Unified CallManager.

Before You Begin

If you try to delete a gateway that a route group is using, Cisco Unified CallManager displays a message. To find out which route groups are using the gateway, choose **Dependency Records** from the Related Links drop-down list box in the Gateway Configuration window and click **Go**. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the “[Accessing Dependency Records](#)” section on page A-2. Before deleting a gateway that is currently in use, you must perform either or both of the following tasks:

- Assign a different gateway to any route groups that are using the gateway that you want to delete. See the “[Adding Devices to a Route Group](#)” section on page 33-5.
- Delete the route groups that are using the gateway that you want to delete. See the “[Deleting a Route Group](#)” section on page 33-6.

Procedure

-
- Step 1** Choose **Device > Gateway**.
The Find and List Gateways window displays.
- Step 2** To locate a specific gateway, enter search criteria.
- Step 3** Click **Find**.
A list of discovered gateways that matches your search criteria displays.
- Step 4** Check the check box next to the gateway that you want to delete.
- Step 5** Click **Delete Selected**.
A message displays that states that you cannot undo this action.

Step 6 To delete the gateway, click **OK** or to cancel the operation, click **Cancel**.

**Tip**

You can delete all the gateways in the window by clicking **Select All** and then clicking **Delete Selected**.

Additional Information

See the [“Related Topics”](#) section on page 69-76.

Resetting and Restarting Gateways

Complete the following steps to reset or restart a gateway by using Cisco Unified CallManager.

Procedure

Step 1 Choose **Device > Gateway**.

The Find and List Gateway window displays.

Step 2 To locate a specific gateway, enter search criteria.

Step 3 Click **Find**.

A list of discovered gateways that matches your search criteria displays.

Step 4 Check the check box next to the gateway that you want to reset.

Step 5 Click **Reset Selected**.

The Device Reset window displays.

Step 6 Click one of the following choices:

- **Restart**—Restarts a device without shutting it down.
- **Reset**—Shuts down a device and brings it back up.
- **Close**—Returns to the previous window without performing any action.

**Note**

Restarting or resetting an H.323 gateway does not physically restart/reset the gateway; it only reinitializes the configuration that was loaded by Cisco Unified CallManager. When you reset any other gateway type, Cisco Unified CallManager automatically drops the calls that are using the gateway. When you restart any other gateway type, Cisco Unified CallManager attempts to preserve the calls that are using the gateway.

Additional Information

See the [“Related Topics”](#) section on page 69-76.

Updating Gateways and Ports

Complete the following steps to update a gateway or reconfigure gateway ports from Cisco Unified CallManager.

Procedure

-
- Step 1** Choose **Device > Gateway**.
The Find and List Gateways window displays.
- Step 2** To locate a specific gateway, enter search criteria.
- Step 3** Click **Find**.
A list of discovered devices displays.
- Step 4** Click the **Device Name** of the gateway that you want to update.
The Gateway Configuration window displays.
- Step 5** Update the appropriate gateway or port settings as described in the following sections.
To access gateway ports, click the icon of the gateway port or the MGCP endpoint link on the left side of the configuration window for the chosen gateway.
- [MGCP Gateway Configuration Settings, page 69-14](#)
 - [FXS/FXO Port Configuration Settings, page 69-16](#)
 - [Digital Access PRI Port Configuration Settings, page 69-20](#)
 - [Digital Access T1 Configuration Settings, page 69-40](#)
 - [Analog Access Gateway Configuration Settings, page 69-53](#)
 - [Port Configuration Settings, page 69-59](#)
- Step 6** Click **Save**.
- Step 7** To apply the changes, click **Reset** to reset the gateway.
-

Additional Information

See the [“Related Topics” section on page 69-76](#).

Related Topics

All Gateway Types

- [Adding Gateways to Cisco Unified CallManager, page 69-1](#)
- [Gateway Configuration Settings, page 69-13](#)
- [Finding Specific Gateways, page 69-66](#)
- [Searching by Device Name, page 69-66](#)
- [Searching by Description, page 69-67](#)
- [Searching by Directory Number/Route Pattern, page 69-68](#)
- [Searching by Calling Search Space, page 69-69](#)

- [Searching by Device Pool, page 69-70](#)
- [Searching by Route Group, page 69-71](#)
- [Searching by Device Type, page 69-72](#)
- [Using Dependency Records, page 69-74](#)
- [Modifying Gateways and Ports, page 69-74](#)
- [Deleting Gateways, page 69-74](#)
- [Resetting and Restarting Gateways, page 69-75](#)
- [Updating Gateways and Ports, page 69-76](#)

IOS MGCP Gateways

- [Adding a Cisco IOS MGCP Gateway, page 69-2](#)
- [MGCP Gateway Configuration Settings, page 69-14](#)
- [Port Configuration Settings, page 69-59](#)
- [Gateway Configuration Checklist, *Cisco Unified CallManager System Guide*](#)

SCCP Gateways

- [Adding a Cisco IOS SCCP Gateway, page 69-8](#)
- [Cisco IOS SCCP Gateway Configuration Settings, page 69-57](#)

Non-IOS MGCP Gateways

- [Adding a Non-IOS MGCP Gateway, page 69-9](#)

H.323 Gateways

- [Adding a Cisco IOS H.323 Gateway, page 69-10](#)
- [H.323 Gateway Configuration Settings, page 69-44](#)

Analog Access Gateways

- [Adding an Analog Access Gateway and Ports, page 69-11](#)
- [Analog Access Gateway Configuration Settings, page 69-53](#)
- [Adding a Cisco VG248 Analog Phone Gateway, page 69-12](#)
- [Cisco VG248 Gateway Configuration Settings, page 69-56](#)
- [Cisco VG248 Analog Phone Gateway Software Configuration Guide](#)

BRI Gateways

- [BRI Gateway Configuration Settings, page 69-33](#)
- [MGCP BRI Call Connections, *Cisco Unified CallManager System Guide*](#)
- [MGCP BRI Gateway Configuration Checklist, *Cisco Unified CallManager System Guide*](#)

Ports

- [Adding FXS Ports to an MGCP Gateway, page 69-4](#)
- [Adding FXO Ports to an MGCP Gateway, page 69-5](#)

- [Adding Digital Access T1 Ports to an MGCP Gateway, page 69-7](#)
- [Adding a Digital Access PRI Device to an MGCP Gateway, page 69-7](#)
- [Adding a BRI Port to an MGCP Gateway, page 69-8](#)
- [FXS/FXO Port Configuration Settings, page 69-16](#)
- [Digital Access PRI Port Configuration Settings, page 69-20](#)
- [Digital Access T1 Configuration Settings, page 69-40](#)
- [POTS Port Configuration Settings, page 69-60](#)
- [Loop-Start Port Configuration Settings, page 69-62](#)
- [Ground-Start Port Configuration Settings, page 69-63](#)
- [E & M Port Configuration Settings, page 69-63](#)

Phones and Directory Numbers

- [Cisco Unified IP Phone Configuration, page 70-1](#)
- [Phone Configuration Settings, page 70-6](#)
- [Directory Number Configuration, page 49-1](#)
- [Directory Number Configuration Settings, page 49-6](#)



Cisco Unified IP Phone Configuration

Cisco Unified IP Phones as full-featured telephones can plug directly into your IP network. You use the Cisco Unified CallManager Administration Phone Configuration window to configure the following Cisco Unified IP Phones and devices:

- Cisco Unified IP Phone 7900 family for both SCCP and SIP protocols
- Cisco IP Video Phone 7985
- Cisco IP Phone model 30 VIP
- Cisco IP Phone model 12 S
- Cisco IP Phone model 12 SP
- Cisco IP Phone model 12 SP+
- Cisco IP Phone model 30 SP+
- H.323 clients
- Computer Telephony Integration (CTI) ports
- Cisco IP Communicator
- Cisco Unified Personal Communicator
- Cisco ATA 186 telephone adapter
- Third-party SIP Device (Basic) and (Advanced)
- IP-STE
- Cisco VG248 ports (analog phones)



Note

You configure the Cisco VG248 gateway from the Gateway Configuration window of Cisco Unified CallManager Administration. From this window, you configure the gateway analog phone ports (doing this takes you to the Phone Configuration window). When you want to update the VG248 ports, use the Phone Configuration window. The following procedures apply to update or delete this phone type. See the [“Gateway Configuration” section on page 69-1](#) for Cisco VG248 Gateway configuration information.

After you add a Cisco Unified IP Phone to Cisco Unified CallManager Administration, information from the RIS Data Collector service displays in the Phone Configuration window. When available, the IP address of the device and the name of the Cisco Unified CallManager with which the device registered display.

The following topics provide information about working with and configuring Cisco Unified IP Phones in Cisco Unified CallManager Administration:

- [Configuring Cisco Unified IP Phones](#), page 70-2
- [Gateway Configuration](#), page 69-1
- [Finding a Phone](#), page 70-29
- [Directory Number Configuration Overview](#), page 49-1
- [Phone Button Template Configuration](#), page 76-1
- [Phone Configuration Settings](#), page 70-6
- [Phone Configuration Checklist](#), *Cisco Unified CallManager System Guide*

Additional Information

See the “[Related Topics](#)” section on page 70-30.

Configuring Cisco Unified IP Phones

You can automatically add phones to the Cisco Unified CallManager database by using auto-registration or manually add phones by using the Phone Configuration windows.

By enabling auto-registration, you can automatically add a Cisco Unified IP Phone to the Cisco Unified CallManager database when you connect the phone to your IP telephony network. During auto-registration, Cisco Unified CallManager assigns the next available sequential directory number to the phone. In many cases, you might not want to use auto-registration; for example, if you want to assign a specific directory number to a phone.



Note

Cisco recommends using auto-registration in small configurations or testing labs only.

If you configure the clusterwide security mode to mixed mode, Cisco Unified CallManager disables auto-registration.

If you do not use auto-registration, you must manually add phones to the Cisco Unified CallManager database.

After you add a Cisco Unified IP Phone to Cisco Unified CallManager Administration, the RIS Data Collector service displays the device name, registration status, and the IP address of the Cisco Unified CallManager to which the phone is registered in the Phone Configuration window.

Before a Cisco Unified IP Phone can be used, you must use this procedure to add the phone to Cisco Unified CallManager. You can also use this procedure to configure third-party SIP phones, H.323 clients, CTI ports, the Cisco ATA 186 telephone adapter, or the Cisco IP Communicator. H.323 clients can be Microsoft NetMeeting clients. CTI ports designate virtual devices that Cisco Unified CallManager applications such as Cisco SoftPhone and Cisco Unified CallManager AutoAttendant use.



Note

Add the Cisco VG248 Phone Ports from the Gateway Configuration window of Cisco Unified CallManager Administration. See the “[Gateway Configuration](#)” section on page 69-1 for configuration information.

**Timesaver**

If you plan on using nonstandard phone button and softkey templates, configure the templates before you add the phones. See the [“Configuring Phone Button Templates” section on page 76-2](#) and the [“Adding Nonstandard Softkey Templates” section on page 77-2](#) for configuration information.

Procedure

Step 1 Choose **Device > Phone**.

The Find and List Phones window displays.

Step 2 Perform one of the followings tasks:



Note For information on obtaining the MAC address, see the [“Displaying the MAC Address of a Phone” section on page 70-4](#).

- To copy an existing phone, locate the appropriate phone as described in [“Finding a Phone” section on page 70-29](#), click the **Copy** button next to the phone that you want to copy, and continue with [Step 5](#).
- To copy an existing phone and copy the directory numbers, speed dials, busy lamp field/speed dials, and service URLs that are associated with the phone, locate the appropriate phone as described in [“Finding a Phone” section on page 70-29](#), click the **Copy w/Lines** button next to the phone that you want to copy and continue with [Step 5](#).



Note The lines that get copied become shared lines between the original phone and the new phone.

- To add a new phone, click the **Add New** button, and continue with [Step 3](#).
- To update an existing phone, locate the appropriate phone as described in [“Finding a Phone” section on page 70-29](#), and continue with [Step 5](#).

Step 3 From the Phone Type drop-down list box, choose the appropriate phone type or device and click **Next**. After you choose a phone type, you cannot modify it.

Step 4 If the Select the device protocol drop-down list box displays, choose the appropriate protocol of the device and click **Next**. Otherwise, continue with [Step 5](#).

The Phone Configuration window displays.

Step 5 Enter the appropriate settings as described in [Table 70-1](#).

Only the settings that are appropriate to the chosen phone type appear in the window.

Step 6 Click **Save**.

If you are adding a phone, a message displays that states that the phone has been added to the database. To add a directory number to this phone, click one of the line links, such as *Line [1] - Add a new DN*, in the Association Information pane that displays on the left side of the window. Continue with the [“Directory Number Configuration Settings” section on page 30-5](#).

If you are updating a phone, a message displays that states that you must click the **Reset Phone** button for your changes to take effect. For more information about the **Reset Phone** button, see the [“Resetting a Phone” section on page 70-4](#).

Next Steps

To configure speed-dial buttons on this phone, see the [“Configuring Speed-Dial Buttons”](#) section on page 70-23. To configure services for this phone, see the [“Configuring Cisco Unified IP Phone Services”](#) section on page 70-24. To configure service URL buttons for this phone, see the [“Adding a Cisco Unified IP Phone Service to a Phone Button”](#) section on page 78-8. To configure busy lamp field/speed-dial settings for this phone, see the [“BLF/SpeedDial Configuration Settings”](#) section on page 70-24.

Additional Information

For more information on phone configuration, as well as H.323 clients, CTI ports, and other devices from Cisco Unified CallManager Administration, see the [“Related Topics”](#) section on page 70-30.

Displaying the MAC Address of a Phone

The Media Access Control (MAC) address comprises a unique, 12-character, hexadecimal number that identifies a Cisco Unified IP Phone or other hardware device. Locate the number on a label on the bottom of the phone (for example, 000B6A409C405 for Cisco Unified IP Phone 7900 family models or SS-00-0B-64-09-C4-05 for Cisco IP Phone models SP 12+ and 30 VIP). Cisco Unified CallManager makes the MAC address a required field for Cisco Unified IP Phone device configuration. When entering the MAC address in Cisco Unified CallManager fields, do not use spaces or dashes and do not include the “SS” that may precede the MAC address on the label.

For more information on displaying the MAC Address or additional configuration settings on Cisco Unified IP Phones, refer to the *Cisco Unified IP Phone Administration Guide* for Cisco Unified CallManager that supports the phone model. To display the MAC address for the Cisco IP Phone model 12 Series and Cisco IP Phone model 30 Series phones or the Cisco VG248 Gateway, perform the following tasks:

- Cisco IP Phone Models 12 (SP +) Series and 30 Series (VIP)—Press ** to display the MAC address on the second line of the LCD display.
- Cisco VG248 phone ports—The MAC address specifies the endpoint from the Gateway Configuration window of Cisco Unified CallManager Administration. See the [“Gateway Configuration”](#) section on page 69-1 for configuration information.
- Cisco IP Communicator—Get the MAC address from the network interface of the client PC on which you want to install the Cisco IP Communicator application.

Additional Information

See the [“Related Topics”](#) section on page 70-30.

Resetting a Phone

You do not have to reset a Cisco Unified IP Phone after you add a directory number or update its settings for your changes to take effect. Cisco Unified CallManager automatically performs the reset; however, you can reset a Cisco Unified IP Phone at any time by using the following procedure.



Note If a call is in progress, the phone does not reset until the call completes.

Procedure

- Step 1** Choose **Device > Phone**.
The Find and List Phones window displays.
- Step 2** To locate a specific phone, enter search criteria and click **Find**.
A list of phones that match the search criteria displays.
- Step 3** Check the check boxes next to the phones that you want to reset. To choose all the phones in the window, click **Select All**.
- Step 4** Click **Reset Selected**.
The Device Reset window displays.
- Step 5** Click one of the following buttons:
- **Restart**—Restarts the chosen devices without shutting them down (reregisters the phones with Cisco Unified CallManager).
 - **Reset**—Shuts down the chosen devices and brings them back up (performs a complete shutdown and reinitialization of the phones).
 - **Close**—Returns you to the previous window without restarting or resetting the chosen devices.
-

Additional Information

See the [“Related Topics” section on page 70-30](#).

Deleting a Phone

To delete a Cisco Unified IP Phone by using Cisco Unified CallManager Administration, perform the following procedure.

Before You Begin

Before deleting the phone, determine whether the directory number that is associated with the phone needs to be removed or deleted. To remove the directory number before deleting the phone, see the [“Removing a Directory Number from a Phone” section on page 49-4](#); otherwise, the directory number remains in the Cisco Unified CallManager database when the phone gets deleted. To delete a directory number from the database, see the [“Deleting Unassigned Directory Numbers” section on page 51-3](#).

You can view the directory numbers that are assigned to the phone from the Association Information area of the Phone Configuration window. You can also choose **Dependency Records** from the Related Links drop-down list box in the Phone Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#).

Procedure

- Step 1** Choose **Device > Phone**.
The Find and List Phones window displays.
- Step 2** To locate a specific phone, enter search criteria and click **Find**.
A list of phones that match the search criteria displays.

Step 3 Perform one of the following actions:

- Check the check boxes next to the phones that you want to delete and click **Delete Selected**.
- Delete all the phones in the window by clicking **Select All** and clicking **Delete Selected**.
- Choose the name of the phone that you want to delete from the list to display its current settings and click **Delete**.

A confirmation dialog displays.

Step 4 Click **OK**.

Additional Information

See the [“Related Topics” section on page 70-30](#).

Phone Configuration Settings

[Table 70-1](#) describes the available settings in the Phone Configuration window. For related procedures, see the [“Related Topics” section on page 70-30](#).



Note

The Product-Specific Configuration section contains model-specific fields that the phone manufacturer defines. Cisco Unified CallManager dynamically populates the fields with default values.

To view field descriptions and help for product-specific configuration items, click the “?” question icon in the Product Specific Configuration area to display help in a popup window.

If you need more information, refer to the documentation for the specific phone that you are configuring or contact the manufacturer.

Table 70-1 Phone Configuration Settings

Field	Description
Device Information	
MAC Address	Enter the Media Access Control (MAC) address that identifies Cisco Unified IP Phones (hardware phones only). Make sure that the value comprises 12 hexadecimal characters. For information on how to access the MAC address for your phone, refer to the <i>Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager</i> that supports your phone model. Cisco VG248 Analog Phone Gateway The MAC address for the Cisco VG248 gateway specifies the endpoint from the Gateway Configuration window of Cisco Unified CallManager Administration. See the “Gateway Configuration” section on page 69-1 for configuration information. Only one MAC address exists for the Cisco VG248 Analog Phone Gateway. All 48 ports share the same MAC address. Cisco Unified CallManager requires unique MAC addresses for all devices. Cisco Unified CallManager converts the MAC address for each device by • Dropping the first two digits of the MAC address • Shifting the MAC address two places to the left • Adding the two-digit port number to the end of the MAC address (to the right of the number) EXAMPLE MAC Address for the Cisco VG248 is 000039A44218 the MAC address for registered port 12 in the Cisco Unified CallManager is 0039A4421812
Device Name	Enter a name to identify software-based telephones, H.323 clients, and CTI ports. The value can include 1 to 15 characters, including alphanumeric characters, dot, dash, and underscores.
Description	Identify the purpose of the device. You can enter the user name (such as John Smith) or the phone location (such as Lobby) in this field. For Cisco VG248 gateways, begin the description with VGC<mac address>.
Device Pool	Choose the device pool to which you want this phone assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, softkey template, and MLPP information.

Table 70-1 Phone Configuration Settings (continued)

Field	Description
Phone Button Template	Choose the appropriate phone button template. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button. Cisco Unified CallManager does not make this field available for H.323 clients or CTI ports.
Softkey Template	Choose the appropriate softkey template. The softkey template determines the configuration of the softkeys on Cisco Unified IP Phones. Leave this field blank if the device pool contains the assigned softkey template.
Common Phone Profile	From the drop-down list box, choose a common phone profile from the list of available common phone profiles.
Calling Search Space	From the drop-down list box, choose the appropriate calling search space (CSS). A calling search space comprises a collection of partitions that are searched to determine how a dialed number should be routed. The calling search space for the device and the calling search space for the directory number get used together. The directory number CSS takes precedence over the device CSS. For more information, refer to Partitions and Calling Search Spaces in the <i>Cisco Unified CallManager System Guide</i>. For configuration information about calling search space for phones, see the “Calling Search Space” section on page 49-23.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth. For configuration information about calling search space for phones, see the “Calling Search Space” section on page 49-23.
Media Resource Group List	Choose the appropriate Media Resource Group List. A Media Resource Group List comprises a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from the available media resources according to the priority order that is defined in a Media Resource Group List. If you choose <None>, Cisco Unified CallManager uses the Media Resource Group List that is defined in the device pool. For more information, see the “Media Resource Management” section in the <i>Cisco Unified CallManager System Guide</i>.

Table 70-1 Phone Configuration Settings (continued)

Field	Description
User Hold Audio Source	To specify the audio source that plays when a user initiates a hold action, click the drop-down arrow and choose an audio source from the list that displays. If you do not choose an audio source, Cisco Unified CallManager uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID. Note You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose Media Resources > Music On Hold Audio Source.
Network Hold Audio Source	To specify the audio source that is played when the network initiates a hold action, click the drop-down arrow and choose an audio source from the list that displays. If you do not choose an audio source, Cisco Unified CallManager uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID. Note You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose Media Resources > Music On Hold Audio Source.
Location	Choose the appropriate location for this Cisco Unified IP Phone. The location specifies the total bandwidth that is available for calls to and from this location. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this Cisco Unified IP Phone consumes.
User Locale	From the drop-down list box, choose the locale that is associated with the phone user interface. The user locale identifies a set of detailed information to support users, including language and font. Cisco Unified CallManager makes this field available only for phone models that support localization. Note If no user locale is specified, Cisco Unified CallManager uses the user locale that is associated with the device pool. Note If the users require that information be displayed (on the phone) in any language other than English, verify that the locale installer is installed before configuring user locale. Refer to the Cisco Unified CallManager Locale Installer documentation.

Table 70-1 Phone Configuration Settings (continued)

Field	Description
Network Locale	From the drop-down list box, choose the locale that is associated with the phone. The network locale contains a definition of the tones and cadences that the phone in a specific geographic area uses. Cisco Unified CallManager makes this field available only for phone models that support localization. Note If no network locale is specified, Cisco Unified CallManager uses the network locale that is associated with the device pool. Note If users require that country-specific tones to be played (on the phone), verify that the locale is installed before configuring the network locale. Refer to the Cisco Unified CallManager Locale Installer documentation.
Built In Bridge	Enable or disable the built-in conference bridge for the barge feature by using the Built In Bridge drop-down list box (choose <i>On</i>, <i>Off</i>, or <i>Default</i>).  Note Cisco Unified IP Phone models 7940 and 7960 cannot support two media stream encryptions or SRTP streams simultaneously. To prevent instability due to this condition, the system automatically disables the built-in bridge for models 7940 and 7960 when the device security mode is set to encrypted. For more configuration information, refer to Barge and Privacy in the <i>Cisco Unified CallManager Features and Services Guide</i>. You can also refer to the <i>Cisco Unified CallManager Security Guide</i> for more information.
Privacy	For each phone that wants Privacy, choose <i>On</i> in the Privacy drop-down list box. For more configuration information, refer to Barge and Privacy in the <i>Cisco Unified CallManager Features and Services Guide</i>.
Signaling Port	This field applies only to H.323 devices. The value designates the H.225 signaling port that this device uses. Default value specifies 1720. Valid values range from 1 to 65535.
Video Capabilities Enabled/disabled	This check box turns video capabilities on and off.
Owner User ID	From the drop-down list box, choose the user ID of the person to whom this phone is assigned. The user ID gets recorded in the call detail record (CDR) for calls that are made from this device. Note Do not configure this field if you are using extension mobility. Extension mobility does not support device owners.

Table 70-1 Phone Configuration Settings (continued)

Field	Description
Wait for Far End H.245 Terminal Capability Set	This field applies only to H.323 devices. This check box specifies that Cisco Unified CallManager waits to receive the far-end H.245 Terminal Capability Set before it sends its H.245 Terminal Capability Set. By default, the system checks this check box. To specify that Cisco Unified CallManager should initiate capabilities exchange, uncheck this check box.
Phone Load Name	Enter the custom software for the Cisco Unified IP Phone. The value that you enter overrides the default value for the current model. For more information, see the “Device Defaults Configuration” section on page 72-1. For more information about Cisco Unified IP Phone software and configuration, refer to the <i>Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager 5.0</i>, which is specific to the phone model.
Retry Video Call as Audio	This check box applies only to video endpoints that receive a call. If this phone receives a call that does not connect as video, the call tries to connect as an audio call. By default, the system checks this check box to specify that this device should immediately retry a video call as an audio call (if it cannot connect as a video call) prior to sending the call to call control for rerouting. If you uncheck this check box, a video call that fails to connect as video does not try to establish as an audio call. The call then fails to call control, and call control routes the call via Automatic Alternate Routing (AAR) and/or route/hunt list.
Ignore Presentation Indicators (internal calls only)	Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Cisco Unified CallManager ignores any presentation restriction that is received for internal calls. Use this configuration in combination with the calling line ID presentation and connected line ID presentation configuration at the translation pattern level. Together, these settings allow you to configure call display restrictions to selectively present or block calling and/or connected line display information for each call. See Table 46-1 in the “Translation Pattern Configuration Settings” section on page 46-4 for more information about the calling line ID presentation and the connected line ID presentation parameters. For more information about call display restrictions, refer to the “Call Display Restrictions” chapter in the <i>Cisco Unified CallManager Features and Services Guide</i>.

Table 70-1 Phone Configuration Settings (continued)

Field	Description
Allow Control of Device from CTI	Check this check box to allow CTI to control and monitor this device. If the associated directory number specifies a shared line, the check box should be enabled as long as at least one associated device specifies a combination of device type and protocol that CTI supports.
Protocol Specific Information	
Packet Capture Mode	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. Choose one of the following options from the drop-down list box: • None—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting. • Batch Processing Mode—Cisco Unified CallManager writes the decrypted or nonencrypted messages to file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Cisco Unified CallManager, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified CallManager stores the file in /var/pktCap. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file. Tip For more information on packet capturing, refer to the <i>Cisco Unified CallManager Security Guide</i>.
Packet Capture Duration	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes that is allotted for one session of packet capturing. The default setting equals 0, although the range exists from 0 to 300 minutes. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays. Tip For more information on packet capturing, refer to the <i>Cisco Unified CallManager Security Guide</i>.
SRTP Allowed	As this check box explains, if this flag is checked, IPSec needs to be configured in the network to provide end-to-end security. Failure to do so will expose keys and other information.

Table 70-1 Phone Configuration Settings (continued)

Field	Description
Presence Group	Configure this field with the Presence feature. From the drop-down list box, choose a Presence group for the end user. The selected group specifies the devices, end users, and application users that can monitor this directory number. The default value for Presence Group specifies Standard Presence group, configured with installation. Presence groups that are configured in Cisco Unified CallManager Administration also appear in the drop-down list box. Presence authorization works with presence groups to allow or block presence requests between groups. Refer to the “Presence” chapter in the <i>Cisco Unified CallManager Features and Services Guide</i> for information about configuring permissions between groups and how presence works with extension mobility.
SCCP Phone Security Profile	For SCCP phones, choose the security profile that you want to apply to the device. If the phone does not support the profile that you choose, Cisco Unified CallManager does not allow you to apply the configuration. All phones require that you apply a security profile. If the phone does not support security, choose a nonsecure profile. To identify the settings that are contained in the profile, choose System > Security Profile > SCCP Phone Security Profile. Tip The CAPF settings that are configured in the profile relate to the Certificate Authority Proxy Function settings that display in the Phone Configuration window. If you want to manage manufacture-installed certificates (MICs) or locally significant certificates (LSC), you must configure the CAPF settings in the profile and in the Phone Configuration window.
SIP Dial Rules	If required, choose the appropriate SIP dial rule. SIP dial rules provide local dial plans for Cisco SIP IP Phones model 7905, 7912, 7940, and 7960, so users do not have to press a key or wait for a timer before the call gets processed. Leave the SIP Dial Rules field set to <None> if you do not want dial rules applied to the SIP IP Phone. This means the user will have to use the Dial softkey or wait for the timer to expire before the call gets processed.
MTP Preferred Originating Codec	From the drop-down list box, choose the codec to use if a media termination point is required for SIP calls.

Table 70-1 Phone Configuration Settings (continued)

Field	Description
SIP Phone Security Profile	For SIP phones, choose the security profile that you want to apply to the device. If the phone does not support the profile that you choose, Cisco Unified CallManager does not allow you to apply the configuration. All phones require that you apply a security profile. If the phone does not support security, choose a nonsecure profile. To identify the settings that are contained in the profile, choose System > Security Profile > SIP Phone Security Profile. The CAPF settings that are configured in the profile relate to the Certificate Authority Proxy Function settings that display in the Phone Configuration window. If you want to manage manufacture-installed certificates (MICs) or locally significant certificates (LSC), you must configure the CAPF settings in the profile and in the Phone Configuration window.
Rerouting Calling Search Space	From the drop-down list box, choose a calling search space to use for rerouting. The rerouting calling search space of the referrer gets used to find the route to the refer-to target. When the Refer fails due to the rerouting calling search space, the Refer Primitive rejects the request with the “405 Method Not Allowed” message. The redirection (3xx) primitive and transfer feature also uses the rerouting calling search space to find the redirect-to or transfer-to target.
Out-of-Dialog Refer Calling Search Space	From the drop-down list box, choose an out-of-dialog refer calling search space. Cisco Unified CallManager uses the out-of-dialog (OOD) Refer Authorization calling search space (CSS) to authorize the SIP out-of-dialog Refer. The administrator can restrict the use of out-of-dialog Refer by configuring the OOD CSS of the Referrer. Refer Primitive rejects the OOD Refer request with a “403 Forbidden” message.

Table 70-1 Phone Configuration Settings (continued)

Field	Description
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Cisco Unified CallManager routes presence requests that come from the phone. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the phone. From the drop-down list box, choose the SUBSCRIBE calling search space to use for presence requests for the phone. All calling search spaces that you configure in Cisco Unified CallManager Administration display in the SUBSCRIBE Calling Search Space drop-down list box. If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces. For information on how to configure a calling search space, see the “Calling Search Space Configuration” section on page 43-1
SIP Profile	Choose the default SIP profile or a specific profile that was previously created. SIP profiles provide specific SIP information for the phone such as registration and keepalive timers, media ports, and do not disturb control.
Digest User	Used with digest authentication (SIP security), choose an end user that you want to associate with the phone. Ensure that you configured digest credentials for the user that you choose, as specified in the End User Configuration window. After you save the phone configuration and reset the phone, the digest credentials for the user get added to the phone configuration file. Tip For more information on digest authentication, refer to the <i>Cisco Unified CallManager Security Guide</i>.
Media Termination Point Required	Indicate whether a media termination point is used to implement features that H.323 does not support (such as hold and transfer). Check the Media Termination Point Required check box if you want to use an MTP to implement features. Uncheck the Media Termination Point Required check box if you do not want to use an MTP to implement features. Use this check box only for H.323 clients and those H.323 devices that do not support the H.245 empty capabilities set or if you want media streaming to terminate through a single source. If you check this box to require an MTP and this device becomes the endpoint of a video call, the call will be audio only.

Table 70-1 Phone Configuration Settings (continued)

Field	Description
Unattended Port	Check this check box to indicate an unattended port on this device.
Require DTMF Reception	For SIP and SCCP phones, check this check box to require DTMF reception for this phone.
RFC2833 Disabled	For SCCP phones, check this check box to disable RFC2833 support.
Expansion Module Information	
Module 1	Choose the appropriate expansion module or none.
Module 1 Load Name	Enter the custom software for the appropriate expansion module, if applicable. The value that you enter overrides the default value for the current model. Ensure the firmware load matches the module load.
Module 2	Choose the appropriate expansion module or none.
Module 2 Load Name	Enter the custom software for the second expansion module, if applicable. The value that you enter overrides the default value for the current model. Ensure the firmware load matches the module load.
External Data Locations Information (Leave blank to use default)	
Information	Enter the location (URL) of the help text for the information (i) button. Leave this field blank to accept the default setting.
Directory	Enter the server from which the phone obtains directory information. Leave this field blank to accept the default setting.
Messages	Leave this field blank (not used by Cisco Unified CallManager).
Services	Enter the location (URL) for Cisco Unified IP Phone Services.
Authentication Server	Enter the URL that the phone uses to validate requests that are made to the phone web server. If you do not provide an authentication URL, the advanced features on the Cisco Unified IP Phone that require authentication will not function. By default, this URL accesses a Cisco Unified IP Phone User Options window that was configured during installation. Leave this field blank to accept the default setting.

Table 70-1 Phone Configuration Settings (continued)

Field	Description
Proxy Server	Enter the host and port (for example, proxy.cisco.com:80) that are used to proxy HTTP requests for access to non-local host addresses from the phone HTTP client. If the phone receives a URL such as www.cisco.com in a service and the phone is not configured in the cisco.com domain, the phone uses the proxy server to access the URL. If the phone is configured in cisco.com domain, the phone accesses the URL without using the proxy because the phone is in the same domain as the URL. If you do not configure this URL, the phone attempts to connect directly to the URL. Leave this field blank to accept the default setting.
Idle	Enter the URL that displays on the Cisco Unified IP Phone display when the phone has not been used for the time that is specified in Idle Timer field. For example, you can display a logo on the LCD when the phone has not been used for 5 minutes. Leave this field blank to accept the default setting.
Idle Timer (seconds)	Enter the time (in seconds) that you want to elapse before the URL that is specified in the Idle field displays. Leave this field blank to accept the value of the Idle URL Timer enterprise parameter.
Extension Information	
Enable Extension Mobility	Check this check box if this phone supports extension mobility.
Log Out Profile	This field specifies the device profile that the device uses when no one is logged into the device by using Cisco Extension Mobility. Choose an option from the drop-down list box. Options include Use Current Device Settings and Select a User Device Profile. When you choose Select a User Device Profile, a configuration window displays for you to choose the user device profile that was already configured.
Log In User ID	This field remains blank until a user logs in. When a user logs in to the device by using Cisco Extension Mobility, the userid displays in this field.
Log In Time	This field remains blank until a user logs in. When a user logs in to the device by using Cisco Extension Mobility, the time at which the user logged in displays in this field.
Log Out Time	This field remains blank until a user logs in. When a user logs in to the device by using Cisco Extension Mobility, the time at which the system will log out the user displays in this field.

Table 70-1 Phone Configuration Settings (continued)

Field	Description
Symmetric Key Information	
Symmetric Key	Enter a string of hexadecimal characters that you want to use for the symmetric key. Valid characters include numerals, 0-9, and upper/lower case characters, A-F (or a-f). Make sure that you enter the correct bits for the key size; otherwise, Cisco Unified CallManager rejects the value. Cisco Unified CallManager supports the following key sizes: • Cisco Unified IP Phone models 7905 and 7912 (SIP Protocol only)—256 bits • Cisco Unified IP Phone models 7940 and 7960 (SIP Protocol only)—128 bits This string is for one-time use only. Every time that you update the configuration settings, you must generate a new key before you reset the phone.
Generate String	If you want Cisco Unified CallManager Administration to generate a hexadecimal string for you, click the Generate String button.
Revert to Database Value	If you want to restore the value that exists in the database, click this button. This button proves useful if you enter an error in the Symmetric Key field before you save the configuration.
Certification Authority Proxy Function (CAPF) Information	
Certificate Operation	From the drop-down list box, choose one of the following options: • No Pending Operation—Displays when no certificate operation is occurring (default setting). • Install/Upgrade—Installs a new or upgrades an existing locally significant certificate in the phone. • Delete—Deletes the locally significant certificate that exists in the phone. • Troubleshoot—Retrieves the locally significant certificate (LSC) or the manufacture installed certificate (MIC), so you can view the certificate credentials in the CAPF trace file. If both certificate types exist in the phone, Cisco Unified CallManager creates two trace files, one for each certificate type. By choosing the Troubleshooting option, you can verify that an LSC or MIC exists in the phone.

Table 70-1 Phone Configuration Settings (continued)

Field	Description
Authentication String	If you chose the By Authentication String option in the Authentication Mode drop-down list box, this field applies. Manually enter a string or generate a string by clicking the Generate String button. Ensure that the string contains 4 to 10 digits. To install, upgrade, delete, or troubleshoot a locally significant certificate, the phone user or administrator must enter the authentication string on the phone.
Operation Completes by	This field, which supports the Install/Upgrade, Delete, and Troubleshoot Certificate Operation options, specifies the date and time in which you must complete the operation. The values that display are for the publisher database server.
Certificate Operation Status	This field displays the progress of the certificate operation; for example, <operation type> pending, failed, or successful, where operating type equals the Install/Upgrade, Delete, or Troubleshoot Certificate Operation options. You cannot change the information that displays in this field.
H.323 Information	
Outgoing Caller ID Pattern	For incoming calls to the phone, enter the pattern, from 0 to 24 digits, that you want to use for caller ID.
Calling Party Selection	Choose the directory number that is sent on an outbound call on a gateway. The following options specify which directory number is sent: • Originator—Send the directory number of the calling device. • First Redirect Number—Send the directory number of the redirecting device. • Last Redirect Number—Send the directory number of the last device to redirect the call. • First Redirect Number (External)—Send the external directory number of the redirecting device. • Last Redirect Number (External)—Send the external directory number of the last device to redirect the call.
Calling Party Presentation	Choose whether the Cisco Unified CallManager transmits or blocks caller ID. Choose <i>Allowed</i> if you want the Cisco Unified CallManager to send caller ID. Choose <i>Restricted</i> if you do not want the Cisco Unified CallManager to send caller ID.
Display IE Delivery	This check box enables delivery of the display information element (IE) in SETUP and CONNECT messages for the calling and called party name delivery service. The default setting checks this check box.

Table 70-1 Phone Configuration Settings (continued)

Field	Description
Redirecting Number IE Delivery Outbound	Check this check box to include the Redirecting Number IE in the outgoing SETUP message from the Cisco Unified CallManager to indicate the first redirecting number and the redirecting reason of the call when the call is forwarded. Uncheck the check box to exclude the first redirecting number and the redirecting reason from the outgoing SETUP message. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box. Note The default setting leaves this check box unchecked.
Redirecting Number IE Delivery Inbound	Check this check box to accept the Redirecting Number IE in the incoming SETUP message to the Cisco Unified CallManager. Uncheck the check box to exclude the Redirecting Number IE in the incoming SETUP message to the Cisco Unified CallManager. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box. Note Default leaves the check box unchecked.
Gatekeeper Information	
Gatekeeper Name	This field specifies the name of the gatekeeper that controls the H.323 client. Ensure the gatekeeper is configured in Cisco Unified CallManager before an H.323 client is allowed to specify the gatekeeper in its configuration. Default specifies empty.
E.164	Always use a unique E.164 number. Do not use null value.
Technology Prefix	This field specifies a number ending with the # sign that describes the capability of an endpoint in a zone. This field has no impact if via Zone configuration can be used. Default specifies 1#*. Do not use null value.
Zone	This field specifies the zone name of the zone that the gatekeeper manages. Do not use the following values: same zone name for the H.323 client and trunk; null.
Gatekeeper Controlled H.323 Client	This check box enables the gatekeeper control of the H.323 client.
Multilevel Precedence and Preemption (MLPP) Information	
MLPP Domain	Choose an MLPP domain from the drop-down list box for the MLPP domain that is associated with this device. If you leave the <i>None</i> value, this device inherits its MLPP domain from the value that was set for the device's device pool. If the device pool does not have an MLPP domain setting, this device inherits its MLPP domain from the value that was set for the MLPP Domain Identifier enterprise parameter.

Table 70-1 Phone Configuration Settings (continued)

Field	Description
MLPP Indication	If available, this setting specifies whether a device that can play precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options: • Default—This device inherits its MLPP indication setting from its device pool. • Off—This device does not handle nor process indication of an MLPP precedence call. • On—This device does handle and process indication of an MLPP precedence call. Note Do not configure a device with the following combination of settings: MLPP Indication is set to <i>Off</i> or <i>Default</i> (when default is <i>Off</i>) while MLPP Preemption is set to <i>Forceful</i>. Note Turning on MLPP Indication (at the enterprise parameter, device pool, or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device.
MLPP Preemption	If available, this setting specifies whether a device that can preempt calls in progress will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options: • Default—This device inherits its MLPP preemption setting from its device pool. • Off—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. • On—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. Note Do not configure a device with the following combination of settings: MLPP Indication is set to <i>Off</i> or <i>Default</i> (when default is <i>Off</i>) while MLPP Preemption is set to <i>Forceful</i>.
Secure Shell Information	
Secure Shell User	Enter a user ID for the secure shell user. Cisco Technical Assistance Center (TAC) uses secure shell for troubleshooting and debugging. Contact TAC for further assistance.
Secure Shell Password	Enter the password for a secure shell user. Contact TAC for further assistance.

Table 70-1 Phone Configuration Settings (continued)

Field	Description
Association Information	
Modify Button Items	After you add a phone, the Association Information area displays on the left side of the Phone Configuration window. Click this button to manage button associations for this phone. A dialog box warns that any unsaved changes to the phone may be lost. If you have saved any changes that you made to the phone, click OK to continue. The Reorder Phone Button Configuration window displays for this phone. See the “Modifying Phone Button Template Button Items” section on page 70-28 for a detailed procedure.
Line [1] - Add a new DN Line [2] - Add a new DN	After you add a phone, the Association Information area displays on the left side of the Phone Configuration window. Click these links to add a directory number(s) that associates with this phone. When you click one of the links, the Directory Number Configuration window displays. See the “Configuring a Directory Number” section on page 49-2 for a detailed procedure.
Add a new SD	After you add a phone, the Association Information area displays on the left side of the Phone Configuration window. Click this link to add speed-dial settings for this phone. When you click the link, the Speed Dial and Abbreviated Dial Configuration window displays for this phone. See the “Configuring Speed-Dial Buttons” section on page 70-23 for a detailed procedure.
Add a new SURL	After you add a phone, the Association Information area displays on the left side of the Phone Configuration window. Click this link to configure service URL buttons for this phone. When you click the link, the Configure Service URL Buttons window displays for this phone. See the “Configuring Service URL Buttons” section on page 70-27 for a detailed procedure.
Add a new BLF SD	After you add a phone, the Association Information area displays on the left side of the Phone Configuration window. Click this link to configure busy lamp field/speed dial settings for this phone. When you click the link, the Busy Lamp Field Configuration window displays for this phone. See the “BLF/SpeedDial Configuration Settings” section on page 70-24 for more information.

Table 70-1 Phone Configuration Settings (continued)

Field	Description
Product-Specific Configuration	
Model-specific configuration fields that the device manufacturer defines	To view field descriptions and help for product-specific configuration items, click the “?” information icon in the Product Specific Configuration area to display help in a popup dialog box. If you need more information, refer to the documentation for the specific device that you are configuring or contact the manufacturer.

Configuring Speed-Dial Buttons

You use Cisco Unified CallManager Administration to configure speed-dial buttons for phones if you want to provide speed-dial buttons for users or if you are configuring phones that do not have a specific user who is assigned to them. Users use the Cisco Unified IP Phone User Options Menu to change the speed-dial buttons on their phones.

Procedure

- Step 1** From the Phone Configuration window, choose **Add/Update Speed Dials** from the Related Links drop-down list box at the top of the window and click **Go**.

The Speed Dial and Abbreviated Dial Configuration window displays for this phone.



- Note** To display the Phone Configuration window, choose **Device > Phone**. Enter your search criteria and click **Find**. Choose the phone for which you want to configure speed-dial buttons.

- Step 2** Enter the appropriate settings as described in [Table 70-2](#).
- Step 3** To apply the changes, click **Save**.
- Step 4** To close the window, click **Close**.

Additional Information

See the [“Related Topics”](#) section on page 70-30.

Speed-Dial and Abbreviated-Dial Configuration Settings

[Table 70-2](#) describes the speed-dial button configuration settings. The Speed Dial and Abbreviated Dial Configuration window has two sections: speed-dial settings on the phone and abbreviated-dial settings that are not associated with a button. The descriptions in [Table 70-2](#) apply to both sections.

The system provides a total of 99 speed-dial and abbreviated-dial settings.

Speed Dial Settings

Configure these settings for the physical buttons on the phone.

Abbreviated Dial Settings

Configure these settings for the speed-dial numbers that you access with abbreviated dialing.

**Note**

Not all Cisco Unified IP Phones support abbreviated dialing. Refer to the phone user guide for information.

Table 70-2 **Speed-Dial and Abbreviated-Dial Configuration Settings**

Field	Description
(number from 1 to 99 in the left column)	This column identifies the speed-dial button on the phone or on the Cisco Unified IP Phone model 7914 Expansion Module (for example, 1, 2, 3, or 4), or the abbreviated-dial index for abbreviated dial.
Number	Enter the number that you want the system to dial when the user presses the speed-dial button.
Label	Enter the text that you want to display for the speed-dial button or abbreviated-dial number. Cisco Unified CallManager does not make this field available for the Cisco Unified IP Phone model 7910.
ASCII Label	This field provides the same information as the <i>Label</i> field, but you must limit input to ASCII characters. Devices that do not support Unicode (internationalized) characters display the content of the <i>ASCII Label</i> field.

Additional Information

See the [“Related Topics”](#) section on page 70-30.

BLF/SpeedDial Configuration Settings

When you configure Presence in Cisco Unified CallManager Administration, an interested party, known as a watcher, can monitor the real-time status of a directory number or SIP URI with a BLF/SpeedDial button on the device of the watcher.

For Presence-supported SIP phones, you can configure directory numbers or SIP URIs as BLF/SpeedDial buttons. For Presence-supported SCCP phones, you can only configure directory numbers as BLF/SpeedDial buttons.

For information on configuring BLF/SpeedDial buttons, refer to the [“Presence”](#) chapter in the *Cisco Unified CallManager Features and Services Guide*.

Configuring Cisco Unified IP Phone Services

From certain phones, such as Cisco Unified IP Phone model 7970, 7960, and 7940, users can access information services, such as weather, stock quotes, or other services that are available to them. Using Cisco Unified CallManager Administration, you can set up the available services for phones. Users use the Cisco Unified IP Phone User Options Menu to modify the services. For information about the Cisco Unified IP Phone User Options Menu, refer to the *Cisco Unified IP Phone User Guide* that is

specific to your phone model. For more information on maintaining services in Cisco Unified CallManager Administration, see the [“Cisco Unified IP Phone Services Configuration” section on page 78-1](#).

See the following sections for details of subscribing to a phone service, updating a phone service, and unsubscribing from a phone service:

- [Subscribing to a Service, page 70-25](#)
- [Updating Services, page 70-26](#)
- [Unsubscribing from a Service, page 70-26](#)

Subscribing to a Service

To subscribe to new services for a phone, perform the following steps.

Before You Begin

Add the phone services to Cisco Unified CallManager. For more information, see the [“Configuring a Cisco Unified IP Phone Service” section on page 78-3](#).

Procedure

-
Step 1	Choose Device > Phone . The Find and List Phones window displays.
Step 2	To locate a specific phone, enter search criteria and click Find . A list of phones that match the search criteria displays.
Step 3	Choose the phone to which you want to add a service. The Phone Configuration window displays.
Step 4	On the upper, right side of the window, choose Subscribe/Unsubscribe Services from the Related Links drop-down list box and click Go . The Subscribed Cisco Unified IP Phone Services window displays for this phone.
Step 5	From the Select a Service drop-down list box, choose the service that you want to add to the phone.
Step 6	Click Next . The window displays with the service that you chose. If you want to choose a different service, click Back and repeat Step 5 .
Step 7	If the service has required parameters, enter that information into the field that is provided.
Step 8	Click Subscribe . The service displays in the Subscribed Services list.
Step 9	If you want to subscribe to additional services, click the Subscribe a New Service link in the Subscribed Services area. Repeat Step 5 through Step 8 .
-

Additional Information

See the [“Related Topics” section on page 70-30](#).

Updating Services

Perform the following steps to update a service. You can update the service name and service parameter values, if necessary.

Procedure

- Step 1** Choose **Device > Phone**.
The Find and List Phones window displays.
- Step 2** To locate a specific phone, enter search criteria and click **Find**.
A list of phones that match the search criteria displays.
- Step 3** Choose the phone for which you want to update a service.
The Phone Configuration window displays.
- Step 4** On the upper, right side of the window, choose **Subscribe/Unsubscribe Services** from the Related Links drop-down list box and click **Go**.
- Step 5** From the Subscribed Services list, choose a service.
- Step 6** Update the appropriate parameter and click **Save**.
-

Additional Information

See the [“Related Topics” section on page 70-30](#).

Unsubscribing from a Service

To unsubscribe from a service, perform the following steps.

Procedure

- Step 1** Choose **Device > Phone**.
The Find and List Phones window displays.
- Step 2** Enter search criteria to locate a specific phone and click **Find**.
A list of phones that match the search criteria displays.
- Step 3** Choose the phone from which you want to delete a service.
The Phone Configuration window displays.
- Step 4** On the upper, right side of the window, choose **Subscribe/Unsubscribe Services** from the Related Links drop-down list box and click **Go**.
- Step 5** From the Subscribed Services list, choose a service.
- Step 6** Click **Unsubscribe**.
A warning message verifies that you want to unsubscribe from the service.
- Step 7** To unsubscribe, click **OK** or click **Cancel** to restore your previous settings.
-

Additional Information

See the [“Related Topics”](#) section on page 70-30.

Configuring Service URL Buttons

From a Cisco Unified IP Phone model 7970, 7960, and 7940, users can access information services, such as weather, stock quotes, or other services that are available to them. Using Cisco Unified CallManager Administration, you can configure services to be available on a phone button and then configure that button for the phone. Users use the Cisco Unified IP Phone User Options Menu to modify the services. For information about the Cisco Unified IP Phone User Options Menu, refer to the *Cisco Unified IP Phone User Guide* that is specific for your phone model. For more information on maintaining services in Cisco Unified CallManager Administration, see the [“Cisco Unified IP Phone Services Configuration”](#) section on page 78-1.

Adding a Service URL Button

To configure the service URL buttons for a phone, perform the following steps.

Before You Begin

Before you begin, perform the following configurations:

- Add the services to Cisco Unified CallManager. For more information, see the [“Configuring a Cisco Unified IP Phone Service”](#) section on page 78-3.
- Configure the service URL button on the phone button template. For more information, see the [“Configuring Phone Button Templates”](#) section on page 76-2.
- Subscribe to the service. See the [“Configuring Cisco Unified IP Phone Services”](#) section on page 70-24.

Procedure

-
Step 1	Choose Device > Phone . The Find and List Phones window displays.
Step 2	To locate a specific phone, enter search criteria and click Find . A list of phones that match the search criteria displays.
Step 3	Choose the phone to which you want to add a service URL button. The Phone Configuration window displays.
Step 4	In the Association Information area on the left side of the Phone Configuration window, click the Add a new SURL link. The Configure Service URL Buttons window displays for this phone.
Step 5	From the Button Service drop-down list box, choose the service that you want to add to or update for the phone.
Step 6	You can change the values in the Label and ASCII Label fields.
Step 7	To add the service to or update for the phone button, click Save .

- Step 8** If more buttons and services are available, you can assign additional services to additional buttons by repeating [Step 5](#) through [Step 7](#).
- Step 9** To close this window and return to the Phone Configuration window, click **Close**.

Additional Information

See the [“Related Topics”](#) section on page 70-30.

Modifying Phone Button Template Button Items

When you configure a phone and associate it with a custom, nonstandard phone button template, you can modify the phone button items in the associated phone button template. When you do so, you create a new phone button template that is customized for this particular phone. The new phone button template displays in the list of phone button templates with a name of the format “SEP999999999999-Individual Template,” where 999999999999 specifies the MAC address of the phone.



Note

You cannot perform this procedure if the phone is associated with a standard phone button template. You must first associate this phone with a custom, nonstandard phone template.

To modify the button items of a custom, nonstandard phone button template, perform the following steps.

Procedure

- Step 1** Choose **Device > Phone**.
- The Find and List Phones window displays.
- Step 2** To locate a specific phone, enter search criteria and click **Find**.
- A list of phones that match the search criteria displays.
- Step 3** Choose the phone for which you want to modify the phone button items.
- The Phone Configuration window displays.
- Step 4** Click **Modify Button Items** in the Association Information area on the left side of the window.
- A popup window warns you that unsaved changes (to the phone) may be lost. If you have made changes to the phone configuration, click **Cancel** and save those changes before proceeding.
- Step 5** To continue, click **OK**.
- The Reorder Phone Button Configuration window displays. This window comprises the following panes:
- **Associated Items**—This pane displays a list of the items that are assigned to the phone buttons in this phone button template. The system assigns the first item in the list to button 1, the second item to button 2, and so forth.
 - **Unassigned Associated Items**—This pane displays a list of the items that are not assigned to phone buttons in this phone button template.
 - **Dissociate These Items**—This pane displays a list of the items that cannot presently be assigned to a phone button.

- Step 6** To change the order of the associated items, select an item in the Associated Items pane and click the up or down arrows to change its order.
- Step 7** To move an item from the Associated Items pane to the Unassigned Associated Items pane or vice versa, select the item in either pane and click the left or right arrows to move the item to the other pane.
- Step 8** To move an item from the Associated Items or Unassigned Associated Items pane to the Dissociate These Items pane or vice versa, select the item in any pane and click the up or down arrows that are located between the two panes that you want to affect.
- Step 9** After you have finished moving items among the panes and all items are in the desired order, click **Save**.
- Step 10** To close the Reorder Phone Button Configuration window, click **Close**.

Additional Information

See the [“Related Topics”](#) section on page 70-30.

Finding a Phone

Because you might have thousands of Cisco Unified IP Phones in your network, Cisco Unified CallManager lets you search for phones on the basis of specified criteria. Follow these steps to search for a specific Cisco Unified IP Phone in the Cisco Unified CallManager database.



Note

The Cisco VG248 Gateway will not display when you search for phones. You can search for the Cisco VG248 Analog Phone ports from the Find and List Phones window of Cisco Unified CallManager Administration. See the [“Gateway Configuration”](#) section on page 69-1 for configuration information on the Cisco VG248 Gateway.



Tip

For methods to limit your search, refer to the [“Phone Search”](#) section in the *Cisco Unified CallManager System Guide*.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your phone search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your phone search preferences until you modify your search or close the browser.

Procedure

- Step 1** Choose **Device > Phone**.
The Find and List Phones window displays.
- Step 2** Choose the field that you want to specify to locate a phone.



Note

To find all phones that are registered in the database, choose Device Name from the list of fields and choose “is not empty” from the list of patterns; then, click **Find**.

- Step 3** Choose the appropriate search pattern for your text search; for example, Begins with.
- Step 4** In the Find field, enter your search text, if any.
- Step 5** To choose a wildcard search on the search string, leave the Allow wildcards check box checked; if you do not want a wildcard search, uncheck the check box. For more information about wildcard search, refer to the [“Phone Search”](#) section in the *Cisco Unified CallManager System Guide*.



Note Searching for directory numbers or patterns that contain special characters, with the Allow wildcards check box checked, may not return expected results.

- Step 6** Click **Find**.
- A list of devices that match the criteria displays. The field that you chose in [Step 2](#) determines how the devices in the list are sorted.

This window also lists the total number of devices in this window.



Tip To search for phones within the search results, click the **Search Within Results** check box and enter your search criteria as described in [Step 4](#).

- Step 7** To view the next set of discovered devices, click **Next**.



Note You can delete or reset multiple phones from the Find and List Phones window by checking the check boxes next to the appropriate phones and clicking **Delete Selected** to delete the phones or clicking **Reset Selected** to reset the phones. You can choose all the phones in the window by checking the check box in the matching records title bar.

Additional Information

See the [“Related Topics”](#) section on page 70-30.

Related Topics

- [Cisco Unified IP Phone Configuration, page 70-1](#)
- [Configuring Cisco Unified IP Phones, page 70-2](#)
- [Displaying the MAC Address of a Phone, page 70-4](#)
- [Resetting a Phone, page 70-4](#)
- [Deleting a Phone, page 70-5](#)
- [Phone Configuration Settings, page 70-6](#)
- [Configuring Speed-Dial Buttons, page 70-23](#)
- [Speed-Dial and Abbreviated-Dial Configuration Settings, page 70-23](#)
- [BLF/SpeedDial Configuration Settings, page 70-24](#)
- [Configuring Cisco Unified IP Phone Services, page 70-24](#)
- [Configuring Service URL Buttons, page 70-27](#)

- [Modifying Phone Button Template Button Items](#), page 70-28
- [Finding a Phone](#), page 70-29
- [Directory Number Configuration](#), page 49-1
- [Gateway Configuration](#), page 69-1
- [Phone Button Template Configuration](#), page 76-1
- [Cisco Unified IP Phone Services Configuration](#), page 78-1
- [Cisco Unified IP Phones](#), *Cisco Unified CallManager System Guide*
- [Phone Configuration Checklist](#), *Cisco Unified CallManager System Guide*
- [Phone Features](#), *Cisco Unified CallManager System Guide*
- [Understanding Directory Numbers](#), *Cisco Unified CallManager System Guide*
- [Presence](#), *Cisco Unified CallManager Features and Services Guide*



Trunk Configuration

Use a trunk device to configure a logical route to a gatekeeper (that is, the wholesale network or an intercluster trunk with gatekeeper control), to an intercluster trunk without a gatekeeper, or to a SIP network. Choose from the following available trunk types:

- H.225 trunk (gatekeeper controlled)
- Intercluster trunk (gatekeeper controlled)
- Intercluster trunk (non-gatekeeper controlled)
- SIP trunk

The following topics cover Cisco Unified CallManager trunk configuration:

- [Finding a Trunk, page 71-1](#)
- [Configuring a Trunk, page 71-2](#)
- [Trunk Configuration Settings, page 71-3](#)
- [Deleting a Trunk, page 71-27](#)
- [Resetting a Trunk, page 71-27](#)

The following topics contain additional information that is related to trunks:

- [Call Admission Control, Cisco Unified CallManager System Guide](#)
- [Gatekeepers and Trunks, Cisco Unified CallManager System Guide](#)
- [Gatekeeper and Trunk Configuration in Cisco Unified CallManager, Cisco Unified CallManager System Guide](#)
- [Cisco Unified Communications Solution Reference Network Design \(SRND\)](#)

Finding a Trunk

Because you might have multiple trunks in your network, Cisco Unified CallManager lets you search for trunks on the basis of specified criteria. Follow these steps to search for a specific trunk in the Cisco Unified CallManager database.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your trunk search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your trunk search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Device > Trunk**.

The Find and List Trunks window displays.

Step 2 Choose the field that you want to use to locate a trunk.



Note To find all trunks that are registered in the database, choose Device Name from the list of fields and choose “is not empty” from the list of patterns; then, click **Find**.

Step 3 Choose the appropriate search pattern for your text search. If you do not want to perform a text search, choose “is empty.”

Step 4 Enter your search text, if any, in the Find field.

Step 5 If you choose calling search space or device pool in [Step 2](#), the options available in the database display. From the drop-down list box below the **Find** button, you can choose one of these options.

Step 6 Click **Find**.

A list of devices that match the criteria displays. This window also lists the total number of devices.

Step 7 To view the next set of discovered devices, click **Next**.



Note You can delete or reset multiple trunks from the Find and List Trunks window by checking the check boxes next to the appropriate trunks and clicking **Delete Selected** to delete the trunks or clicking **Reset Selected** to reset the trunks. You can choose all of the trunks in the window by clicking **Select All**.

Additional Topics

See the [“Related Topics” section on page 71-28](#).

Configuring a Trunk

Perform the following procedure to add a new trunk device or update an existing trunk device.



Note You can configure multiple trunk devices per Cisco Unified CallManager cluster.

Before You Begin

Configure SIP Trunk Security Profiles and SIP Profiles before you configure a SIP Trunk. For more information, see the [“Configuring SIP Profiles” section on page 79-2](#), [SIP Trunk Security Profile Configuration](#), and the *Cisco Unified CallManager Security Guide*.

Procedure

Step 1 Choose **Device > Trunk**.

The Find and List Trunks window displays.

- Step 2** Perform one of the followings tasks:
- To add a new trunk device, click the **Add New** button. The Trunk Configuration window displays. Continue with [Step 3](#).
 - To update trunk settings, locate the appropriate trunk as described in “[Finding a Trunk](#)” section on [page 71-1](#). Click the name of the trunk that you want to update. Continue with [Step 6](#).
- Step 3** From the Trunk Type drop-down list, choose the type of trunk.
- Step 4** If applicable, from the Device Protocol drop-down list, choose the device protocol.
- Step 5** Click **Next**.
- Step 6** On the Trunk Configuration window that displays, enter the appropriate settings for gatekeeper-controlled H.225 trunks, gatekeeper-controlled intercluster trunks, and non-gatekeeper-controlled intercluster trunks as described in [Table 71-1](#). For SIP trunks, enter the appropriate settings as described in [Table 71-2](#).
- Step 7** To add the new trunk, click **Save**.
- The trunk gets added to the database.
- If you are updating an existing trunk, click **Reset Trunk** to reset or restart the trunk and apply the new settings.



Note Resetting a trunk **drops** any calls in progress that are using that trunk. Restarting a gateway tries to preserve the calls in progress that are using that gateway, if possible. Other devices wait until calls complete before restarting or resetting. Resetting/restarting an H.323 or SIP device does not physically reset/restart the hardware; it only reinitializes the configuration that is loaded by Cisco Unified CallManager

Additional Topics

See the “[Related Topics](#)” section on [page 71-28](#).

Trunk Configuration Settings

[Table 71-1](#) describes the trunk configuration settings for gatekeeper-controlled H.225 trunks, gatekeeper-controlled intercluster trunks, and non-gatekeeper-controlled intercluster trunks.

[Table 71-2](#) describes the trunk configuration settings for SIP trunks.

For more information about related procedures, see the “[Related Topics](#)” section on [page 71-28](#).

Table 71-1 *Trunk Configuration Settings for H.225 and Intercluster Trunks*

Field	Description
Device Information	
Device Name	Enter a unique identifier for the trunk.
Description	Enter a descriptive name for the trunk.

Table 71-1 **Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)**

Field	Description
Device Pool	Choose the appropriate device pool for the trunk. For trunks, device pools specify a list of Cisco Unified CallManagers that the trunk uses to distribute the call load dynamically. Note Calls that are initiated from a phone that is registered to a Cisco Unified CallManager that does not belong to the trunk's device pool use different Cisco Unified CallManagers of this device pool for different outgoing calls. Selection of nodes occurs in a random order. A call that is initiated from a phone that is registered to a Cisco Unified CallManager that does belong to the trunk's device pool uses the same Cisco Unified CallManager node for outgoing calls if the Cisco Unified CallManager is up and running.
Call Classification	This parameter determines whether an incoming call through this trunk is considered off the network (OffNet) or on the network (OnNet). When the Call Classification field is configured as Use System Default, the setting of the Cisco Unified CallManager clusterwide service parameter, Call Classification, determines whether the trunk is OnNet or OffNet. This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively. The alerting tones are provided by Cisco Unified CallManager Annunciators. Use this parameter in conjunction with the settings on the Route Pattern Configuration window to classify an outgoing call as OnNet or OffNet.
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that a Media Resource Group List defines.
Location	Choose the appropriate location for the trunk. The location specifies the total bandwidth that is available for calls between this location and the central location, or hub. A location setting of Hub_None specifies unlimited available bandwidth.
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.

Table 71-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

Field	Description
Tunneled Protocol	This drop-down list box displays for H.225 trunks, gatekeeper-controlled trunks, and non-gatekeeper-controlled trunks. Choose the QSIG option if you want to use trunks to transport (tunnel) non-H.323 protocol information in H.323 signaling messages from Cisco Unified CallManager to other Annex M.1-compliant H.323 PINXs. QSIG tunneling supports the following features: Call Completion, Call Diversion, Call Transfer, Identification Services, Message Waiting Indication, and.
Packet Capture Mode	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. Choose one of the following options from the drop-down list box: • None—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting. • Batch Processing Mode—Cisco Unified CallManager writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Cisco Unified CallManager, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified CallManager stores the file in /var/pktCap. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The IREC tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file.  Note You do not have to reset the trunk after enabling/disabling Packet Capturing. Tip For more information on capturing packets, refer to the <i>Cisco Unified CallManager Security Guide</i>.

Table 71-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

Field	Description
Packet Capture Duration	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes that is allotted for one session of packet capturing. The default setting equals 0, although the range exists from 0 to 300 minutes. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays. Tip For more information on capturing packets, refer to the <i>Cisco Unified CallManager Security Guide</i>.
Media Termination Point Required	This check box is used to indicate whether a media termination point (MTP) is used to implement features that H.323 does not support (such as hold and transfer). Check the Media Termination Point Required check box if you want to use a media termination point to implement features. Uncheck the Media Termination Point Required check box if you do not want to use a media termination point to implement features. Use this check box only for H.323 clients and those H.323 devices that do not support the H.245 Empty Capabilities Set or if you want media streaming to terminate through a single source. If you check this check box to require an MTP and one or both parties are a video endpoint, the call operates as audio only.
Retry Video Call as Audio	This check box applies only to video endpoints that receive a call. For trunks, this check box pertains to calls that are received from Cisco Unified CallManager but not to calls that are received from the wide-area network (WAN). By default, the system checks this check box to specify that this device should immediately retry a video call as an audio call (if it cannot connect as a video call) prior to sending the call to call control for rerouting. If you uncheck this check box, a video call that fails to connect as video does not try to establish as an audio call. The call then fails to call control, and call control routes the call via Automatic Alternate Routing (AAR) and/or route/hunt list.
Wait for Far-End H.245 Terminal Capability Set (H.225 trunks only)	This field applies only to H.323 devices. This check box specifies that Cisco Unified CallManager waits to receive the far-end H.245 Terminal Capability Set before it sends its H.245 Terminal Capability Set. By default, the system checks this check box. To specify that Cisco Unified CallManager should initiate capabilities exchange, uncheck this check box.

Table 71-1 **Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)**

Field	Description
Path Replacement Support	If you choose the QSIG option from the Tunneled Protocol drop-down list box, this check box displays for H.225 trunks, gatekeeper-controlled trunks, and non-gatekeeper-controlled trunks. This setting works with QSIG tunneling (Annex M.1) to ensure that non-H.323 information gets sent on the leg of the call that uses path replacement. Note The default setting leaves the check box unchecked. When you choose the QSIG Tunneled Protocol option, the system automatically checks the check box.
Transmit UTF-8 for Calling Party Name	This device uses the user locale setting of the SIP trunks to determine whether to send Unicode and whether to translate received Unicode information. For the sending device, if you check this check box and the user locale setting in the device's device pool matches the terminating phone's user locale, the device sends Unicode. If the user locale settings do not match, the device sends ASCII. The receiving device translates incoming Unicode characters based on the user locale setting of the sending device's device pool. If the user locale setting matches the terminating phone's user locale, the phone displays the characters. Note The phone may display garbled characters if the two ends of the trunk configure user locales that do not belong to the same language group.
Unattended Port	Check this check box if calls can be redirected, transferred and forwarded to an unattended port, such as a voice mail port. The default value for this check box is unchecked.
SRTP Allowed	Check the SRTP Allowed check box if you want Cisco Unified CallManager to allow secure and nonsecure calls over the trunk. If you do not check this check box, Cisco Unified CallManager prevents SRTP negotiation with the trunk and uses RTP.  Caution If you check this check box, Cisco strongly recommends that you configure IPsec, so you do not expose keys and other security-related information during call negotiations. If you do not configure IPsec correctly, signaling between Cisco Unified CallManager and the gateway is nonsecure. For more information on encryption for trunks, refer to the <i>Cisco Unified CallManager Security Guide</i>.

Table 71-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

Field	Description
Multilevel Precedence and Preemption (MLPP) Information	
MLPP Domain	From the drop-down list box, choose an MLPP domain to associate with this device. If you leave this field blank, this device inherits its MLPP domain from the value that was set for the device's device pool. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value that was set for the MLPP Domain Identifier enterprise parameter.
MLPP Indication	If available, this setting specifies whether a device that is capable of playing precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options: • Default-This device inherits its MLPP indication setting from its device pool. • Off-This device does not handle nor process indication of an MLPP precedence call. • On-This device does handle and process indication of an MLPP precedence call. Note Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.
Call Routing Information	
Inbound Calls	
Significant Digits	Significant digits represent the number of final digits that are retained on inbound calls. Use for the processing of incoming calls and to indicate the number of digits that are used to route calls that are coming in to the H.323 device. Choose the number of significant digits to collect, from 0 to 32. Cisco Unified CallManager counts significant digits from the right (last digit) of the number that is called.

Table 71-1 **Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)**

Field	Description
Calling Search Space	From the drop-down list box, choose the appropriate calling search space for the trunk. The calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the number that are configured in the Max List Box Items enterprise parameter, the ellipsis button (...) displays next to the drop-down list box. Click the “...” button to display the Select Calling Search Space window. Enter a partial calling search space name in the List items where Name contains field. Click the desired calling search space name in the list of calling search spaces that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when performing automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.
Prefix DN	Enter the prefix digits that are appended to the called party number on incoming calls. Cisco Unified CallManager adds prefix digits after first truncating the number in accordance with the Significant Digits setting.
Redirecting Diversion Header Delivery - Inbound	Check this check box to accept the Redirecting Number IE in the incoming SETUP message to the Cisco Unified CallManager. Uncheck the check box to exclude the Redirecting Number IE in the incoming SETUP message to the Cisco Unified CallManager. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box. Note Default leaves the check box checked. You cannot check this check box if you choose the QSIG option from the Tunneled Protocol drop-down list box.

Table 71-1 **Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)**

Field	Description
Enable Inbound FastStart	Check this check box to enable the H.323 FastStart call connections on incoming calls. By default, the check box remains unchecked for the H.323 gateway. For intercluster calls, you must check the Enable Inbound FastStart check box on Cisco Unified CallManager servers in other clusters for the outbound FastStart feature to work. If you updated Cisco CallManager 3.3(2) servers in other clusters with support patch B, do not enable inbound FastStart because 3.3(2)spB does not support the inbound FastStart feature over intercluster trunks
Outbound Calls	
Calling Party Selection	Choose the directory number that is sent on an outbound call on a gateway. The following options specify which directory number is sent: • Originator—Send the directory number of the calling device. • First Redirect Number—Send the directory number of the redirecting device. • Last Redirect Number—Send the directory number of the last device to redirect the call. • First Redirect Number (External)—Send the external directory number of the redirecting device. • Last Redirect Number (External)—Send the external directory number of the last device to redirect the call.
Calling Line ID Presentation	Cisco Unified CallManager uses calling line ID presentation (CLIP) as a supplementary service to control the display of the calling party's number on the called party's phone display screen. Choose Default if you do not want to change the presentation setting. Choose Allowed if you want calling number information to display. Choose Restricted if you do not want the calling number information to display.

Table 71-1 **Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)**

Field	Description
Called Party IE Number Type Unknown	Choose the format for the type of number in called party directory numbers. Cisco Unified CallManager sets the called directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans, such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified CallManager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the called directory number to be encoded to a non-national numbering plan type. Choose one of the following options: • Cisco Unified CallManager—Cisco Unified CallManager sets the directory number type. • Unknown—This option indicates that the dialing plan is unknown. • National—Use when you are dialing within the dialing plan for your country. • International—Use when you are dialing outside the dialing plan for your country. • Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number.

Table 71-1 **Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)**

Field	Description
Calling Party IE Number Type Unknown	Choose the format for the type of number in calling party directory numbers. Cisco Unified CallManager sets the calling directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans, such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified CallManager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the calling directory number to be encoded to a non-national numbering plan type. Choose one of the following options: • Cisco Unified CallManager—Cisco Unified CallManager sets the directory number type. • Unknown—This option indicates that the dialing plan is unknown. • National—Use when you are dialing within the dialing plan for your country. • International—Use when you are dialing outside the dialing plan for your country. • Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number.
Called Numbering Plan	Choose the format for the numbering plan in called party directory numbers. Cisco Unified CallManager sets the called DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans, such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified CallManager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the called numbering plan to be encoded to a non-national numbering plan. Choose one of the following options: • Cisco Unified CallManager—Cisco Unified CallManager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—This option indicates that the dialing plan is unknown.

Table 71-1 **Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)**

Field	Description
Calling Numbering Plan	Choose the format for the numbering plan in calling party directory numbers. Cisco Unified CallManager sets the calling DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans, such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified CallManager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the calling numbering plan to be encoded to a non-national numbering plan. Choose one of the following options: • Cisco Unified CallManager—Cisco Unified CallManager sets the Numbering Plan in the directory number. • ISDN—Use when you are dialing outside the dialing plan for your country. • National Standard—Use when you are dialing within the dialing plan for your country. • Private—Use when you are dialing within a private network. • Unknown—This option indicates that the dialing plan is unknown.
Caller ID DN	Enter the pattern, from 0 to 24 digits, that you want to use to format the caller ID on outbound calls from the trunk. For example, in North America • 555XXXX = Variable Caller ID, where X represents an extension number. The Central Office (CO) appends the number with the area code if you do not specify it. • 5555000 = Fixed Caller ID. Use this form when you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it.
Display IE Delivery	Check this check box to enable delivery of the display information element (IE) in SETUP and CONNECT messages for the calling and called party name delivery service. Note The default setting leaves this check box checked. You cannot check this check box if you choose the QSIG option from the Tunneled Protocol drop-down list box.

Table 71-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

Field	Description
Redirecting Diversion Header Delivery - Outbound	Check this check box to include the Redirecting Number IE in the outgoing SETUP message from the Cisco Unified CallManager to indicate the first Redirecting Number and the redirecting reason of the call when the call is forwarded. Uncheck the check box to exclude the first Redirecting Number and the redirecting reason from the outgoing SETUP message. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box. Note The default setting leaves this check box checked. You cannot check this check box if you choose the QSIG option from the Tunneled Protocol drop-down list box.
Enable Outbound FastStart	Check this check box to enable the H.323 FastStart feature on outgoing calls. By default, the check box remains unchecked for the H.323 gateway or trunk. When you check the Enable Outbound FastStart check box, you must set the Media Termination Point Required, Media Resource Group Lists, and Codec for Outbound FastStart.
Codec For Outbound FastStart	Choose the codec for use with the H.323 device for an outbound FastStart call: • G711 mu-law 64K (default) • G711 a-law 64K • G723 • G729 • G729AnnexA • G729AnnexB • G729AnnexA-AnnexB When you check the Enable Outbound FastStart check box, you must choose the codec for supporting outbound FastStart calls.
Gatekeeper Information	
(for gatekeeper-controlled H.225 trunks and intercluster trunks)	
Gatekeeper Name	Choose the gatekeeper that controls this trunk.
Terminal Type	Use the Terminal Type field to designate the type for all devices that this trunk controls. Always set this field to Gateway for normal trunk call admission control.

Table 71-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

Field	Description
Technology Prefix	Use this optional field to eliminate the need for entering the IP address of every Cisco Unified CallManager when configuring the gw-type-prefix on the gatekeeper: - If you leave this field blank (the default setting), you must specify the IP address of each Cisco Unified CallManager that can register with the gatekeeper when you enter the gw-type-prefix command on the gatekeeper. - When you use this field, make sure that the value that you enter exactly matches the <i>type-prefix</i> value that is specified with the gw-type-prefix command on the gatekeeper. For example, if you leave this field blank and you have two Cisco Unified CallManagers with IP addresses of 10.1.1.2 and 11.1.1.3, enter the following gw-type-prefix command on the gatekeeper: <pre>gw-type-prefix 1#* default-technology gw ip 10.1.1.2 gw ip 11.1.1.3</pre> If you enter 1#* in this field, enter the following gw-type-prefix command on the gatekeeper: <pre>gw-type-prefix 1#* default-technology</pre>
Zone	Use this optional field to request a specific zone on the gatekeeper with which Cisco Unified CallManager will register. The zone specifies the total bandwidth that is available for calls between this zone and another zone: - If you do not enter a value in this field, the zone subnet command on the gatekeeper determines the zone with which Cisco Unified CallManager registers. Cisco recommends the default setting for most configurations. - If you want Cisco Unified CallManager to register with a specific zone on the gatekeeper, enter the value in this field that exactly matches the zone name that is configured on the gatekeeper with the zone command. Specifying a zone name in this field eliminates the need for a zone subnet command for each Cisco Unified CallManager that is registered with the gatekeeper. Refer to the command reference documentation for your gatekeeper for more information.
Remote Cisco Unified CallManager Information	
(for non-gatekeeper-controlled intercluster trunks)	
Server 1 IP Address/Host Name	Enter the IP address or host name of the first remote Cisco Unified CallManager that this trunk accesses.

Table 71-1 **Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)**

Field	Description
Server 2 IP Address/Host Name	Enter the IP address or host name of the second remote Cisco Unified CallManager that this trunk accesses. Note If this non-gatekeeper-controlled intercluster trunk accesses the device pool of a remote non-gatekeeper-controlled intercluster trunk and that device pool has a second Cisco Unified CallManager node, you must enter the second remote Cisco Unified CallManager IP address/host name in this field.
Server 3 IP Address/Host Name	Enter the IP address or host name of the third remote Cisco Unified CallManager that this trunk accesses. Note If this non-gatekeeper-controlled intercluster trunk accesses the device pool of a remote non-gatekeeper-controlled intercluster trunk and that device pool has a third Cisco Unified CallManager node, you must enter the third remote Cisco Unified CallManager IP address/host name in this field.

Table 71-1 Trunk Configuration Settings for H.225 and Intercluster Trunks (continued)

Field	Description
MLPP Indication	If available, this setting specifies whether a device that is capable of playing precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options: • Default—This device inherits its MLPP indication setting from its device pool. • Off—This device does not handle nor process indication of an MLPP precedence call. • On—This device does handle and process indication of an MLPP precedence call. Note Do not configure a device with the following combination of settings: MLPP Indication is set to <i>Off</i> or <i>Default</i> (when default is <i>Off</i>) while MLPP Preemption is set to <i>Forceful</i>.
MLPP Preemption (not available for H.323 ICT)	If available, this setting specifies whether a device that is capable of preempting calls in progress will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options: • Default—This device inherits its MLPP preemption setting from its device pool. • Disabled—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. • Forceful—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. Note Do not configure a device with the following combination of settings: MLPP Indication is set to <i>Off</i> or <i>Default</i> (when default is <i>Off</i>) while MLPP Preemption is set to <i>Forceful</i>. Note MLPP Preemption flag currently is not available on the Trunk page. The preemption logic is controlled by the location based MLPP preemption flag.

Table 71-2 describes the trunk configuration settings for SIP trunks.

Table 71-2 Trunk Configuration Settings for SIP Trunks

Field	Description
Device Information	
Device Name	Enter a unique identifier for the trunk.
Description	Enter a descriptive name for the trunk.

Table 71-2 **Trunk Configuration Settings for SIP Trunks (continued)**

Field	Description
Device Pool	Choose the appropriate device pool for the trunk. For trunks, device pools specify a list of Cisco Unified CallManagers that the trunk uses to distribute the call load dynamically. Note Calls that are initiated from a phone that is registered to a Cisco Unified CallManager that does not belong to the trunk's device pool use different Cisco Unified CallManagers of this device pool for different outgoing calls. Selection of Cisco Unified CallManager nodes occurs in a random order. A call that is initiated from a phone that is registered to a Cisco Unified CallManager that does belong to the trunk's device pool uses the same Cisco Unified CallManager node for outgoing calls if the Cisco Unified CallManager is up and running. The default value for Device Pool is Not Selected.
Call Classification	This parameter determines whether an incoming call through this trunk is considered off the network (OffNet) or on the network (OnNet). The default value for Call Classification is Use System Default. When the Call Classification field is configured as Use System Default, the setting of the Cisco Unified CallManager clusterwide service parameter, Call Classification, determines whether the trunk is OnNet or OffNet. This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively. Use this parameter in conjunction with the settings on the Route Pattern Configuration window to classify an outgoing call as OnNet or OffNet.
Media Resource Group List	This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that a Media Resource Group List defines. The default value for Media Resource Group List is None.
Location	Choose the appropriate location for the trunk. The location specifies the total bandwidth that is available for calls between this location and the central location, or hub. A location setting of Hub_None specifies unlimited available bandwidth. The location is also associated with the RSVP policy with regard to other locations. The configuration allows RSVP to be enabled and disabled based upon location pairs. The default value for Location is Hub_None.

Table 71-2 **Trunk Configuration Settings for SIP Trunks (continued)**

Field	Description
AAR Group	Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted. The default value for AAR Group is None.
Packet Capture Mode	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. Choose one of the following options from the drop-down list box: • None—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting. • Batch Processing Mode—Cisco Unified CallManager writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Cisco Unified CallManager, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified CallManager stores the file in /var/pktCap. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file. Before you contact TAC, you must capture the SRTP packets by using a sniffer trace between the affected devices. Tip For more information on capturing packets, refer to the <i>Cisco Unified CallManager Security Guide</i>.
Packet Capture Duration	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes that is allotted for one session of packet capturing. The default setting equals 0, although the range exists from 0 to 300 minutes. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays. Tip For more information on capturing packets, refer to the <i>Cisco Unified CallManager Security Guide</i>.

Table 71-2 **Trunk Configuration Settings for SIP Trunks (continued)**

Field	Description
Media Termination Point Required	Cisco Unified CallManager SIP trunks can be configured to always use an MTP. Check this box to provide media channel information in the outgoing INVITE request. When this box is checked all media channels are required to terminate and re-originate on the MTP device. If you uncheck the check box, the Cisco Unified CallManager can decide if calls are to go through the MTP device or if they will be connected directly between the endpoints. Note If unchecked (default case), Cisco Unified CallManager will attempt to dynamically allocate an MTP if the DTMF methods for the call legs are not compatible. For example, existing SCCP phones support only out-of-band DTMF and existing SIP phones support RFC2833. Since the DTMF methods are not identical the Cisco Unified CallManager will dynamically allocate an MTP. If however a new SCCP phone, which supports RFC2833 and out-of-band, calls an existing SIP phone Cisco Unified CallManager will not allocate an MTP since both phones support RFC2833. So by having the same type of DTMF method supported on each phone no MTP is needed.
Retry Video Call as Audio	This check box pertains to outgoing SIP trunk calls and does not impact incoming calls. By default, the system checks this check box to specify that this device should immediately retry a video call as an audio call (if it cannot connect as a video call) prior to sending the call to call control for rerouting. If you uncheck this check box, a video call that fails to connect as video does not try to establish as an audio call. The call then fails to call control, and call control routes the call via Automatic Alternate Routing (AAR) and/or route/hunt list.
Transmit UTF-8 for Calling Party Name	This device uses the user locale setting of the device's device pool to determine whether to send Unicode and whether to translate received Unicode information. For the sending device, if you check this check box and the user locale setting in the device's device pool matches the terminating phone's user locale, the device sends Unicode. If the user locale settings do not match, the device sends ASCII. The receiving device translates incoming Unicode characters based on the user locale setting of the sending device's device pool. If the user locale setting matches the terminating phone's user locale, the phone displays the characters. Note The phone may display malformed characters if the two ends of the trunk configure user locales that do not belong to the same language group. The default value for Transmit UTF-8 for Calling Party Name check box is unchecked.

Table 71-2 **Trunk Configuration Settings for SIP Trunks (continued)**

Field	Description
Unattended Port	Check this check box if calls can be redirected and transferred to an unattended port, such as a voice mail port. The default value for this check box is unchecked.
Multilevel Precedence and Preemption (MLPP) Information	
MLPP Domain	From the drop-down list, choose an MLPP domain to associate with this device. If you leave this field blank, this device inherits its MLPP domain from the value that is set for the device's device pool. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value that is set for the MLPP Domain Identifier enterprise parameter. The default value for MLPP Domain is None.
Call Routing Information	
Inbound Calls	
Significant Digits	Significant digits represent the number of final digits that are retained on inbound calls. Use for the processing of incoming calls and to indicate the number of digits that are used to route calls that are coming in to the SIP device. Choose the number of significant digits to collect, from 0 to 32 or choose All.  Note Cisco Unified CallManager counts significant digits from the right (last digit) of the number that is called. The default value for Significant Digits is All.
Connected Line ID Presentation	Cisco Unified CallManager uses connected line ID presentation (COLP) as a supplementary service to provide the calling party with the connected party's number. The SIP trunk level configuration takes precedence over the call-by-call configuration. The default value for Connected Line ID Presentation is Default which translates to Allowed. Choose Default if you want Cisco Unified CallManager to send connected line information. Choose Restricted if you do not want Cisco Unified CallManager to send connected line information.
Connected Name Presentation	Cisco Unified CallManager uses connected name ID presentation (CONP) as a supplementary service to provide the calling party with the connected party's name. The SIP trunk level configuration takes precedence over the call-by-call configuration. The default value for Connected Name Presentation is Default which translate to Allowed. Choose Default if you want Cisco Unified CallManager to send connected name information. Choose Restricted if you do not want Cisco Unified CallManager to send connected name information.

Table 71-2 **Trunk Configuration Settings for SIP Trunks (continued)**

Field	Description
Calling Search Space	From the drop-down list box, choose the appropriate calling search space for the trunk. The calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more calling search spaces exist than the number that is configured in the Max List Box Items enterprise parameter, the ellipsis button (...) displays next to the drop-down list box. Click the “...” button to display the Select Calling Search Space window. Enter a partial calling search space name in the List items where Name contains field. Click the desired calling search space name in the list of calling search spaces that displays in the Select item to use box and click OK. Note To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters. The default value for Calling Search Space is None.
AAR Calling Search Space	Choose the appropriate calling search space for the device to use when performing automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth. The default value for AAR Calling Search Space is None.
Prefix DN	Enter the prefix digits that are appended to the called party number on incoming calls. Cisco Unified CallManager adds prefix digits after first truncating the number in accordance with the Significant Digits setting.
Redirecting Diversion Header Delivery - Inbound	Check this check box to accept the Redirecting Number in the incoming INVITE message to the Cisco Unified CallManager. Uncheck the check box to exclude the Redirecting Number in the incoming INVITE message to the Cisco Unified CallManager. You use Redirecting Number for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number, you should check the check box. The default value for Redirecting Number IE Deliver - Inbound is not checked.

Table 71-2 **Trunk Configuration Settings for SIP Trunks (continued)**

Field	Description
Outbound Calls	
Calling Party Selection	Choose the directory number that is sent on an outbound call. The following options specify which directory number is sent: • Originator—Send the directory number of the calling device. • First Redirect Number—Send the directory number of the redirecting device. • Last Redirect Number—Send the directory number of the last device to redirect the call. • First Redirect Number (External)—Send the external directory number of the redirecting device. • Last Redirect Number (External)—Send the external directory number of the last device to redirect the call. The default value for Calling Party Selection is Originator.
Calling Line ID Presentation	Cisco Unified CallManager uses calling line ID presentation (CLIP) as a supplementary service to provide the calling party's number. The SIP trunk level configuration takes precedence over the call-by-call configuration. The default value for Calling Line ID Presentation is Default which translates to Allowed. Choose Default if you want Cisco Unified CallManager to send calling number information. Choose Restricted if you do not want Cisco Unified CallManager to send the calling number information.
Calling Name Presentation	Cisco Unified CallManager uses calling name ID presentation (CNIP) as a supplementary service to provide the calling party's name. The SIP trunk level configuration takes precedence over the call-by-call configuration. Choose <i>Allowed</i>, which is the default, if you want Cisco Unified CallManager to send calling name information. Choose <i>Restricted</i> if you do not want Cisco Unified CallManager to send the calling name information. The default value for Calling Name Presentation is Default.
Caller ID DN	Enter the pattern, from 0 to 24 digits, that you want to use to format the caller ID on outbound calls from the trunk. For example, in North America • 555XXXX = Variable Caller ID, where X represents an extension number. The Central Office (CO) appends the number with the area code if you do not specify it. • 5555000 = Fixed Caller ID. Use this form when you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it.

Table 71-2 **Trunk Configuration Settings for SIP Trunks (continued)**

Field	Description
Caller Name	Check this box to override the caller name that is received from the originating SIP device.
Redirecting Diversion Header Delivery - Outbound	Check this check box to include the Redirecting Number in the outgoing INVITE message from the Cisco Unified CallManager to indicate the original called party number and the redirecting reason of the call when the call is forwarded. Uncheck the check box to exclude the first Redirecting Number and the redirecting reason from the outgoing INVITE message. You use Redirecting Number for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number, you should check the check box. The default value for Redirecting Number IE Delivery - Outbound does not get checked.
SIP Information	
Destination Address	This field requires the IP address, fully qualified domain name (FQDN), or DNS SRV address of the remote SIP device. This field also routes incoming calls. Note SIP trunks only accept incoming messages from the host that the Destination Address field specifies and the incoming port specifies in the security profile that this trunk used. The host value in the Destination Address field can be an IP address, DNS SRV, or a FQDN entry. If the remote end is a Cisco Unified CallManager cluster, DNS SRV represents the recommended choice for this field. The DNS SRV record should include all Cisco Unified CallManagers within the cluster.
Destination Address is an SRV	Check the check box if the destination address specifies a Domain Name System Server (DNS SRV) address. The default value for Destination Address is an SRV is not checked.
Destination Port	Choose the destination port. Ensure that the value that you enter specifies any port from 1024 - 65535. Note You can now have the same port number that is specified for multiple trunks. You need not enter a value if the destination address is an DNS SRV port. The default 5060 indicates the SIP port. The default value for Destination Port specifies 5060.
MTP Preferred Originating Codec	Indicate the preferred outgoing codec. This field is used only when the MTP Termination Point Required check box is checked.

Table 71-2 **Trunk Configuration Settings for SIP Trunks (continued)**

Field	Description
Presence Group	Configure this field with the Presence feature. From the drop-down list box, choose a Presence group for the SIP trunk. The selected group specifies the destinations that the device/application/server that is connected to the SIP trunk can monitor. The default value for Presence Group specifies Standard Presence group, configured with installation. Presence groups that are configured in Cisco Unified CallManager Administration also appear in the drop-down list box. Presence authorization works with presence groups to allow or block presence requests between groups. Refer to the “Presence” chapter in the <i>Cisco Unified CallManager Features and Services Guide</i> for information about configuring permissions between groups. Tip A presence group can be applied to the SIP trunk or to the application that is connected to the SIP trunk. If a presence group is configured for both a SIP trunk and SIP trunk application, the presence group that is applied to the application overrides the presence group that is applied to the trunk.
SIP Trunk Security Profile	For this mandatory entry, from the drop-down list box, choose the security profile that you want to apply to the SIP trunk. For information on how to configure security profiles, refer to the <i>Cisco Unified CallManager Security Guide</i>. The default value for SIP Trunk Security Profile specifies Not Selected.
Rerouting Calling Search Space	Calling search spaces determine the partitions that calling devices can search when attempting to complete a call. The rerouting calling search space gets used to determine where a SIP user (A) can refer another user (B) to a third party (C). After the refer is completed, B and C connect. In this case, the rerouting calling search space that is used is that of the initial SIP user (A). Note Calling Search Space also applies to 3xx redirection and INVITE with Replaces features. The default value for Rerouting Calling Search Space specifies None.
Out-of-Dialog Refer Calling Search Space	Calling search spaces determine the partitions that calling devices can search when attempting to complete a call. The out-of-dialog calling search space is used when a Cisco Unified CallManager refers a call (B) coming into SIP user (A) to a third party (C) when there is no involvement of SIP user (A). In this case, the out-of-dialog calling search space the system uses is that of SIP user (A). The default value for Out-of-Dialog Refer Calling Search Space specifies None.

Table 71-2 **Trunk Configuration Settings for SIP Trunks (continued)**

Field	Description
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Cisco Unified CallManager routes presence requests from the device/server/application that connects to the SIP trunk. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the SIP trunk. From the drop-down list box, choose the SUBSCRIBE calling search space to use for presence requests for the SIP trunk. All calling search spaces that you configure in Cisco Unified CallManager Administration display in the SUBSCRIBE Calling Search Space drop-down list box. If you do not select a different calling search space for the SIP trunk from the drop-down list, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces. For information on how to configure a calling search space, see the “Calling Search Space Configuration” section on page 43-1.
SIP Profile	From the drop-down list box, choose the SIP profile to be used for this SIP trunk. The default value for SIP Profile specifies None Selected.
DTMF Signaling Method	Choose from the following options: No Preference (default)—Cisco Unified CallManager will pick the DTMF method to negotiate DTMF, so an MTP is not required for the call. If Cisco Unified CallManager has no choice but to allocate an MTP (if the Media Termination Point Required check box is checked), SIP trunk will negotiate DTMF to RFC2833. RFC 2833—Choose this configuration if the preferred DTMF method to be used across the trunk is RFC2833. Cisco Unified CallManager makes every effort to negotiate RFC2833 regardless of MTP usage. Out-of-band provides the fallback method if the peer endpoint supports it. OOB and RFC 2833—Choose this configuration if both out-of-band and RFC2833 should be used for DTMF. Note If the peer endpoint supports both out-of-band and RFC2833, Cisco Unified CallManager will negotiate both out-of-band and RFC2833 DTMF methods. As a result, two DTMF events would be sent for the same DTMF keypress (one out-of-band and the other, RFC2833).

Additional Topics

See the [“Related Topics” section on page 71-28](#).

Deleting a Trunk

Perform the following steps to delete a trunk.

Before You Begin

You cannot delete a trunk that is assigned to one or more route patterns. To find out which route patterns are using the trunk, in the Trunk Configuration window, choose **Dependency Records** from the Related Links drop-down list box and click **Go**. If dependency records are not enabled for the system, the Dependency Records Summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#). If you try to delete a trunk that is in use, Cisco Unified CallManager displays a message. Before deleting a trunk that is currently in use, you must perform either or both of the following tasks:

- Assign a different trunk to any route patterns that are using the trunk that you want to delete. See the [“Configuring a Route Pattern” section on page 35-3](#).
- Delete the route patterns that are using the trunk that you want to delete. See the [“Deleting a Route Pattern” section on page 35-10](#).

Procedure

Step 1 Choose **Device > Trunk**.

The Find and List Trunks window displays.

Step 2 To locate a specific trunk, enter search criteria and click **Find**.

A list of trunks that match the search criteria displays.

Step 3 Perform one of the following actions:

- Check the check boxes next to the trunks that you want to delete and click **Delete Selected**.
- Delete all trunks in the window by clicking **Select All** and then clicking **Delete Selected**.
- From the list, choose the name of the trunk that you want to delete to display its current settings and click **Delete**.

A confirmation dialog displays.

Step 4 To delete the trunk, click **OK**.

Additional Topics

See the [“Related Topics” section on page 71-28](#).

Resetting a Trunk

Perform the following procedure to reset the trunk.



Caution

Resetting devices can cause them to drop calls.

Procedure

-
- Step 1** Choose **Device > Trunk**.
The Find and List Trunks window displays.
- Step 2** To locate a specific trunk, enter search criteria and click **Find**.
A list of trunks that match the search criteria displays.
- Step 3** From the list, click the name of the trunk that you want to reset.
The Trunk Configuration window displays.
- Step 4** After you change any settings for the Trunk Device, click **Reset Trunk**.
The Device Reset dialog displays.
- Step 5** Click one of the following choices:
- **Restart**—Restarts the trunk device without shutting it down first.
 - **Reset**—Shuts down, then restarts the internal trunk device. The Cisco Unified CallManager cluster unregisters (URQ) and then reregisters (RRQ) with the trunk if the trunk is gatekeeper controlled.
 - **Close**—Closes the Reset Device dialog without performing any action.

**Note**

For SIP trunks Restart and Reset behave the same way where all active calls will be disconnected when pressed. Trunks do not have to undergo a Restart or Reset when enabling/disabling PAKet Capture.

Additional Topics

See the [“Related Topics”](#) section on page 71-28.

Related Topics

- [Finding a Trunk, page 71-1](#)
- [Configuring a Trunk, page 71-2](#)
- [Trunk Configuration Settings, page 71-3](#)
- [Deleting a Trunk, page 71-27](#)
- [Resetting a Trunk, page 71-27](#)
- [Configuring SIP Profiles, page 79-2](#)
- [SIP Trunk Security Profile Configuration](#)
- [Call Admission Control, Cisco Unified CallManager System Guide](#)
- [Gatekeepers and Trunks, Cisco Unified CallManager System Guide](#)
- [Gatekeeper and Trunk Configuration in Cisco Unified CallManager, Cisco Unified CallManager System Guide](#)
- [Cisco Unified CallManager Security Guide](#)
- [Cisco Unified Communications Solution Reference Network Design \(SRND\)](#)



Device Defaults Configuration

Use device defaults to set the default characteristics of each type of device that registers with a Cisco Unified CallManager. The device defaults for a device type apply to all auto-registered devices of that type within a Cisco Unified CallManager cluster. You can set the following device defaults for each device type to which they apply:

- Device load
- Device pool
- Phone button template

When a device auto-registers with a Cisco Unified CallManager, it acquires the device default settings for its device type. After a device registers, you can update its configuration individually to change the device settings.

Installing Cisco Unified CallManager automatically sets device defaults. You cannot create new device defaults or delete existing ones, but you can change the default settings.

This section covers the following topics:

- [Updating Device Defaults, page 72-1](#)
- [Device Defaults Configuration Settings, page 72-2](#)

Updating Device Defaults

This section describes how to modify the device defaults in the Cisco Unified CallManager configuration database.

Before You Begin

Before updating the device defaults, perform any of the following tasks that apply to your system:

- Add new firmware files for the devices to the TFTP server.
- If you use device defaults to assign a firmware load that does not exist in the directory, those devices will fail to load the assigned firmware.
- Configure new device pools. See the [“Configuring a Device Pool” section on page 9-3](#).
- If the device is a phone, configure new phone templates. See the [“Configuring Phone Button Templates” section on page 76-2](#).

Procedure

-
- Step 1** Choose **Device > Device Settings > Device Defaults**.
- Step 2** Update the appropriate settings for the device that you want to change as described in [Table 72-1](#).
- Step 3** To save the changes in the Cisco Unified CallManager configuration database, click **Save**.
- Step 4** To reset all the devices of that type, click the Reset icon to the left of the device name and load the new defaults on all Cisco Unified CallManagers in the cluster.
- If you choose not to reset all devices of that type, only new devices that are added after you change the device defaults receive the latest defaults.
-

Additional Information

See the [“Related Topics”](#) section on page 72-2.

Device Defaults Configuration Settings

[Table 72-1](#) describes the configuration settings for device defaults. For more information about related procedures, see the [“Related Topics”](#) section on page 72-2.

Table 72-1 *Device Defaults Configuration Settings*

Field Name	Description
Load Information	Enter the ID number of the firmware load that is used with a particular type of hardware device. If you install an upgrade or patch load, you must update the load information for each type of device that uses the new load.
Device Pool	Choose the device pool that is associated with each type of device. The device pool defines common characteristics for all devices in the pool.
Phone Template	Choose the phone button template that each type of Cisco Unified IP Phone uses. The template defines what keys on the phone perform that function.

Related Topics

- [Updating Device Defaults, page 72-1](#)
- [Device Defaults Configuration Settings, page 72-2](#)
- [Finding Devices With Non-Default Firmware Loads, page 73-1](#)
- [Device Firmware Loads, Cisco Unified CallManager System Guide](#)



Device Firmware Load Information

Use device firmware load information to locate devices that are not using the default firmware load for their device type.

Finding Devices With Non-Default Firmware Loads

The Firmware Load Information window in Cisco Unified CallManager Administration enables you to quickly locate devices that are not using the default firmware load for their device type.



Note

Each device can have an individually assigned firmware load that overrides the default.

Use the following procedure to locate devices that are not using the default firmware load.

Procedure

Step 1 Choose **Device > Device Settings > Firmware Load Information**.

The page updates to display a list of device types that require firmware loads. For each device type, the **Devices Not Using Default Load** column links to configuration settings for any devices that use a non-default load.

Step 2 To view a list of devices that are using a non-default device load, click the **Devices Not Using Default Load** column.



Default Device Profile Configuration

Use the default device profile for whenever a user logs on to a phone model for which no user device profile exists. To create a default device profile for each phone model that supports Cisco Extension Mobility, use the Default Device Profile Configuration window. The maximum number of default device profiles cannot exceed the number of phone models that support Cisco Extension Mobility.

For example, a user logs on to a Cisco Unified IP Phone model 7960, for which there is a user device profile. The user device profile for the user gets downloaded to the phone to which the user logged on. Later, the same user logs on to a Cisco Unified IP Phone model 7940, for which he does not have a user device profile. In this case, the default device profile for the model 7940 gets downloaded to the phone.

A default device profile comprises the set of attributes (services and/or features) that are associated with a particular device. Device profiles include device type, user locale, phone button template, softkey template, multilevel precedence and preemption (MLPP) information, and Cisco Unified IP Phone services.

Configuring a New Default Device Profile

The default device profile contains attributes such as device type, phone template, user locale, expansion modules, softkey template, MLPP information, and subscribed Cisco Unified IP Phone services. Perform the following procedure to add or update a default device profile,

Procedure

-
- Step 1** Choose **Device > Device Settings > Default Device Profile**.
The Default Device Profile Configuration window displays.
- Step 2** Perform one of the followings tasks:
- To add a new profile, choose the type of device that you want to add from the Device Profile Type drop-down list box; then, click **Next** and continue with [Step 3](#).
 - To update an existing profile, click the device profile that you want to update from the Default Device Profile pane. The Default Device Profile Configuration window displays the profile information of the profile that you chose; continue with [Step 3](#)
- Step 3** Enter the appropriate settings in the profile as described in [Table 74-1](#).
- Step 4** Click **Save**.

- Step 5** To add Cisco Unified IP Phone services to this profile, from the Related Links drop-down list box, choose the **Subscribe/Unsubscribe Services** and click **Go**.
- The Subscribe Cisco Unified IP Phone services window displays.
- Step 6** From the Select a Service drop-down list box, choose the service that you want to add to the profile.
- Step 7** Click **Next**.
- The window displays with the service that you chose. If you want to choose a different service, click **Back** and repeat Step 6.
- Step 8** Click **Subscribe**.
- The service appears in the Subscribed Services list.

Additional Topics

See the [“Related Topics” section on page 74-5](#).

Default Device Profile Configuration Settings

[Table 74-1](#) describes the fields that are available in the Default Device Profile Configuration window.

Table 74-1 *Default Device Profile Configuration Settings*

Field	Description
Default Device Profile Information	
Description	Enter a description for the default device profile configuration.
User Hold Audio Source	To specify the audio source that plays when a user initiates a hold action, click the drop-down arrow and choose an audio source from the list that displays. If you do not choose an audio source, Cisco Unified CallManager uses the audio source that is defined in the device pool or uses the system default if the device pool does not specify an audio source ID. Note You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose Media Resources > Music On Hold Audio Source.
User Locale	From the drop-down list box, choose the locale that is associated with the phone user interface. The user locale identifies a set of detailed information, including language and font, to support users. Cisco Unified CallManager makes this field available only for phone models that support localization. Note If no user locale is specified, Cisco Unified CallManager uses the user locale that is associated with the device pool. Note If the users require information to display (on the phone) in any language other than English, verify that the locale installer is installed before configuring user locale. Refer to the Cisco Unified CallManager Locale Installer documentation.

Table 74-1 **Default Device Profile Configuration Settings (continued)**

Field	Description
Privacy	From the drop-down list box, choose On for each phone on which you want privacy. For more configuration information, refer to “Barge and Privacy” in the <i>Cisco Unified CallManager Features and Services Guide</i> .
Ignore Presentation Indicators (internal calls only)	Check the Ignore Presentation Indicators (internal calls only) check box to configure call display restrictions and ignore any presentation restriction that is received for internal calls. Note Use this configuration in combination with the calling line ID presentation and connected line ID presentation configuration at the translation pattern-level. Together, these settings allow you to configure call display restrictions to selectively present or block calling and/or connected line display information for each call. For more information about call display restrictions, refer to Call Display Restrictions in the <i>Cisco Unified CallManager Features and Services Guide</i>.
Allow Control of Device from CTI	Check this check box to allow CTI to control and monitor this device.
Phone Button Template Information	
Phone Button Template	Choose the appropriate phone button template. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button.
Softkey Template Information	
Softkey Template	Choose the appropriate softkey template. The softkey template determines the configuration of the softkeys on Cisco Unified IP Phones. If the device pool contains the assigned softkey template, leave this field blank.
Expansion Module Information	
Module 1	Choose the 7914 14-button expansion module or none.
Module 2	Choose the 7914 14-button expansion module or none.
Multilevel Precedence and Preemption (MLPP) Information	
MLPP Domain (e.g., “0000FF”)	Choose MLPP domain that is associated with this device from the drop-down list box.

Table 74-1 **Default Device Profile Configuration Settings (continued)**

Field	Description
MLPP Indication	If available, this setting specifies whether a device that is capable of playing precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to devices that use this default device profile from the following options: • Default—This device inherits its MLPP indication setting from its device pool. • Off—This device does not handle nor process indication of an MLPP precedence call. • On—This device does handle and process indication of an MLPP precedence call. Note Do not configure a default device profile with the following combination of settings: MLPP Indication is set to <i>Off</i> or <i>Default</i> (when default is <i>Off</i>) while MLPP Preemption is set to <i>Forceful</i>. Note Turning on MLPP Indication (at the enterprise parameter, device pool, or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device.
MLPP Preemption	If available, this setting specifies whether a device that is capable of preempting calls in progress will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to devices that use this default device profile from the following options: • Default—This device inherits its MLPP preemption setting from its device pool. • Disabled—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. • Forceful—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. Note Do not configure a default device profile with the following combination of settings: MLPP Indication is set to <i>Off</i> or <i>Default</i> (when default is <i>Off</i>) while MLPP Preemption is set to <i>Forceful</i>.
Logged Out (Default) Profile Information	
Login User Id	Enter a valid login user ID. If the user device profile is used as a logout profile, specify the login user ID that will be associated with the phone. After the user logs out from this user device profile, the phone will automatically log in to this login user ID.

Additional Topics

See the [“Related Topics”](#) section on page 74-5.

Deleting a Default Device Profile

This section describes how to delete a default device profile.

Procedure

-
Step 1	Choose Device > Device Settings > Default Device Profile .
Step 2	From the Default Device Profile pane, click the device profile that you want to delete. The Default Device Profile Configuration window displays the profile information of the profile that you chose.
Step 3	Click Delete . A message displays that states that this action cannot be undone.
Step 4	To delete the default device profile, click OK or, to cancel the deletion, click Cancel .
-

Additional Topics

See the [“Related Topics”](#) section on page 74-5.

Subscribing Services to a Default Device Profile

To subscribe a service such as Cisco Extension Mobility to the default device profile, see the [“Configuring a Cisco Unified IP Phone Service”](#) section on page 78-3.

Additional Topics

See the [“Related Topics”](#) section on page 74-5.

Related Topics

Use the following topics to configure and update default device profiles:

- [Configuring a New Default Device Profile, page 74-1](#)
- [Deleting a Default Device Profile, page 74-5](#)
- [Subscribing Services to a Default Device Profile, page 74-5](#)
- [Default Device Profile Configuration Settings, page 74-2](#)



Device Profile Configuration

A device profile comprises the set of attributes (services and/or features) that are associated with a particular device. Device profiles include name, description, phone template, add-on modules, softkey templates, multilevel precedence and preemption (MLPP) information, directory numbers, subscribed services, and speed-dial information. Two kinds of device profiles exist: autogenerated and user. You can assign the user device profile to a user, so, when the user logs in to a device, the user device profile that you have assigned to that user loads onto that device as a default login device profile. After a user device profile is loaded onto the phone, the phone picks up the attributes of that device profile.

You can also assign a user device profile to be the default logout device profile for a particular device. When a user logs out of a phone, for instance, the logout device profile loads onto the phone and gives that phone the attributes of the logout device profile. In the Cisco Unified CallManager Administration windows, you can create, modify, or delete the user device profile. If a user device profile is used as the logout device profile, you cannot delete the user device profile.

The autogenerated device profile, which is a special device profile, gets generated when you configure a phone for Cisco Extension Mobility and choose “Use Current Device Settings” from the Phone Configuration window. The autogenerated device profile then associates with a specific phone to be the logout device profile.

Cisco Unified CallManager also supports a device profile default. Use the device profile default for whenever a user logs on to a phone model for which no user device profile exists. To create a device profile default for each phone model that supports Cisco Extension Mobility, use the Device Profile Default Configuration window. The maximum number of device profile defaults cannot exceed the number of phone models that support Cisco Extension Mobility. For more information about the device profile default, see the [“Default Device Profile Configuration” section on page 74-1](#).

Use the following topics to configure and locate device profiles:

- [Finding a Device Profile, page 75-2](#)
- [Configuring a New User Device Profile, page 75-2](#)
- [Deleting a User Device Profile, page 75-5](#)
- [Updating Autogenerated Device Profiles, page 75-6](#)
- [Directory Number Configuration Overview, page 49-1](#)
- [Directory Number Configuration Settings, page 49-6](#)

Finding a Device Profile

This topic describes how to use the Find and List Device Profile window. The Find and List lookup function allows you to search for user and autogenerated device profiles or both types. The function searches every type of device profile against the following categories:

- Profile name
- Description
- Device type

Procedure

Step 1 Choose **Device > Device Settings > Device Profile**.

The Find and List Device Profile window displays.

Step 2 From the drop-down lists, choose your search text for the type of device profiles that you want listed and click **Find**.



Note To find all device profiles that are registered in the database, click **Find** without entering any text.

The window refreshes and then displays the device profiles that match your search criteria.

To Jump to an Autogenerated Device Profile or User Device Profile:

Step 3 From the Find drop-down list box, choose either **User**, **Autogenerated** or **All** and then click **Find**.

Step 4 Choose the user or autogenerated device profile from the list of records that match your search criteria.

To Delete Device Profiles:

Step 5 Use the check box in the first column to delete multiple device profiles at once. Check the first check box in the list and click **Delete Selected**. You can also choose individual user device profiles to delete them separately.



Note You cannot delete autogenerated device profiles. You cannot delete user device profiles if phones are using them as a logout profile.

Additional Information

See the [“Related Topics” section on page 75-8](#).

Configuring a New User Device Profile

The user device profile contains attributes such as device profile name, description, phone template, user locale, expansion modules, softkey template, MLPP information, directory numbers, subscribed services, and speed-dial information. Perform the following procedure to add or update a user device profile.

Before You Begin

Make sure that phone button template(s) are already configured before proceeding with the steps. See the [“Configuring Phone Button Templates”](#) section on page 76-2 for more information.

Procedure

Step 1 Choose **Device > Device Settings > Device Profile**.

The Find and List Device Profile window displays.

Step 2 Perform one of the followings tasks:

- To add a new device profile, click the **Add New** button. The User Device Profile Configuration window displays. Continue with [Step 3](#).
- To update an existing user device profile, locate the appropriate device profile as described in [“Finding a Device Profile”](#) section on page 75-2, and continue with [Step 5](#).



Note Before updating a user device profile, make sure that the device profile that you want to update is configured in Cisco Unified CallManager.

Step 3 From the Device Profile Type drop-down list box, choose a device type. Click **Next**.

Step 4 From the Select the device profile protocol drop-down list box, choose the protocol for the device profile. Click **Next**.

Step 5 In the User Device Profile Name field, enter a unique name. This name can comprise up to 50 characters in length.

Step 6 In the Description field, enter a description of the user device profile. For text, use anything that describes this particular user device profile.

Step 7 To specify the audio source that plays when a user initiates a hold action, choose an audio source from the User Hold Audio Source drop-down list box.

If you do not choose an audio source, Cisco Unified CallManager uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID.



Note You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose **Media Resources > Music On Hold Audio Source**.

Step 8 From the User Locale drop-down list, choose the language in which the device displays.

Step 9 To configure call display restrictions and ignore any presentation restriction that is received for internal calls, check the “Ignore Presentation Indicators (internal calls only)” check box.



Note Use this configuration in combination with the calling line ID presentation and connected line ID presentation configuration at the translation pattern-level. Together, these settings allow you to configure call display restrictions to selectively present or block calling and/or connected line display information for each call. For more information about call display restrictions, refer to the [Call Display Restrictions](#) chapter in the *Cisco Unified CallManager Features and Services Guide*.

Step 10 To allow CTI to control and monitor the device, check the Allow Control of Device from CTI check box.

Step 11 From the Phone Button Template drop-down list, choose a phone button template.



Tip

If you want to configure BLF/SpeedDials for the profile for presence monitoring, choose a phone button template that you configured for BLF/SpeedDials. After you save the configuration, the Add a New BLF SD link displays in the Association Information pane. For more information on BLF/SpeedDials, refer to [“Presence”](#) in the *Cisco Unified CallManager Features and Services Guide*.

Step 12 From the Softkey Template drop-down list box choose the softkey template from the list that displays.

Step 13 You can configure one or two expansion modules for this device profile by choosing phone templates from the expansion module drop-down lists in the expansion module fields.



Note

You can view a phone button list at any time by choosing the View button list link next to the phone button template fields. A separate dialog box pops up and displays the phone buttons for that particular expansion module.

Step 14 From the Privacy drop-down list box, choose **On** for each phone on which you want privacy. For more information, refer to [“Barge and Privacy”](#) in the *Cisco Unified CallManager Features and Services Guide*.

Step 15 If this user device profile will be used for MLPP precedence calls, choose the MLLP Domain from the drop-down list box.

Step 16 If this user device profile will be used for MLPP precedence calls, assign an MLPP Indication setting to the device profile. This setting specifies whether a device that can play precedence tones will use the capability when it places an MLPP precedence call.

From the drop-down list box, choose a setting to assign to this device profile from the following options:

- **Default**—This device profile inherits its MLPP indication setting from the associated device’s device pool.
- **Off**—This device does not handle nor process indication of an MLPP precedence call.
- **On**—This device profile does handle and process indication of an MLPP precedence call.



Note

Do not configure a device profile with the following combination of settings: MLPP Indication is set to *Off or Default* (when default is *Off*) while MLPP Preemption is set to *Forceful*.

Step 17 If this user device profile will be used for MLPP precedence calls, assign an MLPP Preemption setting to the device profile. This setting specifies whether a device that can preempt calls in progress will use the capability when it places an MLPP precedence call.

From the drop-down list box, choose a setting to assign to this device profile from the following options:

- **Default**—This device profile inherits its MLPP preemption setting from the associated device’s device pool.
- **Off**—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls.

- **On**—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls.



Note Do not configure a device profile with the following combination of settings: MLPP Indication is set to *Off or Default* (when default is *Off*) while MLPP Preemption is set to *On*.

Step 18 From the Login User ID drop-down list box, choose a valid login user ID.



Note If the user device profile is used as a logout profile, specify the login user ID that will be associated with the phone. After the user logs out from this user device profile, the phone will automatically log in to this login user ID.

Step 19 Click **Save**.

From Association Info, you can configure directory numbers and speed dials for the profile. Refer to the [“Directory Number Configuration Overview” section on page 49-1](#), [“Cisco Unified IP Phone Configuration” section on page 70-1](#), of the Cisco Unified CallManager Administration Guide, and the [“Presence” section in the Cisco Unified CallManager Features and Services Guide](#) for the appropriate settings as described in these sections.

Step 20 Click **Save**.



Note You must log in to a device for changes to a user device profile to take effect.

Additional Information

See the [“Related Topics” section on page 75-8](#).

Deleting a User Device Profile

This section describes how to delete a user device profile.

Before You Begin

You cannot delete a device profile if it is assigned to devices. To find out which devices are using the device profile, choose **Dependency Records** link from the Related Links drop-down list box in the Device Profile Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#). If you try to delete a device profile that is in use, Cisco Unified CallManager displays message. Before deleting a device profile that is currently in use, you must perform either or both of the following tasks:

- Assign a different device profile to any devices that are using the device profile that you want to delete.
- Delete the devices that are using the device profile that you want to delete.

Procedure

-
- Step 1** Locate the user device profile that you want to delete. See the [“Finding a Device Profile” section on page 75-2](#).
- Step 2** From the User Device Profile Configuration window, click **Delete**.
A message displays that states that this you cannot undo this action.
- Step 3** To delete the device profile, click **OK** or to cancel the deletion, click **Cancel**.



Note If a user device profile is configured as a default logout device profile, you cannot delete it. If you want to delete a logout device profile, you must change it from a logout device profile and configure another device profile as the logout device profile for that phone. After the user device profile is no longer a logout device profile, you can delete it.

Additional Information

See the [“Related Topics” section on page 75-8](#).

Updating Autogenerated Device Profiles

This section describes how to update an autogenerated device profile. You can modify the autogenerated device profile but not delete it or change the profile name.

Before You Begin

Make sure that the autogenerated device profile(s) are configured before proceeding with the steps. See the [“Configuring Cisco Unified IP Phones” section on page 70-2](#) and the [“Autogenerated Device Profile” section in the *Cisco Unified CallManager Features and Services Guide*](#) for more information.

Procedure

-
- Step 1** Locate the autogenerated device profile that you want to update. See the [“Finding a Device Profile” section on page 75-2](#).
- Step 2** From the Autogenerated Device Profile Configuration window, make the desired changes to the autogenerated device profile; then, click **Save**.

Refer to [Configuring a New User Device Profile, page 75-2](#), for field descriptions, except for the following variations:

- To configure a SUBSCRIBE Calling Search Space, choose a SUBSCRIBE calling search space (for Presence feature only) from the drop-down list box. The SUBSCRIBE calling search space determines how Cisco Unified CallManager routes presence requests that come from phones with this autogenerated device profile. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for phones with this autogenerated device profile.

If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE Calling Search Space defaults to None.

For information on how to configure a calling search space, see the [“Calling Search Space Configuration” section on page 43-1](#)

- To configure a Presence Group, choose a Presence Group for the autogenerated device profile (for Presence feature only) from the drop-down list box. This group specifies the destinations that the phone with this autogenerated device profile can monitor.

Presence authorization works with presence groups to allow or block presence requests between groups. Refer to the [“Presence”](#) chapter in the *Cisco Unified CallManager Features and Services Guide* for information about configuring permissions between groups and how presence works with extension mobility.

- To add or change BLF/SpeedDial buttons for monitoring directory numbers or SIP URIs, refer to the [“Presence”](#) chapter in the *Cisco Unified CallManager Features and Services Guide*

The changes that you made should now appear in this autogenerated device profile.



Note You must log out of a device for changes to an autogenerated device profile to take effect.

Additional Information

See the [“Related Topics” section on page 75-8](#).

Configuring New Directory Numbers for Autogenerated Device Profiles

Before You Begin

Make sure that the following prerequisites are met before proceeding with the steps:

- Make sure that the autogenerated device profile(s) are configured before proceeding with the steps. See the [“Configuring Cisco Unified IP Phones” section on page 70-2](#) for more information.
- You must add new directory numbers for an autogenerated device profile from the Autogenerated Device Profile Configuration window. See the [“Finding a Device Profile” section on page 75-2](#) for more information.

Procedure

-
- Step 1** From the Autogenerated Device Profile Configuration window, choose the line on which you want to add a new DN, from the directory number list on the left side of the window.
- The Directory Number Configuration window displays. For information on configuring directory numbers, see the [“Directory Number Configuration Overview” section on page 49-1](#).
- Step 2** Enter the appropriate settings as described in the [“Directory Number Configuration Settings” section on page 49-6](#).

Step 3 Click **Save**.

The window refreshes and displays the settings that you configured.



Note You can also update, delete, and restart devices from the Directory Number Configuration window by clicking the corresponding buttons for these functions. Deleting a directory number removes it from the line, and you cannot undo this action.

Step 4 Return to the Autogenerated Device Profile window by clicking the Configure Device Profile link.

The new directory number should appear on the appropriate line in the list on the left side of the window.



Note When you update the configuration settings for a phone, if an autogenerated device profile has a different default setting than the phone, the setting of the device profile gets overwritten when you choose <User Current Device Setting> as the logout device profile from the Phone Configuration web window.



Note Set the value of the Synchronization Between Auto Device Profile and Phone Configuration enterprise parameter to True (default). This ensures that, when a phone gets updated, the autogenerated device profile also gets updated.

Additional Information

See the [“Related Topics”](#) section on page 75-8.

Related Topics

- [Finding a Device Profile, page 75-2](#)
- [Configuring a New User Device Profile, page 75-2](#)
- [Deleting a User Device Profile, page 75-5](#)
- [Updating Autogenerated Device Profiles, page 75-6](#)

Directory Numbers

- [Directory Number Configuration Overview, page 49-1](#)
- [Directory Number Configuration Settings, page 49-6](#)

Presence

- [Presence, Cisco Unified CallManager Features and Services Guide](#)



Phone Button Template Configuration

Cisco Unified CallManager includes several default phone button templates. When adding phones, you can assign one of these templates to the phones or create a new template.

Creating and using templates provides a fast way to assign a common button configuration to a large number of phones. For example, if users in your company do not use the conference feature, you can create a template that reassigns this button to a different feature, such as speed dial.

Make sure that all phones have at least one line assigned. Normally, this is button 1. You can assign additional lines to a phone, depending on the Cisco IP Phone model. Phones also generally have several features, such as speed dial and call forward, that are assigned to the remaining buttons.

Finding a Phone Button Template

Because you may have several phone button templates in your network, Cisco Unified CallManager Administration lets you locate specific phone button templates on the basis of specific criteria. Use the following procedure to locate phone button templates.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your phone button template search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your phone button template search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Device > Device Settings > Phone Button Template**.

The Find and List Phone Button Templates window displays. Use the three drop-down list boxes to search for a phone button template.

Step 2 From the Find Phone Button Template where Phone Button Template drop-down list box, choose one of the following criteria:

- begins with
- contains

- ends with
- is exactly
- is empty
- is not empty

From the and where Phone Button Template is drop-down list box, choose one of the following criteria:

- Both
- Standard
- Non-Standard

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Tip To find all phone button templates that are registered in the database, click **Find** without entering any search text.

A list of discovered phone button templates displays by the phone button template Name.

Step 4 From the list of records, click the phone button template name that matches your search criteria. The window displays the phone button template that you choose.

Additional Topics

See the [“Related Topics” section on page 76-6](#).

Configuring Phone Button Templates

Cisco Unified CallManager includes default templates for each Cisco Unified IP Phone model. When adding phones, you can assign one of these templates to the phone or create a template of your own.

You can make changes to the custom, nonstandard templates that you created, and you can change the label of the custom phone button template. You cannot change the function of the buttons in the default templates.

You can update a custom, nonstandard phone button template to add or remove features, add or remove lines and speed dials, or assign features, lines, and speed dials to different buttons on the phone. You can change the button labels in the default phone button templates, but you cannot change the function of the buttons in the default templates. If you update a phone template, be sure to inform affected users of the changes.

Use the following procedures to add, rename, update custom, nonstandard templates, or to add, remove features, lines or speed dials.

If you create a template for a phone (Cisco Unified IP Phone model 7960), you can change the default template for that phone during auto-registration. See the [“Updating Device Defaults” section on page 72-1](#).

Before You Begin

If you are creating a custom, nonstandard phone button template, refer to the guidelines for creating new phone button templates. See the [“Guidelines for Customizing Phone Button Templates”](#) section in the *Cisco Unified CallManager System Guide*.

Procedure

Step 1 Choose **Device > Device Settings > Phone Button Template**.

The Find and List Phone Button Templates window displays.

Step 2 Perform one of the followings tasks:

- To rename an existing phone button template, locate the appropriate phone button template as described in [“Finding a Phone Button Template”](#) section on page 76-1. The Phone Button Template Configuration page displays. In the Button Template Name field, enter the new name. Click **Save**. The template redisplay with the new name.



Note Renaming a template does not affect the phones that use that template. All Cisco IP Phones that use this template continue to use this template after it is renamed. You can rename only phone button templates that display a check box in the left column. All other phone button templates serve as standard, read-only templates.

- To add a new phone button template, click the **Add New** button. The Phone Button Template Configuration window displays. Continue with [Step 3](#).
- To update an existing phone button template, locate the appropriate phone as described in [“Finding a Phone Button Template”](#) section on page 76-1. From the list of matching records, choose the phone button template that you want to update. The Phone Button Template Configuration window displays. Continue with [Step 4](#).



Note When you update a template, the change affects all phones that use the template. You can update only phone button templates that display a check box in the left column. All other phone button templates serve as standard, read-only templates. After updating the template, you must restart devices that are using the template by clicking **Restart Devices**

Step 3 From the Phone Button Template drop-down list box, choose a template and click **Copy** to create a new template.

The new template exactly duplicates the existing template. You must assign a new name for the new template. Update this new template if you want it to differ from the original.

Step 4 Update the appropriate settings as described in [Table 76-1](#).

Step 5 Click **Save**.

Additional Topics

See the [“Related Topics”](#) section on page 76-6.

Configuring a Cisco IP Phone 7914 Expansion Module Phone Button Template

You can create a phone button template for the Cisco IP Phone 7914 Expansion Module by using the Standard Cisco IP Phone model 7960 phone button template as described in the following procedure.

Procedure

-
- Step 1** Find the phone button template by using the procedure in the [“Finding a Phone Button Template”](#) section on page 76-1.
 - Step 2** From the list of matching records, locate the Standard 7960 (for SCCP or SIP) phone button template and click the **Copy** icon.
 - Step 3** For Button Template Name, enter a unique name for the phone button template (for example, 7914 Expansion Module).
 - Step 4** Click **Save**.
 - Step 5** Update the appropriate settings for Feature and Label as described in [Table 76-1](#) (the button template name that you just created will already display).
 - Step 6** Click **Save**.
-

Additional Topics

See the [“Related Topics”](#) section on page 76-6.

Phone Button Template Configuration Settings

[Table 76-1](#) describes the phone button template configuration settings.

Table 76-1 Phone Button Template Configuration Settings

Field	Description
Phone Button Template Information	
Button Template Name	Enter a unique name that Cisco Unified CallManager uses to identify the template.
Button Information	
Feature	Choose the function of the phone button that you want to specify in the template. Available functions include Speed Dial, Line, None, Privacy, and Service URL. Note You cannot change the function of buttons in default phone button templates.
Label	Enter a description of the button.

Additional Topics

See the [“Related Topics”](#) section on page 76-6.

Deleting a Phone Button Template

Use this procedure to delete a phone button template.

Before You Begin

You can delete phone templates that are not currently assigned to any phone in your system. You cannot delete a template that is assigned to one or more devices or device profiles or the default template for a model (which is specified in the Device Defaults Configuration window).

To find out which devices are using the phone button template, choose **Dependency Records** link from the Related Links drop-down list box in the Phone Button Template Configuration window and click **Go**. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#). If you try to delete a phone button template that is in use, Cisco Unified CallManager displays a message. Before deleting a phone button template that is currently in use, you must perform either or both of the following tasks:

- Assign a different phone button template to any devices that are using the phone button template that you want to delete. See the [“Deleting a Phone” section on page 70-5](#).
- Delete the devices that are using the phone button template that you want to delete. See the [“Deleting a Phone” section on page 70-5](#).

Procedure

Step 1 Find the phone button template by using the procedure in the [“Finding a Phone Button Template” section on page 76-1](#).

Step 2 From the list of matching records, choose the phone button template that you want to delete.



Note You can delete only phone button templates that display a check box in the left column. All other phone button templates serve as standard, read-only templates.

The Phone Button Template Configuration window displays.

Step 3 Click **Delete**.



Note You can delete multiple nonstandard phone button templates from the Find and List Phone Button Templates window by checking the check boxes next to the appropriate phone button templates and clicking **Delete Selected**. You can delete all phone button templates in the window by clicking **Select All** and **Delete Selected**. You can delete only phone button templates that display a check box in the left column. All other phone button templates serve as standard, read-only templates.

A message verifies that you want to delete the template.

Step 4 To delete the template, click **OK**.

A message verifies that the template was deleted.

Step 5 To continue, click **OK**.

Additional Topics

See the “Related Topics” section on page 76-6.

Related Topics

- [Updating Device Defaults, page 72-1](#)
- [Finding a Phone Button Template, page 76-1](#)
- [Configuring Phone Button Templates, page 76-2](#)
- [Configuring a Cisco IP Phone 7914 Expansion Module Phone Button Template, page 76-4](#)
- [Phone Button Template Configuration Settings, page 76-4](#)
- [Deleting a Phone Button Template, page 76-5](#)
- [Cisco Unified IP Phones](#), *Cisco Unified CallManager System Guide*
- [Guidelines for Customizing Phone Button Templates](#), *Cisco Unified CallManager System Guide*
- [Phone Button Templates](#), *Cisco Unified CallManager System Guide*
- [Cisco Unified IP Phone Configuration, page 70-1](#)
- [Phone Configuration Checklist](#), *Cisco Unified CallManager System Guide*



Softkey Template Configuration

Softkey template configuration allows the administrator to manage softkeys that the Cisco IP Phones (such as model 7960) support. Cisco Unified CallManager supports two types of softkey templates: standard and nonstandard. Applications that support softkeys can have one or more standard softkey templates that are associated with them; for example, Cisco Unified CallManager has the Standard Feature and the Standard User softkey templates that are associated with it. You cannot modify standard softkey templates.

The administrator can copy, update, or delete nonstandard softkey templates by using softkey template configuration.

The following sections provide details about softkey template configuration:

- [Finding a Softkey Template, page 77-1](#)
- [Adding Nonstandard Softkey Templates, page 77-2](#)
- [Adding Application Softkeys to Nonstandard Softkey Templates, page 77-3](#)
- [Configuring Softkey Positions in a Nonstandard Softkey Template, page 77-4](#)
- [Modifying Softkey Templates, page 77-5](#)
- [Assigning Softkey Templates to IP Phones, page 77-8](#)

Finding a Softkey Template

Because you might have several softkey templates in your network, Cisco Unified CallManager Administration lets you locate specific softkey templates on the basis of specific criteria. Use the following procedure to locate softkey templates.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your softkey template search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your softkey template search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Device > Device Settings > Softkey Template**.

The Find and List Softkey Templates window displays. Use the three drop-down list boxes to search for a softkey template.

Step 2 From the first Find softkey templates where drop-down list box, choose one of the following criteria:

- Name
- Description



Note The criterion that you choose in this drop-down list box specifies how the list of softkey templates that your search generates will be sorted. For example, if you choose Description, the Description column will display as the left column of the results list.

From the second Find softkey templates where drop-down list box, choose one of the following criteria:

- begins with
- contains
- ends with
- is exactly
- is empty
- is not empty

From the third Find softkey templates where drop-down list box, choose one of the following criteria:

- Both
- Standard
- Non-Standard

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Tip To find all softkey templates that are registered in the database, click **Find** without entering any search text.

A list of discovered softkey templates displays by

- Softkey Template Name
- Description

Step 4 From the list of records, click the Softkey Template Name or the Description that matches your search criteria.

The window displays the softkey template that you choose.

Additional Information

See the [“Related Topics”](#) section on page 77-8.

Adding Nonstandard Softkey Templates

Cisco Unified CallManager includes standard softkey templates for call processing and applications. When creating custom, nonstandard softkey templates, copy the standard templates and make modifications as required.

Procedure

-
- Step 1** Choose **Device > Device Settings > Softkey Template**.
The Find and List Softkey Templates window displays.
- Step 2** Click the **Add New**.
The Softkey Template Configuration window displays.
- Step 3** From the drop-down list box, choose a softkey template and click the **Copy** button to create a new template.
The Softkey Template Configuration window redisplay and contains the fields in which to enter a unique softkey template name, description, and application that are associated with the soft keys.
- Step 4** In the Softkey Template Name field, enter a unique name to identify the softkey template.
- Step 5** Enter a description that describes use of the template.
- Step 6** Click the **Save** button.
The standard template gets copied, and the Softkey Template Configuration window redisplay.
- Step 7** If you want to add additional application softkeys to the nonstandard softkey template, see the [“Adding Application Softkeys to Nonstandard Softkey Templates”](#) section on page 77-3.
- Step 8** To configure the positions of the softkeys on the Cisco Unified IP Phone LCD screen, see the [“Configuring Softkey Positions in a Nonstandard Softkey Template”](#) section on page 77-4.
- Step 9** To save your configuration, click the **Save** button.
-

Additional Information

See the [“Related Topics”](#) section on page 77-8.

Adding Application Softkeys to Nonstandard Softkey Templates

Cisco Unified CallManager includes standard softkey templates for call processing and applications. When creating custom, nonstandard softkey templates, copy the standard templates and make modifications as required. This procedure describes how to add application softkeys to a nonstandard softkey template that you created.

Procedure

-
- Step 1** Find the softkey template by using the procedure in the [“Finding a Softkey Template”](#) section on page 77-1.
- Step 2** From the list of matching records, choose the softkey template to which you want to add application softkeys.



Note You can modify only softkey templates that display a check box in the left column. All other softkey templates are standard, read-only templates.

The Softkey Template Configuration window displays.

- Step 3** To add additional application softkeys to the nonstandard softkey template, click the **Add Application** button.
- The Add Application window displays.
- Step 4** Choose the standard softkey template that you want added to the nonstandard softkey template.
- Step 5** Click the **Insert** button and click **Close**.
- The softkeys that are associated with the standard softkey template that you chose get added at the end of the nonstandard softkey template. Duplicate softkeys automatically get deleted. If the number of softkeys for a particular call state exceeds 16, the optional softkeys for that call state will be removed (from the end to the front). If after the optional softkeys are removed, the number of softkeys still exceeds 16, a message displays.
- Step 6** To save your softkey set configuration, click the **Save** button.
- Step 7** To make the updates of the softkey template take effect on the phone, click the **Restart Devices** button.
-

Additional Information

See the [“Related Topics” section on page 77-8](#).

Configuring Softkey Positions in a Nonstandard Softkey Template

Cisco Unified CallManager includes standard softkey templates for call processing and applications. When creating custom, nonstandard softkey templates, copy the standard templates and make modifications as required. This procedure describes how to configure softkey positions for each call state in a nonstandard softkey template that you created.

Procedure

- Step 1** Find the softkey template by using the procedure in the [“Finding a Softkey Template” section on page 77-1](#).
- Step 2** From the list of matching records, choose the softkey template in which you want to configure softkey positions.



Note You can modify only softkey templates that display a check box in the left column. All other softkey templates are standard, read-only templates.

The Softkey Template Configuration window displays.

- Step 3** To configure the positions of the softkeys on the Cisco Unified IP Phone LCD screen, choose **Configure Softkey Layout** from the Related Links drop-down list box.
- The Softkey Layout Configuration window displays. The Select a Call State to Configure drop-down list box lists each Cisco Unified CallManager call state for an IP phone.
- Step 4** To configure the softkey positions for a call state, choose the call state from the Select a Call State to Configure drop-down list box.

The Softkey Layout Configuration window redisplay, and the fields Unselected Softkeys and Selected Softkeys display softkeys that are applicable to the call state that you chose.

**Tip**

To create a relative place holder for a softkey, add the Undefined softkey. This allows the softkey that you added to occupy the same softkey position in all call states.

- Step 5** To move softkeys from one list to the other, use the right and left arrows.
- Step 6** To rearrange the positions of the Selected Softkeys, use the up and down arrows.
- Step 7** To save your softkey set configuration, click the **Save** button.
- Step 8** To return to the Softkey Template Configuration window, choose the Softkey Template Configuration link from the Related Links drop-down list box in the top, right-hand corner.
- Step 9** To save your configuration, click the **Save** button.
- Step 10** To make the updates of the softkey template take effect on the phone, click the **Restart Devices** button.

Additional Information

See the [“Related Topics” section on page 77-8](#).

Modifying Softkey Templates

You can make changes to custom, nonstandard softkey templates that you created:

- [Renaming a Softkey Template, page 77-5](#)
- [Deleting a Softkey Template, page 77-6](#)
- [Updating a Softkey Template, page 77-7](#)

Additional Information

See the [“Related Topics” section on page 77-8](#).

Renaming a Softkey Template

Use this procedure to rename a nonstandard softkey template that you created.

Procedure

- Step 1** Find the softkey template by using the procedure in the [“Finding a Softkey Template” section on page 77-1](#).
- Step 2** From the list of matching records, choose the softkey template that you want to rename.

**Note**

You can rename only softkey templates that display a check box in the left column. All other softkey templates are standard, read-only templates.

The Softkey Template Configuration page displays.

Step 3 In the Softkey Template Name field, enter the new name.

Step 4 Click the **Save** button.

The Softkey Template Configuration window redisplay with the new softkey template name.

Additional Information

See the [“Related Topics” section on page 77-8](#).

Deleting a Softkey Template

Use this procedure to delete a nonstandard softkey template that you created.

Before You Begin

You cannot delete a nonstandard softkey template that is currently assigned to a device or device pool. To find out which devices and device pools are using the nonstandard softkey template, choose **Dependency Records** from the Related Links drop-down list box in the Softkey Configuration window and click **Go**. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#). If you try to delete a nonstandard softkey template that is in use, Cisco Unified CallManager displays a message. Before deleting a nonstandard softkey template that is currently in use, you must perform either or both of the following tasks:

- Assign a different softkey template to any devices or device pools that are using the nonstandard softkey template that you want to delete. See the [“Deleting a Phone” section on page 70-5](#).
- Delete the devices that are using the nonstandard softkey template that you want to delete. See the [“Deleting a Phone” section on page 70-5](#).

Procedure

Step 1 Find the softkey template by using the procedure in the [“Finding a Softkey Template” section on page 77-1](#).

Step 2 From the list of matching records, choose the softkey template that you want to delete.



Note You can delete only softkey templates that display a check box in the left column. All other softkey templates represent standard, read-only templates.

The Softkey Template Configuration window displays.

Step 3 Click the **Delete** button.



Note You can delete multiple softkey templates from the Find and List Softkey Templates window by checking the check boxes next to the appropriate softkey templates and clicking **Delete Selected**. You can delete all softkey templates in the window by clicking **Select All** and then clicking **Delete Selected**.

A message verifies that you want to delete the template.

Step 4 Click the **OK** button.

The Softkey Template Configuration window redisplay with the softkey template deleted.

Additional Information

See the [“Related Topics” section on page 77-8](#).

Updating a Softkey Template

Use this procedure to update a nonstandard softkey template that you created. You can update the template name, description, application softkeys that are supported, and the softkey layout.

Procedure

Step 1 Find the softkey template by using the procedure in the [“Finding a Softkey Template” section on page 77-1](#).

Step 2 From the list of matching records, choose the softkey template that you want to update.



Note You can update only softkey templates that display a check box in the left column. All other softkey templates represent standard, read-only templates.

The Softkey Template Configuration window displays.

Step 3 Update the settings that you want changed (such as adding an application softkey set or the softkey layout). See the [“Adding Application Softkeys to Nonstandard Softkey Templates” section on page 77-3](#) and the [“Configuring Softkey Positions in a Nonstandard Softkey Template” section on page 77-4](#).

Step 4 Click the **Save** button.

The Softkey Template Configuration window redisplay with the softkey template updated.



Note After making updates to a softkey template, you must restart devices that are using the template.

Step 5 To apply the updated softkey template, click the **Restart Devices** button.

Additional Information

See the [“Related Topics” section on page 77-8](#).

Assigning Softkey Templates to IP Phones

You can assign softkey templates to IP Phones when the phones are configured. You can assign standard and nonstandard softkey templates. Two ways to assign a softkey template to a phone exist:

- Assign the softkey template to a device pool (one that you create or the default) and then assign the device pool to the phone in the Phone Configuration window.
- Assign the softkey template to the phone in the softkey template field in the Phone Configuration window.

For more information about configuring device pools and phones, refer to the [“Device Pool Configuration” section on page 9-1](#) and the [“Configuring Cisco Unified IP Phones” section on page 70-2](#).

Related Topics

- [Finding a Softkey Template, page 77-1](#)
- [Adding Nonstandard Softkey Templates, page 77-2](#)
- [Modifying Softkey Templates, page 77-5](#)
- [Renaming a Softkey Template, page 77-5](#)
- [Deleting a Softkey Template, page 77-6](#)
- [“Assigning Softkey Templates to IP Phones” section on page 77-8](#)
- [Softkey Templates](#), *Cisco Unified CallManager System Guide*



Cisco Unified IP Phone Services Configuration

Using Cisco Unified CallManager Administration, you define and maintain the list of Cisco Unified IP Phone Services to which users can subscribe at their site. Cisco Unified IP Phone Services comprise XML applications that enable the display of interactive content with text and graphics on Cisco Unified IP Phones 7970, 7960, 7940, 7912, and 7905.



Note

Cisco Unified IP Phones 7912 and 7905 only support text-based XML applications.

Cisco Unified CallManager provides sample Cisco Unified IP Phone Services applications. You can also create customized Cisco Unified IP Phone applications for your site.

After you configure the list of services, you can add services to the phones in the database and assign them to phone buttons. In Cisco Unified CallManager Administration, you can view and modify settings for phones and device profiles. Users can log on to the Cisco Unified IP Phone User Options application and subscribe to these services for their Cisco Unified IP Phones.

This section covers the following topics:

- [Finding a Cisco Unified IP Phone Service, page 78-2](#)
- [Configuring a Cisco Unified IP Phone Service, page 78-3](#)
- [Cisco Unified IP Phone Service Configuration Settings, page 78-4](#)
- [Deleting a Cisco Unified IP Phone Service, page 78-5](#)
- [Configuring a Cisco Unified IP Phone Service Parameter, page 78-5](#)
- [Cisco Unified IP Phone Service Parameter Settings, page 78-7](#)
- [Deleting a Cisco Unified IP Phone Service Parameter, page 78-7](#)
- [Adding a Cisco Unified IP Phone Service to a Phone Button, page 78-8](#)
- [Cisco Unified IP Phone Services, *Cisco Unified CallManager System Guide*](#)

Finding a Cisco Unified IP Phone Service

Because you might have several Cisco Unified IP Phone Services in your network, Cisco Unified CallManager lets you locate specific Cisco Unified IP Phone Services on the basis of specific criteria. Use the following procedure to locate Cisco Unified IP Phone Services.

**Note**

During your work in a browser session, Cisco Unified CallManager Administration retains your Cisco Unified IP Phone Service search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your Cisco Unified IP Phone Service search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Device >Device Settings > Phone Services**.

The Find and List IP Phone Services window displays. Use the two drop-down list boxes to search for a Cisco Unified IP Phone Service.

Step 2 From the first Find Service where drop-down list box, choose one of the following criteria:

- IP Phone Service
- Description

From the second Find Service where drop-down list box, choose one of the following criteria:

- begins with
- contains
- is exactly
- ends with
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.

**Tip**

To find all Cisco Unified IP Phone Services that are registered in the database, click **Find** without entering any search text.

A list of discovered Cisco Unified IP Phone Services displays by

- IP Phone Service name
- Description

**Note**

You can delete multiple Cisco Unified IP Phone services from the Find and List IP Phone Services window by checking the check boxes next to the appropriate Cisco Unified IP Phone Services and clicking **Delete Selected**. You can delete all Cisco Unified IP Phone Services in the window by clicking **Select All** and then clicking **Delete Selected**.

- Step 4** From the list of records, click the Cisco Unified IP Phone Service name or description that matches your search criteria.

The window displays the Cisco Unified IP Phone Service that you choose.

Additional Information

See the [“Related Topics” section on page 78-8](#).

Configuring a Cisco Unified IP Phone Service

Perform the following steps to add or update a Cisco Unified IP Phone Service.



Caution

Do not put Cisco Unified IP Phone Services on any Cisco Unified CallManager server at your site or any server that is associated with Cisco Unified CallManager, such as the TFTP server or directory database publisher server. This precaution eliminates the possibility that errors in a Cisco Unified IP Phone Service application will have an impact on Cisco Unified CallManager performance or interrupt call-processing services.

Procedure

- Step 1** Choose **Device >Device Settings > Phone Services**.
- The Find and List IP Phone Services window displays.
- Step 2** Perform one of the followings tasks:
- To add a Cisco Unified IP Phone Service, click the **Add New** button. The Cisco Unified IP Phone Services Configuration window displays. Continue with [Step 3](#).
 - To update an existing Cisco Unified IP Phone Service (for example, to change the service URL or other information), locate the appropriate Cisco Unified IP Phone service as described in [“Finding a Cisco Unified IP Phone Service” section on page 78-2](#). Click the name of the Cisco Unified IP Phone Service that you want to update and continue with [Step 3](#).
- Step 3** Enter the appropriate settings as described in [Table 78-1](#).
- Step 4** Click **Save**.
- You can add, update, or delete parameters as needed as described in [“Configuring a Cisco Unified IP Phone Service Parameter” section on page 78-5](#) and [“Deleting a Cisco Unified IP Phone Service Parameter” section on page 78-7](#).
- Step 5** To apply the changes, update the Cisco Unified IP Phone Services Configuration window:
- If the service was modified after subscriptions existed, click **Update Subscriptions** to rebuild all user subscriptions. You must update subscriptions if you changed the service URL, removed a phone service parameter, or changed the Parameter Name for a phone service parameter.

**Note**

If you change the service URL, remove a Cisco Unified IP Phone Service parameter, or change the name of a phone service parameter for a phone service to which users are subscribed, be sure to click **Update Subscriptions** to update all currently subscribed users with the changes. If you do not do so, users must resubscribe to the service to rebuild the URL correctly.

- If the service is new and you do not need to rebuild user subscriptions, click **Save**.

Additional Information

See the [“Related Topics” section on page 78-8](#).

Cisco Unified IP Phone Service Configuration Settings

[Table 78-1](#) describes the Cisco Unified IP Phone Service configuration settings. See [Table 78-2](#) for Cisco Unified IP Phone Service configuration settings. For more information about related procedures, see the [“Related Topics” section on page 78-8](#).

Table 78-1 *Cisco Unified IP Phone Service Configuration Settings*

Field	Description
Service Information	
Service Name	Enter the name of the service as it will display on the menu of available services in the Cisco Unified IP Phone User Options application. Enter up to 32 characters for the service name.
Service Name (ASCII Format)	Enter the name of the service to display if the phone cannot display Unicode.
Service Description	Enter a description of the content that the service provides.
Service URL	Enter the URL of the server where the Cisco Unified IP Phone Services application is located. Make sure that this server remains independent of the servers in your Cisco Unified CallManager cluster. Do not specify a Cisco Unified CallManager server or any server that is associated with Cisco Unified CallManager (such as a TFTP server or directory database publisher server). For the services to be available, the phones in the Cisco Unified CallManager cluster must have network connectivity to the server.

Deleting a Cisco Unified IP Phone Service

Perform the following steps to delete a Cisco Unified IP Phone Service.

Before You Begin

When you delete a Cisco Unified IP Phone Service, Cisco Unified CallManager removes all service information, user subscriptions, and user subscription data from the database. To find out which devices are using the Cisco Unified IP Phone Service, from the Cisco Unified IP Phone Service Configuration window, choose **Dependency Records** from the Related Records drop-down list box and click **Go**. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#). If you try to delete a Cisco Unified IP Phone Service that is in use, Cisco Unified CallManager displays an error message. Before deleting a Cisco Unified IP Phone Service that is currently in use, you must perform either or both of the following tasks:

- Assign a different Cisco Unified IP Phone Service to any devices that are using the Cisco Unified IP Phone Service that you want to delete. See the [“Deleting a Phone” section on page 70-5](#).
- Delete the devices that are using the Cisco Unified IP Phone Service that you want to delete. See the [“Deleting a Phone” section on page 70-5](#).

Procedure

-
Step 1	Find the Cisco Unified IP Phone Service by using the procedure in the “Finding a Cisco Unified IP Phone Service” section on page 78-2 .
Step 2	Click the name of the IP Phone Service that you want to delete. The Cisco Unified IP Phone Services Configuration window displays.
Step 3	Click Delete . You receive a message that asks you to confirm the deletion.
Step 4	Click OK . The window refreshes, and the Cisco Unified IP Phone Service gets deleted from the database.
-

Additional Information

See the [“Related Topics” section on page 78-8](#).

Configuring a Cisco Unified IP Phone Service Parameter

Use the following procedure to add and configure or update Cisco Unified IP Phone Service parameters. Add the phone service before you configure parameters. Refer to the documentation for the individual Cisco Unified IP Phone Service for specific information about whether the service uses parameters, how those parameters should be configured, and whether you should provide optional parameter definitions.

Procedure

-
- Step 1** Find the Cisco Unified IP Phone service by using the procedure in the [“Finding a Cisco Unified IP Phone Service”](#) section on page 78-2.
- Step 2** From the Cisco Unified IP Phone Services list, choose the service to which you want to add parameters or update existing parameters.
- The Cisco Unified IP Phone Services Configuration window displays.
- Step 3** Perform one of the followings tasks:
- To add a new phone service parameter, click the **New** button to the right of the Parameters list box. The Configure Cisco Unified IP Phone Service Parameter window displays. Continue with [Step 4](#).
 - To update an existing parameter, choose the name of the parameter that you want to update in the Parameters list box. Click **Edit** and continue with [Step 4](#).
- Step 4** Enter the appropriate settings as described in [Table 78-2](#).
- To add the new parameter, click **Save**. To add additional parameters, if needed, click **Add New** in the Configure Cisco Unified IP Phone Service Parameter window and repeat [Step 3](#) and [Step 4](#). To add the last parameter, click **Save and Close**.
- To apply the changes to the updated parameters, click **Save**, or to apply the changes and close the window, click **Save and Close**.
- Step 5** To apply the changes, update the Cisco Unified IP Phone Services Configuration window:
- If the service was modified after subscriptions existed, click **Update Subscriptions** to rebuild all user subscriptions. You must update subscriptions if you changed the service URL, removed a phone service parameter, or changed the name for a phone service parameter.



Note

If you remove a Cisco Unified IP Phone Service parameter or change the parameter name of a phone service for a phone service to which users are subscribed, be sure to click **Update Subscriptions** to update all currently subscribed users with the changes. If you do not do so, users must resubscribe to the service to rebuild the URL correctly.

- If the service is new and you do not need to rebuild user subscriptions, click **Save**.
-

Additional Information

See the [“Related Topics”](#) section on page 78-8.

Cisco Unified IP Phone Service Parameter Settings

Table 78-2 describes the Cisco Unified IP Phone Service parameter settings. For more information about related procedures, see the “[Related Topics](#)” section on page 78-8.

Table 78-2 Cisco Unified IP Phone Service Parameter Settings

Field	Description
Service Parameter Information	
Parameter Name	Enter the exact query string parameter to use when you build the subscription URL; for example, symbol.
Parameter Display Name	Enter a descriptive parameter name to display to the user in the Cisco Unified IP Phone User Options application; for example, Ticker Symbol.
Default Value	Enter the default value for the parameter. This value displays to the user when a service is being subscribed to for the first time; for example, CSCO.
Parameter Description	Enter a description of the parameter. The user can access the text that is entered here while the user is subscribing to the service. The parameter description should provide information or examples to help users input the correct value for the parameter.
Parameter is Required	If the user must enter data for this parameter before the subscription can be saved, check the Parameter is Required check box.
Parameter is a Password (mask contents)	You can mask entries in the Cisco Unified IP Phone User Options application, so asterisks display rather than the actual user entry. You may want to do this for parameters such as passwords that you do not want others to be able to view. To mask parameter entry, check the Parameter is a Password (mask contents) check box in the Configure Cisco Unified IP Phone Service Parameter window in Cisco Unified CallManager Administration.

Deleting a Cisco Unified IP Phone Service Parameter

Perform the following steps to delete a Cisco Unified IP Phone Service parameter.

**Note**

If you remove a phone service parameter or modify the Parameter Name of a phone service parameter for a phone service to which users are subscribed, you must click **Update Subscriptions** to update all currently subscribed users with the changes. If you do not do so, users must resubscribe to the service to rebuild the URL correctly.

Procedure

- Step 1** Find the Cisco Unified IP Phone Service by using the procedure in the “[Finding a Cisco Unified IP Phone Service](#)” section on page 78-2.
- Step 2** From the Cisco Unified IP Phone Services list, choose the phone service whose parameters you want to delete.

- Step 3** In the Parameters list box, choose the name of the parameter that you want to delete.
- Step 4** Click **Delete**.
- You receive a message that asks you to confirm the deletion.
- Step 5** To confirm the deletion, click **OK**.
- Step 6** To apply the changes, update the Cisco Unified IP Phone Services Configuration window:
- If the service was modified after subscriptions existed, click **Update Subscriptions** to rebuild all user subscriptions. You must update subscriptions if you changed the service URL, removed a phone service parameter, or changed the Parameter Name for a phone service parameter.
 - If the service is new and you do not need to rebuild user subscriptions, click **Save**.
-

Additional Information

See the [“Related Topics” section on page 78-8](#).

Adding a Cisco Unified IP Phone Service to a Phone Button

In addition to adding a Cisco Unified IP Phone Service, so it is available to users on their phones, you can assign the service to a phone button that is configured as a service URL. This gives the user one-button access to the service without using the services button on the IP phone.

Perform the following steps to add a service to a service URL button:

Procedure

-
- Step 1** Add the service to Cisco Unified CallManager (see [Configuring a Cisco Unified IP Phone Service, page 78-3](#)).
- Step 2** Customize a phone button template by configuring a Service URL button (refer to the [“Configuring Phone Button Templates” section on page 76-2](#)).
- Step 3** Add the customized phone button template to the phone (refer to the [“Configuring Cisco Unified IP Phones” section on page 70-2](#)).
- Step 4** Subscribe the service to the phone (refer to the [“Configuring Cisco Unified IP Phone Services” section on page 70-24](#)).
- Step 5** Add the service URL to a phone button (refer to the [“Configuring Service URL Buttons” section on page 70-27](#)).
-

Related Topics

- [Finding a Cisco Unified IP Phone Service, page 78-2](#)
- [Configuring a Cisco Unified IP Phone Service, page 78-3](#)
- [Cisco Unified IP Phone Service Configuration Settings, page 78-4](#)
- [Deleting a Cisco Unified IP Phone Service, page 78-5](#)

- [Configuring a Cisco Unified IP Phone Service Parameter, page 78-5](#)
- [Cisco Unified IP Phone Service Parameter Settings, page 78-7](#)
- [Deleting a Cisco Unified IP Phone Service Parameter, page 78-7](#)
- [Adding a Cisco Unified IP Phone Service to a Phone Button, page 78-8](#)
- [Cisco Unified IP Phone Services, *Cisco Unified CallManager System Guide*](#)



SIP Profile Configuration

A SIP profile comprises the set of SIP attributes that are associated with SIP trunks and SIP endpoints. SIP profiles include information such as name, description, timing, retry, call pickup URI, and so on. The profiles contain some standard entries that cannot be deleted or changed.

Use the following topics to configure and locate SIP profiles:

- [Finding SIP Profiles, page 79-1](#)
- [Configuring SIP Profiles, page 79-2](#)
- [SIP Profile Configuration Settings, page 79-2](#)
- [Deleting SIP Profiles, page 79-8](#)
- [Resetting a SIP Profile, page 79-9](#)
- [Related Topics, page 79-9](#)

Finding SIP Profiles

This topic describes how to use the Find and List SIP Profile window. The function searches every type of SIP profile against the following categories:

- Profile name
- Description

Procedure

Step 1 Choose **Device > Device Settings > SIP Profile**.

The Find and List SIP Profile window displays.

Step 2 From the drop-down lists, choose your search text for the type of SIP profiles that you want listed and click **Find**.



Note To find all SIP profiles that are registered in the database, click **Find** without entering any text.

The window refreshes and then displays the SIP profiles that match your search criteria.

- Step 3** From the list of records that match your search criteria, choose the SIP profile.
- Step 4** To delete multiple SIP profiles from the Find and List SIP Profiles window, check the check boxes next to the appropriate SIP profiles and click **Delete Selected**. To choose all the SIP profiles in the window, click the **Select All** button and then click **Delete Selected**.

Additional Information

See the [“Related Topics” section on page 79-9](#).

Configuring SIP Profiles

Perform the following procedure to add, copy, or update a SIP profile.

Procedure

- Step 1** Choose **Device > Device Settings > SIP Profile**.
- The Find and List SIP Profile window displays.
- Step 2** Perform one of the followings tasks:
- To copy an existing SIP profile, locate the appropriate SIP profile as described in [“Finding SIP Profiles” section on page 79-1](#), click the **Copy** button next to the SIP profile that you want to copy and continue with [Step 3](#).
 - To add a new SIP profile, click the **Add New** button and continue with [Step 3](#).
 - To update an existing SIP profile, locate the appropriate SIP profile as described in [“Finding SIP Profiles” section on page 79-1](#) and continue with [Step 3](#).
- Step 3** Enter the appropriate settings as described in [Table 79-1](#).
- Step 4** Click **Save**.

Additional Information

See the [“Related Topics” section on page 79-9](#).

SIP Profile Configuration Settings

[Table 79-1](#) describes the available settings in the SIP Profile Configuration window. For more information about related procedures, see the [“Related Topics” section on page 79-9](#).

Table 79-1 SIP Profile Configuration Settings

Field	Description
SIP Profile Information	
Name	Enter a name to identify the SIP profile; for example, SIP_7905. The value can include 1 to 50 characters, including alphanumeric characters, dot, dash, and underscores.

Table 79-1 SIP Profile Configuration Settings (continued)

Field	Description
Description	This field identifies the purpose of the SIP profile; for example, SIP for Model 7970.
Default Telephony Event Payload Type	This field specifies the default payload type for RFC2833 telephony event. See RFC 2833 for more information. In most cases, the default value specifies the appropriate payload type. Be sure that you have a firm understanding of this parameter before changing it, as changes could result in DTMF tones not being received or generated. The default value specifies 101 with range from 96 to 127. The value of this parameter affects calls with the following conditions: • The call is an outgoing SIP call from Cisco Unified CallManager. • For the calling SIP trunk, the Media Termination Point Required check box is checked on the SIP Trunk Configuration window.
Redirect by Application	Checking this check box and configuring this SIP Profile on the SIP trunk allows the Cisco Unified CallManager administrator to • Apply a specific calling search space to redirected contacts that are received in the 3xx response. • Apply digit analysis to the redirected contacts to make sure that the call get routed correctly. • Prevent DOS attack by limiting the number of redirection (recursive redirection) that a service parameter can set. • Allow other features to be invoked while the redirection is taking place. Getting redirected to a restricted phone number (such as an international number) means that handling redirection at the stack level will cause the call to be routed instead of being blocked. This represents the behavior you will get if the Redirect by Application check box is unchecked. See the “Redirection” section on page 41-12.
Disable Early Media on 180	By default, Cisco Unified CallManager will signal the calling phone to play local ringback if SDP is not received in the 180 or 183 response. If SDP is included in the 180 or 183 response, instead of playing ringback locally, Cisco Unified CallManager will connect media and the calling phone will play whatever the called device is sending (such as ringback or busy signal). If you do not receive ringback, the device to which you are connecting may be including SDP in the 180 response, but it is not sending any media before the 200OK response. In this case, check this check box to play local ringback on the calling phone and connect the media upon receipt of the 200OK response Note Even though the phone that is receiving ringback is the calling phone, you need the configuration on the called device's profile because it determines the behavior. See the “Use of Early Media” section on page 41-6.

Table 79-1 *SIP Profile Configuration Settings (continued)*

Field	Description
Parameters used in Phone	
Timer Invite Expires (seconds)	This field specifies the time, in seconds, after which a SIP INVITE expires. The Expires header uses this value. Valid values include any positive number; 180 specifies the default.
Timer Register Delta (seconds)	Use this parameter in conjunction with the Timer Register Expires setting. The phone will reregister Timer Register Delta seconds before the registration period ends. The registration period gets determined by the value of the SIP Station Keepalive Interval service parameter. Valid values range from 32767 to 0. Default specifies 5.
Timer Register Expires (seconds)	This field specifies the value that the SIP phone will send in the Expires header of the REGISTER message. Valid values include any positive number; however, 3600 (1 hour) specifies the default value. In the 200OK response to REGISTER, Cisco Unified CallManager will include an Expires header with the configured value of the SIP Station KeepAlive Interval service parameter. This value in the 200OK determines the time, in seconds, after which the registration expires. The phone will refresh the registration Timer Register Delta seconds before the end of this interval.
Timer T1 (msec)	This field specifies the lowest value, in milliseconds, of the retransmission timer for SIP messages. Valid values include any positive number. Default specifies 500.
Timer T2 (msec)	This field specifies the highest value, in milliseconds, of the retransmission timer for SIP messages. Valid values include any positive number. Default specifies 4000.
Retry INVITE	This field specifies the maximum number of times that an INVITE request will be retransmitted. Valid values include any positive number. Default specifies 6.
Retry Non-INVITE	This field specifies the maximum number of times that a SIP message other than an INVITE request will be retransmitted. Valid values include any positive number. Default specifies 10.
Start Media Port	This field designates the start real-time protocol (RTP) port for media. Media port ranges from 16384 to 32766. Default specifies 16384.
Stop Media Port	This field designates the stop real-time protocol (RTP) port for media. Media port ranges from 16384 to 32766. Default specifies 32766.
Call Pickup URI	This URI provides a unique address that the SIP phone will send to Cisco Unified CallManager to invoke the call pickup feature.
Call Pickup Group Other URI	This URI provides a unique address that the SIP phone will send to Cisco Unified CallManager to invoke the call pickup group other feature.
Call Pickup Group URI	This URI provides a unique address that the SIP phone will send to Cisco Unified CallManager to invoke the call pickup group feature.
Meet Me Service URI	This URI provides a unique address that the SIP phone will send to Cisco Unified CallManager to invoke the meet me conference feature.
Call Forward URI	This URI provides a unique address that the SIP phone will send to Cisco Unified CallManager to invoke the call forward feature.

Table 79-1 SIP Profile Configuration Settings (continued)

Field	Description
Abbreviated Dial URI	This URI provides a unique address that the SIP phone will send to Cisco Unified CallManager to invoke the abbreviated dial feature. Speed dials that are not associated with a line key (abbreviated dial indices) will not download to the phone. The phone will use the feature indication mechanism (INVITE with Call-Info header) to indicate when an abbreviated dial number has been entered. The request URI will contain the abbreviated dial digits (for example, 14), and the Call-Info header will indicate the abbreviated dial feature. Cisco Unified CallManager will translate the abbreviated dial digits into the configured digit string and extend the call with that string. If no digit string has been configured for the abbreviated dial digits, a 404 Not Found response gets returned to the phone.
User Info	This field configures the user= parameter in the REGISTER message. Valid values follow: • none—No value gets inserted. • phone—The value user=phone gets inserted in the To, From, and Contact Headers for REGISTER. • ip—The value user=ip gets inserted in the To, From, and Contact Headers for REGISTER.
DTMF DB Level	This field specifies in-band DTMF digit tone level. Valid values follow: • 1 to 6 dB below nominal • 2 to 3 dB below nominal • 3 nominal • 4 to 3 dB above nominal • 5 to 6 dB above nominal
KPML	This field specifies key press markup language. Choices include Signal only, DTMF only, None, and Both. • None - KPML is off. • Signal only - Digit collection from the phone that is needed to place the call • DTMF only - Transport of out-of-band DTMF digits after the call is established; for example, to access an IVR system • Both - Signal and DTMF
Call Hold Ring Back	If you have a call on hold and are talking on another call, when you hang up the call, this parameter causes the phone to ring to let you know that you still have another party on hold. Valid values follow: • Off permanently and cannot be turned on and off locally by using the user interface. • On permanently and cannot be turned on and off locally by using the user interface.

Table 79-1 SIP Profile Configuration Settings (continued)

Field	Description
Anonymous Call Block	This field configures anonymous call block. Valid values follow: - Off—Disabled permanently and cannot be turned on and off locally by using the user interface. - On—Enabled permanently and cannot be turned on and off locally by using the user interface.
Caller ID Blocking	This field configures caller ID blocking. When blocking is enabled, the phone blocks its own number or e-mail address from phones that have caller identification enabled. Valid values follow: - Off—Disabled permanently and cannot be turned on and off locally by using the user interface. - On—Enabled permanently and cannot be turned on and off locally by using the user interface.
Do Not Disturb Control	This field sets the Do Not Disturb (DND) feature. Valid values follow: - User controlled (Default)—The phones dndControl parameter should be 0. - Admin Controlled—The phones dndControl parameter should be 2.
Telnet Level for 7940 and 7960	Cisco SIP IP Phone models 7940 and 7960 do not support ssh for login access or http that is used to collect logs; however, these phones support telnet, which lets the user control the phone, collect debugs, and look at configuration settings. This field controls the telnet_level configuration parameter with the following possible values: - Disabled (no access) - Limited (some access but cannot run privileged commands) - Enabled (full access)
Timer Keep Alive Expires (seconds)	Cisco Unified CallManager requires a keepalive mechanism to support redundancy. This field specifies the interval between keepalive messages sent to the backup Cisco Unified CallManager to ensure it is available in the event a failover is required.
Timer Subscribe Expires (seconds)	This field specifies the time, in seconds, after which a subscription expires. This value gets inserted into the Expires header field. Valid values include any positive number; however, 120 specifies the default value.
Timer Subscribe Delta (seconds)	Use this parameter in conjunction with the Timer Subscribe Expires setting. The phone will resubscribe Timer Subscribe Delta seconds before the subscription period ends, as governed by Timer Subscribe Expires. Valid values range from 3 to 15. Default specifies 5.
Maximum Redirections	Use this configuration variable to determine the maximum number of times that the phone will allow a call to be redirected before dropping the call. Default specifies 70 redirections.
Off Hook to First Digit Timer (microseconds)	This field specifies the time in microseconds that passes when the phone goes off hook and the first digit timer gets set. The value ranges from 0 - 15,000 microseconds. Default specifies 15,000 microseconds.

Table 79-1 **SIP Profile Configuration Settings (continued)**

Field	Description
Conference Join Enabled	This check box determines whether the SIP IP phone 7940 or 7960, when the conference initiator that is using that phone hangs up, should attempt to join the remaining conference attendees. Check the check box if you want to join the remaining conference attendees; leave it unchecked if you do not want to join the remaining conference attendees. Note This check box applies to the Cisco SIP IP phones 7941/61/70/71/11 when they are in SRST mode only.
RFC 2543 Hold	Check this check box to enable setting connection address to 0.0.0.0 per RFC2543 when call hold is signaled to Cisco Unified CallManager. This allows backward compatibility with endpoints that do not support RFC3264.
Semi Attended Transfer	This check box determines whether the Cisco SIP IP phone 7940 and 7960 caller can transfer the second leg of an attended transfer while the call is ringing. Check the check box if you want semi-attended transfer enabled; leave it unchecked if you want semi-attended transfer disabled. Note This check box applies to the Cisco SIP IP phones 7941/61/70/71/11 when they are in SRST mode only.
Enable VAD	Check this check box if you want voice activation detection (VAD) enabled; leave it unchecked if you want VAD disabled. When VAD is enabled, no media gets transmitted when voice is detected.

Table 79-1 SIP Profile Configuration Settings (continued)

Field	Description
Stutter Message Waiting	Check this check box if you want stutter dial tone when the phone goes off hook and a message is waiting; leave unchecked if you do not want a stutter dial tone when a message is waiting.
Call Stats	Check this check box if you want RTP statistics in BYE requests and responses enabled; leave unchecked if you want RTP statistics in BYE requests and responses disabled. If this check box is checked, the phone inserts the headers RTP-RxStat and RTP-TxStat as follows: - RTP-RxStat: Dur=a,Pkt=b,Oct=c,LatePkt=d,LostPkt=e,AvgJit=f - RTP-TxStat: Dur=g,Pkt=h,Oct=i where: - Dur—Total number of seconds since the beginning of reception or transmission. - Pkt—Total number of RTP packets received or transmitted. - Oct—Total number of RTP payload octets received or transmitted (not including RTP header). - LatePkt—Total number of late RTP packets received. - LostPkt—Total number of lost RTP packets received (not including the late RTP packets). - AvgJit—Average jitter, which is an estimate of the statistical variance of the RTP packet interarrival time, measured in timestamp unit and calculated according to RFC 1889. - a, b, c, d, e, f, g, h, and i—Integers

Deleting SIP Profiles

This section describes how to delete a SIP profile.

Before You Begin

To find out which devices are using the SIP profile, choose **Dependency Records** link from the Related Links drop-down list box in the SIP Profile Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records”](#) section on page A-2.

Procedure

-
- Step 1** Locate the SIP profile that you want to delete. See the [“Finding SIP Profiles” section on page 79-1](#).
- Step 2** From the SIP Profile Configuration window, click **Delete**.
A message displays that states that this you cannot undo this action.
- Step 3** To delete the SIP profile, click **OK** or, to cancel the deletion, click **Cancel**.
-

Additional Information

See the [“Related Topics” section on page 79-9](#).

Resetting a SIP Profile

Perform the following procedure to reset a SIP profile.

Procedure

-
- Step 1** From Cisco Unified CallManager Administration, choose **Device > Device Settings> SIP Profile**.
- Step 2** Locate the SIP profile that you want to reset. See the [“Finding SIP Profiles” section on page 79-1](#).
- Step 3** Click the SIP profile that you want to reset.
The SIP Profile Configuration window displays.
- Step 4** Click **Reset**.
The Device Reset dialog displays.
- Step 5** Click one of the following choices:
- **Restart**—Restarts the chosen devices without shutting them down (reregisters the phones and trunks with Cisco Unified CallManager).
 - **Reset**—Shuts down, then restarts, the device.
 - **Close**—Closes the Reset Device dialog without performing any action.
-

Additional Information

See the [“Related Topics” section on page 79-9](#).

Related Topics

- [Finding SIP Profiles, page 79-1](#)
- [Configuring SIP Profiles, page 79-2](#)
- [SIP Profile Configuration Settings, page 79-2](#)
- [Deleting SIP Profiles, page 79-8](#)
- [Resetting a SIP Profile, page 79-9](#)

- [Configuring Cisco Unified IP Phones, page 70-2](#)
- [Configuring a Trunk, page 71-2](#)
- [Understanding Session Initiation Protocol \(SIP\), *Cisco Unified CallManager System Guide*](#)



Common Phone Profile Configuration

Common phone profiles provide data that Cisco TFTP requires. After you configure a common phone profile, use the Phone Configuration window to associate an SCCP or SIP phone with a common phone profile.

Use the following topics to configure and locate common phone profiles:

- [Finding Common Phone Profiles, page 80-1](#)
- [Configuring Common Phone Profiles, page 80-2](#)
- [Common Phone Profile Configuration Settings, page 80-3](#)
- [Deleting Common Phone Profiles, page 80-3](#)
- [Related Topics, page 80-4](#)

Finding Common Phone Profiles

This topic describes how to use the Find and List Common Phone Profile window. The function searches every type of common phone profile against the following categories:

- Name
- Description

Procedure

Step 1 Choose **Device > Device Settings > Common Phone Profile**.

The Find and List Common Phone Profiles window displays.

Step 2 From the first Find Common Profile drop-down list box, choose the field that you want to use to search for common phone profiles; for example, Name, Description.



Note To find all common phone profiles that are registered in the database, do not enter any search text and click **Find**. A list of common phone profiles that matches your search criteria displays.

Step 3 From the second Find Common Phone Profile drop-down list box, choose a search pattern for your text search; for example, begins with, contains, or ends with.

Step 4 Specify the appropriate search text, if applicable, and click **Find**.

The records that match your search criteria display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.



Tip

To search for common phone profiles within the search results, click the **Search Within Results** check box and enter your search criteria as described in this step.



Note

You can delete multiple common phone profiles by checking the check boxes next to the appropriate common phone profiles and clicking **Delete Selected**. You can delete all the common phone profiles in the window by clicking **Select All** and then clicking **Delete Selected**.



Note

You cannot delete the Standard Common Phone Profile.

Step 5 From the list of records that match your search criteria, click the name of the common phone profile that you want to view.

The Common Phone Profile Configuration window displays with the common phone profile that you choose.

Additional Information

See the [“Related Topics” section on page 80-4](#).

Configuring Common Phone Profiles

Perform the following procedure to add, copy, or update a common phone profile.

Procedure

Step 1 Choose **Device > Device Settings > Common Phone Profile**.

The Find and List Common Phone Profiles window displays.

Step 2 Perform one of the followings tasks:

- To copy an existing common phone profile, locate the appropriate common phone profile as described in [“Finding Common Phone Profiles” section on page 80-1](#), click the **Copy** button next to the common phone profile that you want to copy and continue with [Step 3](#).
- To add a new common phone profile, click the **Add New** button, and continue with [Step 3](#).
- To update an existing common phone profile, locate the appropriate common phone profile as described in [“Finding Common Phone Profiles” section on page 80-1](#) and continue with [Step 3](#).

Step 3 Enter the appropriate settings as described in [Table 80-1](#).

Step 4 Click **Save**.

Additional Information

See the [“Related Topics”](#) section on page 80-4.

Common Phone Profile Configuration Settings

[Table 80-1](#) describes the available settings in the Common Phone Profile Configuration window. For more information about related procedures, see the [“Related Topics”](#) section on page 80-4.

Table 80-1 Common Phone Profile Configuration Settings

Field	Description
Common Phone Profile Information	
Name	Enter a name to identify the common phone profile; for example, CPP_7905. The value can include 1 to 50 characters, including alphanumeric characters, dot, dash, and underscores.
Description	Identify the purpose of the common phone profile; for example, common phone profile for model 7905.
Local Phone Unlock Password	Enter the password that is used to unlock a local phone. Valid values comprise 1 to 15 characters.
Enable End User Access to Phone Background Image Setting	Check this check box to enable end users to change the background image on phones that use this common phone profile.

Deleting Common Phone Profiles

This section describes how to delete a common phone profile.

Before You Begin

To find out which devices are using the common phone profile, choose **Dependency Records** link from the Related Links drop-down list box in the Common Phone Profile Configuration window. If dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records”](#) section on page A-2.

Procedure

- Step 1** Locate the common phone profile that you want to delete. See the [“Finding Common Phone Profiles”](#) section on page 80-1.



Note You cannot delete the Standard Common Phone Profile.

- Step 2** From the Common Phone Profile Configuration window, click **Delete**.
A message displays that states that you cannot undo this action.
- Step 3** To delete the common phone profile, click **OK** or, to cancel the deletion, click **Cancel**.
-

Additional Information

See the [“Related Topics”](#) section on page 80-4.

Related Topics

- [Finding Common Phone Profiles](#), page 80-1
- [Configuring Common Phone Profiles](#), page 80-2
- [Common Phone Profile Configuration Settings](#), page 80-3
- [Deleting Common Phone Profiles](#), page 80-3
- [Cisco Unified IP Phone Configuration](#), page 70-1
- [Cisco TFTP](#), *Cisco Unified CallManager System Guide*
- [Understanding Session Initiation Protocol \(SIP\)](#), *Cisco Unified CallManager System Guide*
- [Cisco Unified IP Phones](#), *Cisco Unified CallManager System Guide*



PART 7

Application Configuration





Cisco Unified CallManager Assistant Configuration Wizard

With the Cisco Unified CallManager Assistant Configuration Wizard, Unified CallManager Assistant configuration takes less time and eliminates errors. The partitions, calling search spaces, route point, and translation pattern automatically get created when the administrator successfully runs and completes the configuration wizard. The wizard also creates BAT templates for the Unified CallManager Assistant manager phone, the Unified CallManager Assistant assistant phone, and all other user phones. The administrator can use the BAT templates to configure the managers, assistants, and all other users. Refer to the *Cisco Unified CallManager Bulk Administration Guide*.

The Cisco Unified CallManager Assistant Configuration Wizard provides windows for each configuration parameter. The windows provide the administrator with preconfigured information. If the administrator prefers to use other configuration information (for example, partition names), the administrator can change the preconfigured information to the appropriate information.

For more information on how to use the Cisco Unified CallManager Assistant Configuration Wizard, refer to the [Cisco Unified CallManager Assistant Configuration Wizard](#) in the *Cisco Unified CallManager Features and Services Guide*.



Cisco Unified CallManager Attendant Console Pilot Point Configuration

Cisco Unified CallManager Attendant Console, a client-server application, allows you to use a graphical user interface containing speed-dial buttons and quick directory access to look up phone numbers, monitor line status, and direct calls. A receptionist or administrative assistant can use the attendant console to handle calls for a department or company, or another employee can use it to manage his own telephone calls.

For information and configuration procedures for Cisco Unified CallManager Attendant Console, refer to the [“Cisco Unified CallManager Attendant Console”](#) section in the *Cisco Unified CallManager Features and Services Guide*.



Cisco Unified CallManager Attendant Console User Configuration

Cisco Unified CallManager Attendant Console, a client-server application, allows you to use a graphical user interface containing speed-dial buttons and quick directory access to look up phone numbers, monitor line status, and direct calls. A receptionist or administrative assistant can use the attendant console to handle calls for a department or company, or another employee can use it to manage his own telephone calls.

For information and configuration procedures for Cisco Unified CallManager Attendant Console, refer to the [“Cisco Unified CallManager Attendant Console”](#) section in the *Cisco Unified CallManager Features and Services Guide*.



Cisco Unified CallManager Attendant Console User File Upload

Cisco Unified CallManager Attendant Console, a client-server application, allows you to use a graphical user interface containing speed-dial buttons and quick directory access to look up phone numbers, monitor line status, and direct calls. A receptionist or administrative assistant can use the attendant console to handle calls for a department or company, or another employee can use it to manage his own telephone calls.

For information and configuration procedures for Cisco Unified CallManager Attendant Console, refer to the [“Cisco Unified CallManager Attendant Console”](#) section in the *Cisco Unified CallManager Features and Services Guide*.



Plug-in Configuration

Application plug-ins extend the functionality of Cisco Unified CallManager. For example, the Cisco Unified CallManager Attendant Console plug-in allows a receptionist to rapidly answer and transfer calls within an organization, and the JTAPI plug-in allows a computer to host applications that access the Cisco Unified CallManager via the Java Telephony Application Programming Interface (JTAPI).

This section contains the following topics:

- [Installing Plug-ins, page 85-1](#)
- [Updating the Plug-in URL, page 85-2](#)
- [Update Plug-in URL Configuration Settings, page 85-3](#)

Installing Plug-ins



Tip

After Cisco Unified CallManager upgrades, you must reinstall all plug-ins except the Cisco CDR Analysis and Reporting plug-in.

Before you install any plug-ins, disable all intrusion detection or antivirus services that run on the server where you plan to install the plug-in.

Perform the following procedure to install any plug-in.

Procedure

Step 1 Choose **Application > Plugins**.

The Find and List Plugins window displays. Use the drop-down list boxes to search for available plug-in applications.

Step 2 From the first Find Plugins window drop-down list box, choose one of the following criteria:

- Name
- Description

From the second Find Plugins window drop-down list box, choose one of the following criteria:

- begins with
- contains

- is exactly
- ends with
- is empty
- is not empty

From the Plugin Type drop-down list box, choose one of the following criteria:

- Application Menu
- Installation
- User Menu
- Telecaster Menu

Step 3 Specify the appropriate search text, if applicable, and click **Find**.



Tip To find all available plug-ins, click **Find** without entering any search text.

Step 4 Click the plug-in name that you want to install.

Step 5 To download the plug-in, click the **Download** link.

Step 6 Follow the instructions in the installation wizard to complete the installation.

Related Topics

- [Plug-in Configuration, page 85-1](#)
- [Updating the Plug-in URL, page 85-2](#)

Updating the Plug-in URL

During the Cisco Unified CallManager install process, records that are added to the Plugins table specify the URLs that the Administration applications use to build the Application drop-down menu. The domain name server (DNS) provides the basis for the URL that is constructed at installation time. If the DNS changes, the URL does not get updated.

Perform the following procedure to update the URL of the Plug-in URL.

Procedure

Step 1 Choose **Application > Plugins**.

The Find and List Plugins window displays.

Step 2 From the drop-down list boxes, choose the Plugin name and the Plugin type.

Step 3 Click the Plugin name that you want to update.

The Update Plugin URL window displays.

- Step 4** Enter the URL in the Custom URL field.
- Step 5** Click the **Save** icon that displays in the tool bar in the upper, left corner of the window (or click the **Save** button that displays at the bottom of the window) to update and save the URL.
-

Related Topics

- [Plug-in Configuration, page 85-1](#)
- [Installing Plug-ins, page 85-1](#)

Update Plug-in URL Configuration Settings

[Table 85-1](#) describes the update plug-in URL configuration settings.

Table 85-1 *Update Plug-in URL Configuration Settings*

Field	Description
Plugin Settings	
Plugin Name	From the drop-down list box, choose the Plugin Name for which you are changing the URL; for example, Cisco Unified CallManager Attendant Console.
Plugin Type	From the drop-down list box, choose the Plugin Type for which you are changing the URL; for example, application or installation.
URL	The URL automatically displays.
Custom URL	Use only alphanumeric characters for the custom URL.
Show Plugin on User Option Pages	Check this check box to show the plug-in on the user option window.



PART 8

User Management Configuration





Application User Configuration

The Application User Configuration window in Cisco Unified CallManager Administration allows the administrator to add, search, display, and maintain information about Cisco Unified CallManager application users.

The following topics contain information on managing application user information:

- [Finding an Application User, page 86-1](#)
- [Adding an Application User, page 86-3](#)
- [Application User Configuration Settings, page 86-3](#)
- [Changing an Application User Password, page 86-7](#)
- [Configuring Application Profiles for Application Users, page 86-7](#)
- [Associating Devices to an Application User, page 86-8](#)
- [Application Users and End Users, *Cisco Unified CallManager System Guide*](#)
- [Managing Application User and End User Configuration Checklist, *Cisco Unified CallManager System Guide*](#)

Additional Information

See the [“Related Topics”](#) section on page 86-9.

Finding an Application User

Because you may have several application users in your network, Cisco Unified CallManager lets you locate specific application users on the basis of specific criteria. Use the following procedure to locate application users.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your application user search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your application user search preferences until you modify your search or close the browser.

Procedure**Step 1** Choose **User Management > Application User**.

The Find and List Application Users window displays. Use the two drop-down list boxes to search for an application user.

Step 2 From the first Find application user where drop-down list box, choose the following criterion:

- User ID

From the second Find application user where drop-down list box, choose one of the following criteria:

- begins with
- contains
- is exactly
- ends with
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.**Tip**

To find all application users that are registered in the database, click **Find** without entering any search text.

A list of discovered application users displays by

- User ID

**Note**

You can delete multiple application users from the Find and List application users window by checking the check boxes next to the appropriate application users and clicking **Delete Selected**. You can delete all application users in the window, except for default application users, by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records, click the application user name that matches your search criteria.

The window displays the application user that you choose.

Additional Information

See the [“Related Topics” section on page 86-9](#).

Adding an Application User

The following procedure provides instructions on adding a user.

**Note**

If you are adding an application user for Cisco Unity Administrator or Cisco Unity Connection Administrator, you must use the same user name and password that you defined in Cisco Unity and Cisco Unity Connection Administration. Refer to the *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.0* or the *Cisco Unified CallManager 5.0 SCCP Integration Guide for Cisco Unity Connection 2.1*. The user ID provides authentication between Cisco Unity or Cisco Unity Connection and Cisco Unified CallManager Administration.

Procedure

- Step 1** Choose **User Management > Application User**.
- The Find and List Application Users window displays. Use the two drop-down list boxes to search for an application user.
- Step 2** Click **Add New**.
- The Application User Configuration window displays.
- Step 3** Enter the appropriate settings as described in [Table 86-1](#).
- Step 4** When you have completed the user information, save your changes and add the user by clicking **Save**.

Next Steps

If you want to associate devices with this application user, continue with the [“Associating Devices to an Application User”](#) procedure.

Additional Information

See the [“Related Topics”](#) section on page 86-9.

Application User Configuration Settings

[Table 86-1](#) describes the application user configuration settings. For related procedures, see the [“Related Topics”](#) section on page 86-9.

Table 86-1 Application User Configuration Settings

Field	Description
Application User Information	
User ID	Enter the application user identification name. Cisco Unified CallManager does not permit modifying the user ID after it is created. You may use the following special characters: dash (-), underscore (_), “”, and blank spaces.
Password	Enter five or more alphanumeric or special characters for the application user password.

Table 86-1 **Application User Configuration Settings (continued)**

Field	Description
Confirm Password	Enter the user password again.
Digest Credentials	When Cisco Unified CallManager acts as a UAS during digest authentication, the digest credentials that you specify in this field get used for challenges. Enter a string of alphanumeric characters. For information on digest authentication, refer to the <i>Cisco Unified CallManager Security Guide</i>.
Confirm Digest Credentials	To confirm that you entered the digest credentials correctly, enter the credentials in this field.
Presence Group	Configure this field with the Presence feature. Note If you are not using this application user with presence, leave the default (None) setting for presence group. From the drop-down list box, choose a Presence group for the application user. The group selected specifies the destinations that the application user, such as IPMASysUser, can monitor. The Standard Presence group gets configured at installation. Presence groups configured in Cisco Unified CallManager Administration also appear in the drop-down list box. Presence authorization works with presence groups to allow or block presence requests between groups. Refer to the “Presence” chapter in the <i>Cisco Unified CallManager Features and Services Guide</i> for information about configuring permissions between groups.
Accept Presence Subscription	Configure this field with the Presence feature for presence authorization. If you enabled application-level authorization in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified CallManager performs application-level authorization. Check this check box to authorize Cisco Unified CallManager to accept presence requests that come from this SIP trunk application user. If you check this check box in the Application User Configuration window and do not check the Enable Application Level Authorization check box in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified CallManager sends a 403 error message to the SIP user agent that is connected to the trunk. For more information on authorization, refer to the “Presence” chapter in the <i>Cisco Unified CallManager Security Guide</i>.

Table 86-1 **Application User Configuration Settings (continued)**

Field	Description
Accept Out-of-Dialog Refer	If you enabled application-level authorization in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified CallManager performs application-level authorization. Check this check box to authorize Cisco Unified CallManager to accept Out-of-Dialog REFER requests that come from this SIP trunk application user. For example, to use SIP-initiated transfer features and other advanced transfer-related features, you must authorize Cisco Unified CallManager to accept incoming Out-of-Dialog REFER requests for this application user. If you check this check box in the Application User Configuration window and do not check the Enable Application Level Authorization check box in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified CallManager sends a 403 error message to the SIP user agent that is connected to the trunk. For more information on authorization, refer to the <i>Cisco Unified CallManager Security Guide</i>.
Accept Unsolicited Notification	If you enabled application-level authorization in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified CallManager performs application-level authorization. Check this check box to authorize Cisco Unified CallManager to accept unsolicited notifications that come from this SIP trunk application user. For example, to provide MWI support, you must authorize Cisco Unified CallManager to accept incoming unsolicited notifications for this application user. If you check this check box in the Application User Configuration window and do not check the Enable Application Level Authorization check box in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified CallManager sends a 403 error message to the SIP user agent that is connected to the trunk. For more information on authorization, refer to the <i>Cisco Unified CallManager Security Guide</i>.

Table 86-1 Application User Configuration Settings (continued)

Field	Description
Accept Header Replacement	If you enabled application-level authorization in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified CallManager performs application-level authorization. Check this check box to authorize Cisco Unified CallManager to accept header replacements in messages from this SIP trunk application user. For example, to transfer an external call on a SIP trunk to an external device or party, as in attended transfer, you must authorize Cisco Unified CallManager to accept SIP requests with replaces header in REFERS and INVITES for this application user. If you check this check box in the Application User Configuration window and do not check the Enable Application Level Authorization check box in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified CallManager sends a 403 error message to the SIP user agent that is connected to the trunk. For more information on authorization, refer to the <i>Cisco Unified CallManager Security Guide</i>.
CAPF Information	
Associated CAPF Profiles	In the Associated CAPF Profile pane, the Instance ID for the Application User CAPF Profile displays; that is, if you configured an Application User CAPF Profile for the user. To edit the profile, click the Instance ID; then, click Edit Profile. The Application User CAPF Profile Configuration window displays. For information on how to configure the Application User CAPF Profile, refer to the <i>Cisco Unified CallManager Security Guide</i>.
Device Information	
Available Devices	This list box displays the devices that are available for association with this application user. To associate a device with this application user, select the device and click the Down arrow below this list box. If the device that you want to associate with this application user does not display in this pane, click one of these buttons to search for other devices: • Find more Phones—Click this button to find more phones to associate with this application user. The Find and List Phones window displays to enable a phone search. • Find more Route Points—Click this button to find more route points to associate with this application user. The Find and List CTI Route Points window displays to enable a CTI route point search. • Find more Pilot Points—Click this button to find more pilot points to associate with this application user. The Find and List Pilot Points window displays to enable a pilot point search.

Table 86-1 **Application User Configuration Settings (continued)**

Field	Description
Permissions Information	
Groups	This list box displays after an application user has been added. The list box displays the groups to which the application user belongs.
Roles	This list box displays after an application user has been added. The list box displays the roles that are assigned to the application user.

Additional Information

See the [“Related Topics”](#) section on page 86-9.

Changing an Application User Password

Use the following procedure to change an application user password.

Procedure

-
Step 1	Use the procedure in the “Finding an Application User” section on page 86-1 to find the application user whose password you want to change. The Application User Configuration window displays with information about the chosen application user.
Step 2	In the Password field, double-click the existing password, which is encrypted, and enter the new password.
Step 3	In the Confirm Password field, double-click the existing, encrypted password and enter the new password again.
Step 4	Click Save .
-

Additional Information

See the [“Related Topics”](#) section on page 86-9.

Configuring Application Profiles for Application Users

After you add a new application user, you can configure a profile for each application. These profiles allow each application user to personalize phone features, Cisco Unified CM Assistant, Cisco Extension Mobility, Cisco Unified CallManager AutoAttendant, and Cisco IP SoftPhone capability.

Before You Begin

Make sure that the application user is in the database. See the [“Finding an Application User”](#) section on page 86-1 for more information.

Additional Information

See the [“Related Topics” section on page 86-9](#).

Associating Devices to an Application User

You can associate devices over which application users will have control. Application users can control some devices, such as phones. Applications that are identified as users can control other devices, such as CTI ports. When application users have control of a phone, they can control certain settings for that phone, such as speed dial and call forwarding.

Before You Begin

To assign devices to an application user, you must access the Application User Configuration window for that user. See the [“Finding an Application User” section on page 86-1](#) for information on finding existing application users. When the Application User Configuration window displays, perform the following procedure to assign devices.

Procedure

-
Step 1	In the Available Devices list box, choose a device that you want to associate with the application user and click the Down arrow below the list box.
Step 2	To limit the list of available devices, click the Find more Phones , Find more Route Points , or Find more Pilot Points button: • If you click the Find more Phones button, the Find and List Phones window displays. Perform a search to find the phones to associate with this application user. • If you click the Find more Route Points button, the Find and List CTI Route Points window displays. Perform a search to find the CTI route points to associate with this application user. • If you click the Find more Pilot Points button, the Find and List Pilot Points window displays. Perform a search to find the pilot points to associate with this application user.
Step 3	Repeat the preceding steps for each device that you want to assign to the application user.
Step 4	When you complete the assignment, click Save to assign the devices to the application user.
-

Additional Information

See the [“Related Topics” section on page 86-9](#).

Related Topics

- [Finding an Application User](#), page 86-1
- [Adding an Application User](#), page 86-3
- [Application User Configuration Settings](#), page 86-3
- [Changing an Application User Password](#), page 86-7
- [Configuring Application Profiles for Application Users](#), page 86-7
- [Associating Devices to an Application User](#), page 86-8
- [Device Association](#), *Cisco Unified CallManager System Guide*
- [Application Users and End Users](#), *Cisco Unified CallManager System Guide*
- [Managing Application User and End User Configuration Checklist](#), *Cisco Unified CallManager System Guide*
- [Cisco Unity Messaging Integration](#), *Cisco Unified CallManager System Guide*
- [LDAP System Configuration](#), page 12-1
- [Directory Number Configuration](#), page 49-1
- [CTI Route Point Configuration](#), page 67-1
- [Cisco Unified IP Phone Configuration](#), page 70-1
- [Role Configuration](#), page 88-1
- [User Group Configuration](#), page 89-1
- [Cisco Extension Mobility](#), *Cisco Unified CallManager Features and Services Guide*
- [Presence](#), *Cisco Unified CallManager Features and Services Guide*
- *Cisco Unified CallManager Security Guide*



End User Configuration

The End User Configuration window in Cisco Unified CallManager Administration allows the administrator to add, search, display, and maintain information about Cisco Unified CallManager end users.



Note

You can modify end user information only if synchronization with an LDAP server is not enabled. To check whether synchronization with an LDAP server is enabled, use the **System > LDAP > LDAP System** menu option. In the LDAP System window that displays, ensure that the Enable Synchronizing from LDAP Server check box is not checked. If synchronization is enabled, you can view end user data, but you cannot modify the end user data.

The following topics contain information on managing end user directory information:

- [Finding an End User, page 87-1](#)
- [Adding an End User, page 87-3](#)
- [Creating a Cisco Unity or Cisco Unity Connection Voice Mailbox, page 87-3](#)
- [End User Configuration Settings, page 87-5](#)
- [Changing an End User Password, page 87-8](#)
- [Changing an End User PIN, page 87-9](#)
- [Configuring User-Related Information for End Users, page 87-9](#)
- [Associating Devices to an End User, page 87-10](#)
- [Associating Cisco Extension Mobility Profiles, page 87-12](#)
- [Deleting an End User, page 87-13](#)

Additional Information

See the “[Related Topics](#)” section on page 87-13.

Finding an End User

Because you may have several end users in your network, Cisco Unified CallManager lets you locate specific end users on the basis of specific criteria. Use the following procedure to locate end users.

**Note**

During your work in a browser session, Cisco Unified CallManager Administration retains your end user search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your end user search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **User Management > End User**.

The Find and List Users window displays. Use the two drop-down list boxes to search for an end user.

Step 2 From the first Find user where drop-down list box, choose the field that you want to use to search for end users; for example, First Name, Last Name, or User ID.

**Note**

To find all end users that are registered in the database, do not enter any search text and click **Find**. A list of end users that matches your search criteria displays.

Step 3 From the second Find end user where drop-down list box, choose a search pattern for your text search; for example, begins with, contains, or ends with.

Step 4 Specify the appropriate search text, if applicable, and click **Find**.

The records that match your search criteria display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

**Tip**

To search for end users within the search results, click the **Search Within Results** check box and enter your search criteria as described in this step.

**Note**

You can delete multiple end users from the Find and List users window by checking the check boxes next to the appropriate end users and clicking **Delete Selected**. You can delete all end users in the window by clicking **Select All** and then clicking **Delete Selected**.

Step 5 From the list of records that match your search criteria, click the user ID of the end user that you want to view.

The End User Configuration window displays the end user that you choose.

Additional Information

See the [“Related Topics”](#) section on page 87-13.

Adding an End User

The following procedure provides instructions on adding an end user.

**Note**

You can modify end user information only if synchronization with an LDAP server is not enabled. To check whether synchronization with an LDAP server is enabled, use the **System > LDAP > LDAP System** menu option. In the LDAP System window that displays, ensure that the Enable Synchronizing from LDAP Server check box is not checked. If synchronization is enabled, you can view end user data, but you cannot modify the end user data.

Procedure

Step 1 Choose **User Management > End User**.

The Find and List End Users window displays. Use the two drop-down list boxes to search for an end user.

Step 2 Click **Add New**.

The End User Configuration window displays.

Step 3 Enter the appropriate settings as described in [Table 87-1](#).

Step 4 When you have completed the end user information, save your changes and add the end user by clicking **Save**.

Next Steps

If you want to associate devices to this end user, continue with the [“Associating Devices to an End User”](#) procedure.

Additional Information

See the [“Related Topics”](#) section on page 87-13.

Creating a Cisco Unity or Cisco Unity Connection Voice Mailbox

The “Create Cisco Unity User” link on the End User Configuration window allows you to create individual Cisco Unity and Cisco Unity Connection voice mailboxes from Cisco Unified CallManager Administration.

**Note**

The “Create Cisco Unity User” link displays only if the Cisco Unity administrator installed and configured the appropriate software. Refer to the *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.0* or the *Cisco Unified CallManager 5.0 SCCP Integration Guide for Cisco Unity Connection 1.1*.

Before You Begin

- You must configure Cisco Unified CallManager for voice messaging. Refer to [“Cisco Unity Configuration Checklist”](#) in the *Cisco Unified CallManager System Guide*.

- You must configure Cisco Unity servers. See Cisco Unity and Cisco Unity Connection Documentation.
- Ensure Cisco Unity Cisco Unified CallManager Integrated Voice Mailbox Configuration is enabled on the Cisco Unity or Cisco Unity Connection server. Refer to the *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.0* or the *Cisco Unified CallManager 5.0 SCCP Integration Guide for Cisco Unity Connection 1.1*.
- Ensure Cisco RIS Data Collector service is activated. Refer to the *Cisco Unified CallManager Serviceability System Guide* and the *Cisco Unified CallManager Serviceability Administration Guide*.
- A device must associate with the end user before the Create Cisco Unity User link displays. The link displays beside the Primary Extension field.
- Ensure Voice Mail Profile is associated with the Primary Extension Directory Number for the Create Cisco Unity User link displays. See the [“Configuring a Directory Number” section on page 49-2](#).

**Note**

The Directory Number Configuration window also includes the “Create Cisco Unity User” link.

Procedure

Step 1 To associate a device to the end user, choose **User Management > End User** (see the [“Associating Devices to an End User” section on page 87-10](#)).

Step 2 Enter the appropriate settings in [Table 87-1](#).

**Note**

Ensure that you have defined a primary extension; otherwise, the “Create Cisco Unity User” link will not display in the Related Links drop-down list box.

Step 3 From the Related Links drop-down list box, in the upper, right corner of the window, choose the “Create Cisco Unity User” link and click **Go**.

The Add Cisco Unity User dialog box displays.

Step 4 From the Application Server drop-down list box, choose the Cisco Unity or Cisco Unity Connection server on which you want to create a Cisco Unity or Cisco Unity Connection user and click **Next**.

Step 5 From the Subscriber Template drop-down list box, choose the subscriber template that you want to use.

Step 6 Click **Save**.

The Cisco Unity mailbox gets created. The link, in Related Links, changes to “Edit Cisco Unity User” in the End User Configuration window.

You can now see the mailbox that you created from Cisco Unity Administrator. Refer to the *Cisco Unity Installation Guide* or the *Cisco Unity Connection Installation Guide*.

**Note**

When the Cisco Unity user gets integrated with the Cisco Unified CallManager End User, you cannot edit the following fields in Cisco Unity Administrator: Alias (User ID in Cisco Unified CallManager Administration); First Name; Last Name; Extension (Primary Extension in Cisco Unified CallManager Administration). You can only update these fields in Cisco Unified CallManager Administration.

**Note**

Cisco Unity monitors the synchronization of data from Cisco Unified CallManager. You can configure the sync time in Cisco Unity Administrator under Tools (Import CallManager Users, Sync CallManager). Refer to the Cisco Unity documentation.

Additional Information

See the [“Related Topics” section on page 87-13](#).

End User Configuration Settings

Table 87-1 describes the end user configuration settings. For related procedures, see the [“Related Topics” section on page 87-13](#).

Table 87-1 **End User Configuration Settings**

Field	Description
User Information	
LDAP Sync Status	This field displays the LDAP synchronization status, which you set with the System > LDAP > LDAP System menu option.
User ID	Enter the end user identification name. Cisco Unified CallManager does not permit modifying the user ID after it is created.
Password	Enter five or more alphanumeric or special characters for the end user password.
Confirm Password	Enter the end user password again.
PIN	Enter five or more numeric characters for the personal identification number.
Confirm PIN	Enter the PIN again.
Last Name	Enter the end user last name.
Middle Name	Enter the end user middle name.
First Name	Enter the end user first name.
Telephone Number	Enter the end user telephone number. You may use the following special characters: (,), and -.
Mail ID	Enter the end user’s email address.
Manager User ID	Enter the user ID of the end user manager ID. The manager user ID that you enter must already exist in the directory as an end user.
Department	Enter the end user department information (for example, the department number or name).

Table 87-1 **End User Configuration Settings (continued)**

Field	Description
User Locale	From the drop-down list box, choose the locale that is associated with the end user. The user locale identifies a set of detailed information to support end users, including language and font. Cisco Unified CallManager uses this locale for extension mobility and the Cisco Unified IP Phone User Options. For Cisco Extension Mobility log on, the locale that is specified here takes precedence over the device and device profile settings. For Cisco Extension Mobility log off, Cisco Unified CallManager uses the end user locale that the default device profile specifies. Note If you do not choose an end user locale, the locale that is specified in the Cisco CallManager service parameters as Default User Locale applies.
Associated PC	This required field applies for Cisco SoftPhone and Cisco Unified CallManager Attendant Console users.
Digest Credentials	When you configure digest authentication for SIP phones, Cisco Unified CallManager challenges the identity of the phone every time the phone sends a SIP request to Cisco Unified CallManager. The digest credentials that you enter in this field get associated with the phone when you choose a digest user in the Phone Configuration window. Enter a string of alphanumeric characters. Note For more information on digest authentication, refer to the <i>Cisco Unified CallManager Security Guide</i>.
Confirm Digest Credentials	To confirm that you entered the digest credentials correctly, enter the credentials in this field.
Device Associations	
Controlled Devices	After the device is associated, this field displays the description information (for example, the MAC address) that the end user controls. To associate a device with this end user, click the Device Association button on the right. See the “Associating Devices to an End User” section on page 87-10 for a detailed procedure.
Extension Mobility	
Available Profiles	This list box displays the extension mobility profiles that are available for association with this end user. To search for an extension mobility profile, click Find. Use the Find and List Device Profiles window that displays to search for the extension mobility profile that you want. To associate an extension mobility profile with this end user, select the profile and click the Down arrow below this list box.
Controlled Profiles	This field displays a list of controlled device profiles that are associated with an end user who is configured for Cisco Extension Mobility.
Default Profile	From the drop-down list box, choose a default extension mobility profile for this end user.

Table 87-1 **End User Configuration Settings (continued)**

Field	Description
Presence Group	Configure this field with the Presence feature. From the drop-down list box, choose a Presence group for the end user. The selected group specifies the destinations that the end user can monitor. The default value for Presence Group specifies Standard Presence group, configured with installation. Presence groups that are configured in Cisco Unified CallManager Administration also appear in the drop-down list box. Presence authorization works with presence groups to allow or block presence requests between groups. Refer to the “Presence” chapter in the <i>Cisco Unified CallManager Features and Services Guide</i> for information about configuring permissions between groups and how presence works with extension mobility.
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Cisco Unified CallManager routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user. From the drop-down list box, choose the SUBSCRIBE calling search space to use for presence requests for the end user. All calling search spaces that you configure in Cisco Unified CallManager Administration display in the SUBSCRIBE Calling Search Space drop-down list box. If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces. For information on how to configure a calling search space, see the “Calling Search Space Configuration” section on page 43-1
Allow Control of Device from CTI	Check this check box to allow CTI to control devices that this end user owns. If the associated directory number specifies a shared line, ensure the check box is enabled as long as at least one associated device specifies a combination of device type and protocol that CTI supports.
Directory Number Associations	
Primary Extension	This field represents the primary directory number for the end user. You choose no primary line when you associate devices to the end user. End users can have multiple lines on their phones. From the drop-down list box, choose a primary extension for this end user. If the system is configured for Cisco Unity or Cisco Unity Connection integration, the Create Cisco Unity User link displays.

Table 87-1 **End User Configuration Settings (continued)**

Field	Description
IPCC Extension	From the drop-down list box, choose an IPCC extension for this end user. Note This field displays only if the IPCC Express Installed enterprise parameter is set to <i>True</i> .
CAPF Information	
Associated CAPF Profiles	In the Associated CAPF Profile pane, the Instance ID for the End User CAPF Profile displays; that is, if you configured an End User CAPF Profile for the user. To edit the profile, click the Instance ID; then, click Edit Profile . The End User CAPF Profile Configuration window displays. For information on how to configure the End User CAPF Profile, refer to the <i>Cisco Unified CallManager Security Guide</i> .
Permissions Information	
Groups	This list box displays after an end user has been added. The list box displays the groups to which the end user belongs. For more information on configuring user groups, see the “User Group Configuration” section on page 89-1 .
Roles	This list box displays after an end user has been added. The list box displays the roles that are assigned to the end user. For more information on configuring roles, see the “Role Configuration” section on page 88-1 .

Additional Information

See the [“Related Topics” section on page 87-13](#).

Changing an End User Password

Use the following procedure to change an end user password for an end user in the global directory.

Procedure

-
- Step 1** Use the procedure in the [“Finding an End User” section on page 87-1](#) to find the end user whose password you want to change.
- The End User Configuration window displays with information about the chosen end user.
- Step 2** In the Password field, double-click the existing password, which is encrypted, and enter the new password.
- Step 3** In the Confirm Password field, double-click the existing, encrypted password and enter the new password again.
- Step 4** Click **Save**.
-

Additional Information

See the [“Related Topics” section on page 87-13](#).

Changing an End User PIN

Use the following procedure to change the personal identification number (PIN) for an end user.

Procedure

-
Step 1	Use the procedure in the “Finding an End User” section on page 87-1 to find the end user whose PIN you want to change. The End User Configuration window displays with information about the chosen end user.
Step 2	In the PIN field, double-click the existing PIN, which is encrypted, and enter the new PIN.
Step 3	In the Confirm PIN field, double-click the existing, encrypted PIN and enter the new PIN again.
Step 4	Click Save .
-

Additional Information

See the [“Related Topics” section on page 87-13](#).

Configuring User-Related Information for End Users

After you add a new end user, you can configure additional information related to the end user. This information allows each end user to personalize phone features, Cisco Unified CM Assistant Manager, Cisco Unified CM Assistant Assistant, Cisco Extension Mobility, Cisco Unified CallManager AutoAttendant, and Cisco IP SoftPhone capability.

Before You Begin

Make sure that the end user is in the database. See the [“Finding an End User” section on page 87-1](#) for more information.

Procedure

-
Step 1	Use the procedure in the “Finding an End User” section on page 87-1 to find the end user whose application profile(s) you want to configure. The End User Configuration window displays with information about the chosen end user.
Step 2	To configure Cisco Unified CM Assistant Manager for this end user, from the Related Links drop-down list box, choose Cisco Unified CM Assistant Manager and click Go . The Cisco Unified CM Assistant Manager Configuration window displays for this end user. Refer to the “Cisco Unified CallManager Assistant With Proxy Line Support” and “Cisco Unified CallManager Assistant With Shared Line Support” chapters in the <i>Cisco Unified CallManager Features and Services Guide</i> for details of configuring Cisco Unified CM Assistant Manager.

After you configure Cisco Unified CM Assistant Manager for this end user, you can return to the End User Configuration window for this end user. From the Related Links drop-down list box in the Cisco Unified CM Assistant Manager Configuration window, choose Back to User Configuration and click **Go**.

- Step 3** To configure Cisco Unified CM Assistant Assistant for this end user, from the Related Links drop-down list box, choose Cisco Unified CM Assistant Assistant and click **Go**.

The Cisco Unified CM Assistant Assistant Configuration window displays for this end user. Refer to the [“Cisco Unified CallManager Assistant With Proxy Line Support”](#) and [“Cisco Unified CallManager Assistant With Shared Line Support”](#) chapters in the *Cisco Unified CallManager Features and Services Guide* for details of configuring Cisco Unified CM Assistant Assistant.

After you configure Cisco Unified CM Assistant Assistant for this end user, you can return to the End User Configuration window for this end user. From the Related Links drop-down list box in the Cisco Unified CM Assistant Manager Configuration window, choose Back to User Configuration and click **Go**.

- Step 4** To show the user privilege report for this end user, from the Related Links drop-down list box, choose User Privilege Report and click **Go**.

The User Privilege window displays for this end user. Refer to the [“Viewing a User’s Roles, User Groups, and Permissions” section on page 89-7](#) for details of the user privilege report.

After you display the user privilege report for this end user, you can return to the End User Configuration window for this end user. From the Related Links drop-down list box in the User Privilege window, choose Back to User and click **Go**.

Additional Information

See the [“Related Topics” section on page 87-13](#).

Associating Devices to an End User

You can associate devices over which end users will have control. End users can control some devices, such as phones. Applications that are identified as users can control other devices, such as CTI ports. When end users have control of a phone, they can control certain settings for that phone, such as speed dial and call forwarding.



Note

All device association behavior remains identical regardless of the type of device for which the feature is configured.

Before You Begin

To associate devices with an end user, you must access the End User Configuration window for that user. See the [“Finding an End User” section on page 87-1](#) for information on finding existing end users. When the End User Configuration window displays, perform the following procedure to assign devices.

Do not attempt to associate devices to a new end user before you finish adding the new end user. Be sure to click **Save** on the End User Configuration window before you add device associations for a new end user.

Procedure

- Step 1** In the Device Associations pane, click **Device Association**.

The User Device Association window displays.

Finding a Device

Because you may have several devices in your network, Cisco Unified CallManager lets you locate specific devices on the basis of specific criteria. Use the following steps to locate devices.



Note During your work in a browser session, Cisco Unified CallManager Administration retains your device search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your device search preferences until you modify your search or close the browser.

- Step 2** From the first Find User Device Association where drop-down list box, choose the field that you want to use to search for devices; for example, Name or Description.



Note To find all devices that are registered in the database, do not enter any search text and click **Find**. A list of devices that matches your search criteria displays.

- Step 3** From the second Find User Device Association where drop-down list box, choose a search pattern for your text search; for example, begins with, contains, or ends with.

- Step 4** Specify the appropriate search text, if applicable, and click **Find**.

The records that match your search criteria display in the Device association for user (this particular user) portion of the window. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.



Tip To search for devices within the search results, click the **Search Within Results** check box and enter your search criteria as described in this step.

Associating a Device

- Step 5** From the Device association for (this particular user) pane, choose the devices that you want to associate with this end user by checking the box to the left of the device name(s).

Use the buttons at the bottom of the window to select and deselect devices to associate with the end user.



Note The buttons function to select and deselect only the devices that were found as a result of any search for devices that you performed in the preceding steps.



Tip Check the *Show the devices already associated with user* check box to display the devices that are already associated with this end user.

Use the buttons to perform the following functions:

- **Select All on Page**—Click this button to select all devices that display on this page.
- **Clear All on Page**—Click this button to uncheck the check boxes next to all devices that display on this page.
- **Select All in Search**—Click this button to select all devices that match the search criteria that you specified in the Search Options portion of the window. The button performs the search anew and selects all the matching devices.
- **Clear All in Search**—Click this button to deselect all devices that match the search criteria that you specified in the Search Options portion of the window. The button performs the search anew and deselects all the matching devices.
- **Save Selected/Changes**—Click this button to associate the devices that you have selected with this end user.
- **Remove All Associated Devices**—Click this button to disassociate all devices that are already associated with this end user. After you click this button, a popup window asks you to confirm that you want to remove all device associations from this end user. Click **OK** to confirm.

Step 6 Repeat the preceding steps for each device that you want to assign to the end user.

Step 7 To complete the association, click **Save Selected/Changes**.

After you save the user device associations, the associated devices display above a dashed line in the Device association for user (this end user) portion of the window.

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

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

Additional Information

See the [“Related Topics” section on page 87-13](#).

Associating Cisco Extension Mobility Profiles

Use Cisco Extension Mobility to configure a Cisco Unified IP Phone model 7940 or Cisco Unified IP Phone model 7960 to temporarily display as the phone of an end user. The end user can log in to a phone, and the extension mobility profile (including line and speed-dial numbers) for the end user resides on the phone. This feature applies primarily in environments where end users are not permanently assigned to physical phones.

To associate an extension mobility profile to an end user, you must access the End User Configuration window for that end user. See the [“Finding an End User” section on page 87-1](#) for information on accessing information on existing end users. To configure and associate Cisco Extension Mobility for end users, refer to the [“Cisco Extension Mobility” chapter in the *Cisco Unified CallManager Features and Services Guide*](#).

Deleting an End User

To delete an end user by using Cisco Unified CallManager Administration, perform the following procedure.

Before You Begin

Before deleting the end user, determine whether the devices or profiles that are associated with the end user need to be removed or deleted.

You can view the devices and profiles that are assigned to the end user from the Device Associations, Extension Mobility, Directory Number Associations, CAPF Information, and Permissions Information areas of the End User Configuration window. You can also choose **Dependency Records** from the Related Links drop-down list box in the End User Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#).

Procedure

Step 1 Choose **User Management > End User**.

The Find and List Users window displays.

Step 2 To locate a specific end user, enter search criteria and click **Find**.

A list of end users that match the search criteria displays.

Step 3 Perform one of the following actions:

- Check the check boxes next to the end users that you want to delete and click **Delete Selected**.
- Delete all the end users in the window by clicking **Select All** and clicking **Delete Selected**.
- Choose the user ID of the end user that you want to delete from the list to display its current settings and click **Delete**.

A confirmation dialog displays.

Step 4 Click **OK**.

Additional Information

See the [“Related Topics” section on page 87-13](#).

Related Topics

- [Finding an End User, page 87-1](#)
- [Adding an End User, page 87-3](#)
- [Creating a Cisco Unity or Cisco Unity Connection Voice Mailbox, page 87-3](#)
- [End User Configuration Settings, page 87-5](#)
- [Changing an End User Password, page 87-8](#)
- [Changing an End User PIN, page 87-9](#)
- [Configuring User-Related Information for End Users, page 87-9](#)

- [Associating Devices to an End User](#), page 87-10
- [Associating Cisco Extension Mobility Profiles](#), page 87-12
- [Deleting an End User](#), page 87-13
- [LDAP System Configuration](#), page 12-1
- [Directory Number Configuration](#), page 49-1
- [CTI Route Point Configuration](#), page 67-1
- [Cisco Unified IP Phone Configuration](#), page 70-1
- [Role Configuration](#), page 88-1
- [User Group Configuration](#), page 89-1
- [Viewing a User's Roles, User Groups, and Permissions](#), page 89-7
- [Managing Application User and End User Configuration Checklist](#), *Cisco Unified CallManager System Guide*
- [Application Users and End Users](#), *Cisco Unified CallManager System Guide*
- [Cisco Extension Mobility](#), *Cisco Unified CallManager Features and Services Guide*
- [Associating a User Device Profile to a User](#), *Cisco Unified CallManager Features and Services Guide*
- [Cisco Unified CallManager Assistant With Proxy Line Support](#), *Cisco Unified CallManager Features and Services Guide*
- [Cisco Unified CallManager Assistant With Shared Line Support](#), *Cisco Unified CallManager Features and Services Guide*



Role Configuration

Roles allow Cisco Unified CallManager administrators who have full administration privilege (access) to configure end users and application users with different levels of privilege. Administrators with full administration privilege configure roles and user groups. In general, full-access administration users configure the privilege of other administration users and end users to Cisco Unified CallManager Administration and to other applications.

Different levels of privilege exist for each application. For the Cisco Unified CallManager Administration application, two levels of privilege exist: read privilege and update privilege. These privilege levels differ as follows:

- Users with update privilege can view and modify the Cisco Unified CallManager Administration windows to which the user's user group has update privilege.
- A user with read privilege can view the Cisco Unified CallManager Administration windows that belong to the roles to which the user's user group has read privilege. A user with read privilege for a window cannot, however, make any changes on those administration windows to which the user has only read privilege. For a user with read privilege, the Cisco Unified CallManager Administration application does not display any update buttons nor icons.

Roles comprise groups of resources for an application. At installation, default standard roles get created for various administrative functions. You may, however, create custom roles that comprise custom groupings of resources for an application.



Note

Certain standard roles have no associated application nor resource. These roles provide login authentication for various applications.

Use the following topics to configure roles:

- [Finding a Role, page 88-2](#)
- [Configuring a Role, page 88-3](#)
- [Deleting a Role, page 88-4](#)
- [Role Configuration Settings, page 88-4](#)

Additional Information

See the [“Related Topics”](#) section on page 88-5.

Finding a Role

Because you might have several roles in your network, Cisco Unified CallManager lets you locate specific roles on the basis of specific criteria. Use the following procedure to locate roles.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your role search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your role search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **User Management > Role**.

The Find and List Roles window displays. Use the two drop-down list boxes to search for a role.

Step 2 From the first Find Role where drop-down list box, choose one of the following criteria:

- Name
- Application

From the second Find Role where drop-down list box, choose one of the following criteria:

- begins with
- contains
- is exactly
- ends with
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Tip

To find all roles that are registered in the database, click **Find** without entering any search text.

A list of discovered roles displays by

- Name
- Application
- Description



Tip

To search for roles within the search results, click the **Search Within Results** check box and enter your search criteria as described in this step.



Note

You can delete multiple roles from the Find and List Roles window by checking the check boxes next to the appropriate roles and clicking **Delete Selected**. You can delete all roles in the window by clicking **Select All** and then clicking **Delete Selected**.



Note You cannot delete standard roles.

- Step 4** From the list of records, click the role name that matches your search criteria.
The window displays the role that you choose.

Additional Information

See the [“Related Topics” section on page 88-5](#).

Configuring a Role

This section describes how to add a role to Cisco Unified CallManager Administration.

Procedure

- Step 1** Choose **User Management > Role**.
The Find and List Roles window displays.
- Step 2** Perform one of the following tasks:
- To copy an existing role, locate the appropriate role as described in the [“Finding a Role” section on page 88-2](#) and click the **Copy** button next to the role that you want to copy. In the popup window that displays, enter a name for the new role and click **OK**. Continue with [Step 4](#).
-  **Note** Copying a role also copies the privileges that are associated with that role.
- To add a new role, click the Add New button, and continue with [Step 3](#).
 - To update an existing role, locate the appropriate role as described in the [“Finding a Role” section on page 88-2](#) and continue with [Step 4](#).
- Step 3** If you are adding a new role, choose an application from the Application drop-down list box and click **Next**.
- Step 4** In the Role Configuration window that displays, enter the appropriate settings as described in [Table 88-1](#).
- Step 5** To add the role, click **Save**.
The new role gets added to the Cisco Unified CallManager database.

Additional Information

See the [“Related Topics” section on page 88-5](#).

Deleting a Role

This section describes how to delete a role in Cisco Unified CallManager Administration.

Procedure

- Step 1

Choose **User Management > Role**.
The Role Configuration window displays.
- Step 2

In the list of Roles at left, click the name of the role that you want to delete.



Note You cannot delete a standard role.

The role that you chose displays.

- Step 3

Click **Delete**.
You receive a message that asks you to confirm the deletion.
- Step 4

Click **OK**.
The window refreshes, and the role gets deleted from the database.

Additional Information

See the [“Related Topics”](#) section on page 88-5.

Role Configuration Settings

[Table 88-1](#) describes the role configuration settings. For related procedures, see the [“Related Topics”](#) section on page 88-5.

Table 88-1 Role Configuration Settings

Field	Description
Role Information	
Application	From the drop-down list box, choose the application with which this role associates.
Name	Enter a name for the role. Names can have up to 50 characters.
Description	Enter a description for the role. Descriptions can have up to 50 characters.
Resource Access Information	
(list of resource names for the chosen application)	In the Resource Access Information pane, click the check box(es) next to the resource(s) that you want this role to include. Note In some applications, only one check box applies for each resource. In the Cisco Unified CallManager Administration application, a read check box and an update check box apply to each resource.

Table 88-1 **Role Configuration Settings (continued)**

Field	Description
Grant access to all	Click this button to grant privileges for all resources that display on this page for this role. Note If the list of resources displays on more than one page, this button applies only to the resources that display on the current page. You must display other pages and use the button on those pages to change the access of the resources that are listed on those pages.
Deny access to all	Click this button to remove privileges for all resources that display on this page for this role. Note If the list of resources displays on more than one page, this button applies only to the resources that display on the current page. You must display other pages and use the button on those pages to change the access of the resources that are listed on those pages.

Related Topics

- [Finding a Role, page 88-2](#)
- [Configuring a Role, page 88-3](#)
- [Deleting a Role, page 88-4](#)
- [Role Configuration Settings, page 88-4](#)
- [User Group Configuration, page 89-1](#)
- [Roles and User Groups, Cisco Unified CallManager System Guide](#)



User Group Configuration

The role and user group menu options in the Cisco Unified CallManager Administration User Management menu allow users with full access to configure different levels of window access for Cisco Unified CallManager administrators. Users with full access configure roles, user groups, and access privileges for roles. In general, full-access users configure the access of other users to Cisco Unified CallManager Administration.

User groups comprise lists of application users and end users. A user may belong to multiple user groups. After you add a user group, you then add users to a user group. Afterward, you may proceed to assign roles to a user group. If a user belongs to multiple user groups, the MLA permission enterprise parameter determines the effective privilege of the user.

Use the following topics to configure user groups, assign users to user groups, and view a user's roles, user groups, and permissions:

- [Finding a User Group, page 89-1](#)
- [Configuring a User Group, page 89-3](#)
- [Deleting a User Group, page 89-3](#)
- [Adding Users to a User Group, page 89-4](#)
- [Deleting Users from a User Group, page 89-6](#)
- [Assigning Roles to a User Group, page 89-6](#)
- [Viewing a User's Roles, User Groups, and Permissions, page 89-7](#)

Finding a User Group

Because you might have several user groups in your network, Cisco Unified CallManager lets you locate specific user groups on the basis of specific criteria. Use the following procedure to locate user groups.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your user group search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your user group search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **User Management > User Group**.

The Find and List User Groups window displays. Use the two drop-down list boxes to search for a user group.

Step 2 From the first Find User Group where drop-down list box, choose the following criterion:

- Name

From the second Find User Group where drop-down list box, choose one of the following criteria:

- begins with
- contains
- is exactly
- ends with
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.



Tip

To find all user groups that are registered in the database, click **Find** without entering any search text.

A list of discovered user groups displays by

- Name
- Roles (icon)



Tip

To search for user groups within the search results, click the **Search Within Results** check box and enter your search criteria as described in this step.



Note

You can delete multiple user groups from the Find and List User Groups window by checking the check boxes next to the appropriate user groups and clicking **Delete Selected**. You can delete all user groups in the window by clicking **Select All** and then clicking **Delete Selected**.



Note

You cannot delete the standard user groups.

Step 4 From the list of records, click the user group name that matches your search criteria.

The window displays the user group that you choose.

Additional Topics

See the [“Related Topics” section on page 89-8](#).

Configuring a User Group

This section describes how to add, copy and update a user group to and in the Cisco Unified CallManager Administration.

Procedure

Step 1 Choose **User Management > User Group**.

The Find and List User Groups window displays.

Step 2 Perform one of the followings tasks:

- To copy an existing user group, locate the appropriate user group as described in [“Finding a User Group” section on page 89-1](#) and click the **Copy** button next to the user group that you want to copy. In the popup window that displays, enter a name for the new user group and click **OK**. Continue with [Step 3](#).
- To add a new user group, click the **Add New** button. Enter a name for the new user group and click **OK**. Continue with [Step 3](#).



Note The user group name can contain up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that the user group name is unique.

- To update an existing user group, locate the appropriate user group as described in [“Finding a User Group” section on page 89-1](#). Click the name of the user group that you want to update. The user group that you chose displays. Update the appropriate settings. Continue with [Step 3](#).



Note You cannot delete a standard user group, but you can update the user membership for a standard user group.

Step 3 Click **Save**.

Step 4 Proceed to add users to this user group. See [Adding Users to a User Group, page 89-4](#).

Step 5 Proceed to assign roles to the user group. See [Assigning Roles to a User Group, page 89-6](#).

Additional Topics

See the [“Related Topics” section on page 89-8](#).

Deleting a User Group

This section describes how to delete a user group from Cisco Unified CallManager Administration. Use the following procedure to delete a user group entirely. If you want to delete only certain users from a user group, refer to the [“Deleting Users from a User Group” section on page 89-6](#).

Before You Begin

When you delete a user group, Cisco Unified CallManager removes all user group data from the database. To find out which roles are using the user group, in the User Group Configuration window, choose **Dependency Records** from the Related Links drop-down list box and click **Go**. If dependency records are not enabled for the system, the Dependency Records Summary window displays a message. For more information about dependency records, see the [“Accessing Dependency Records” section on page A-2](#).

Procedure

-
- Step 1** Choose **User Management > User Group**.
The Find and List User Groups window displays.
- Step 2** Find the user group that you want to delete by using the procedure in the [“Finding a User Group” section on page 89-1](#).
- Step 3** Click the name of the user group that you want to delete.
The user group that you chose displays. The list shows the users in this user group in alphabetical order.
- Step 4** If you want to delete the group entirely, click **Delete**.
A dialog box displays to warn you that you cannot undo deletion of user groups.
- Step 5** To delete the user group, click **OK** or to cancel the action, click **Cancel**. If you click **OK**, Cisco Unified CallManager removes the user group from the database.
-

Additional Topics

See the [“Related Topics” section on page 89-8](#).

Adding Users to a User Group

This section describes how to add end users and application users to a user group in Cisco Unified CallManager Administration.

Procedure

-
- Step 1** Choose **User Management > User Group**.
The Find and List User Groups window displays.
- Step 2** Find the user group to which you want to add users. Use the procedure in the [“Finding a User Group” section on page 89-1](#).
- Step 3** Click the name of the user group that you want to update.
The user group that you chose displays. The Users in Group list shows the users that currently belong to the user group.
- Step 4** To add end users, click **Add Users to Group**. To add application users, skip to [Step 8](#).
The Find and List Users window displays.

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



Note You can perform the search for users in a variety of ways. You can enter the first name, middle name, last name, user ID, or department of a user. Alternatively, you can leave the field blank, which results in display of all users.

A list of end users that matches your search criteria displays.



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

Step 6 In the list of search results, click the check box next to the users that you want to add to this user group. If the list comprises multiple pages, use the links at the bottom to see more results.

Step 7 Click **Add Selected**.

The User Group Configuration window redisplay with the users that you added listed in the Users in Group pane.



Note After you add a user, you can view the user's roles by clicking the **i** icon in the Permission column for that user.

Step 8 To add application users, click **Add Application Users to Group**.

The Find and List Application Users window displays.

Step 9 Use the Find Application User drop-down list boxes to find the application users that you want to add and click **Find**.



Note You can perform the search for application users by searching for user ID. Alternatively, you can leave the field blank, which results in display of all application users.

A list of application users that matches your search criteria displays.

Step 10 In the list of search results, click the check box next to the application users that you want to add to this user group. If the list comprises multiple pages, use the links at the bottom to see more results.



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

Step 11 Click **Add Selected**.

The User Group Configuration window redisplay with the application users that you added listed in the Users in Group pane.



Note After you add an application user, you can view the user's roles by clicking the **i** icon in the Permission column for that user.

Step 12 To save your changes to this user group, click **Save**.

Additional Topics

See the [“Related Topics”](#) section on page 89-8.

Deleting Users from a User Group

This section describes how to delete users from a user group in Cisco Unified CallManager Administration.

Procedure

-
- Step 1** Choose **User Management > User Group**.
The Find and List User Groups window displays.
- Step 2** Find the user group from which you want to delete users. Use the procedure in the [“Finding a User Group”](#) section on page 89-1.
- Step 3** Click the name of the user group that you want to update.
The user group that you chose displays. The Users in Group list shows the users that currently belong to the user group.
- Step 4** Click the check boxes next to the names of the users that you want to delete from this user group.
- Step 5** Click **Delete Selected**.
A confirmation message asks you to confirm the deletion.
- Step 6** To delete the selected user group members, click **OK** or click **Cancel** to exit this window.
The User Group redisplay with the deleted users removed from the Users in Group pane.
-

Additional Topics

See the [“Related Topics”](#) section on page 89-8.

Assigning Roles to a User Group

Users with full access can assign roles to user groups. A user group that has assigned roles has access to the resources that the role comprises.

This section describes assigning roles to a user group in Cisco Unified CallManager Administration.

**Note**

When an administrator assigns roles to a user group, the administrator should assign the Standard CCM Admin Users role to the user group. This role enables the users to log into Cisco Unified CallManager Administration.

Procedure

-
- Step 1** Choose **User Management > User Group**.
The Find and List User Groups windows displays.

- Step 2** Find the user group to which you want to assign roles. Use the procedure in the [“Finding a User Group” section on page 89-1](#).
- Step 3** Click the name of the user group for which you want to assign roles.
- The user group that you chose displays. The Users in Group list shows the users that currently belong to the user group.
- Step 4** From the Related Links drop-down list box, choose **Assign Role to User Group** and click **Go**.
- The User Group Configuration window changes to display the Role Assignment pane. For the user group that you chose, the list of assigned roles displays. Choose one of the following options:
- To assign roles to the user group, go to [Step 5](#).
 - To delete roles from the user group, go to [Step 9](#).
- Step 5** To assign additional roles to the user group, click **Assign Role to Group**.
- The Find and List Roles popup window displays.
- Step 6** If necessary, use the Find Role search criteria to narrow the list of roles.
- Step 7** Choose the roles to assign to this user group by clicking the check boxes next to the role names. To close the Find and List Roles popup window without assigning roles to this user group, click **Close**.
- Step 8** Click **Add Selected**.
- The Find and List Roles popup window closes. The chosen roles get added to the Role Assignment pane for this user group. If you do not want to delete any assigned roles for this user group, skip to [Step 10](#).
- Step 9** To delete an assigned role from the user group, select a role in the Role Assignment pane and click **Delete Role Assignment**. Repeat this step for each role that you want to delete from this user group.
- Step 10** Click **Save**.
- The system makes the added and deleted role assignments to the user group in the database.

Additional Topics

See the [“Related Topics” section on page 89-8](#).

Viewing a User's Roles, User Groups, and Permissions

This section describes how to view the roles, user groups, and permissions that are assigned to a user that belongs to a specified user group. Use the following procedure to view the roles, user groups, and permissions that are assigned to a user in a user group.



Note

You can also view user roles by using **User Management > Application User** (for application users) or **User Management > End User** (for end users) to view a particular user and then display the user roles.

Procedure

- Step 1** Choose **User Management > User Group**.
- The Find and List User Groups window displays.

- Step 2** Find the user group that has the users for which you want to display assigned roles. Use the procedure in the [“Finding a User Group” section on page 89-1](#).
- Step 3** Click the name of the user group for which you want to view the roles that are assigned to the users. The User Group Configuration window displays for the user group that you chose. The Users in Group pane shows the users that belong to the user group.
- Step 4** For a particular user, click the **i** icon in the Permission column for the user. The User Privilege window displays. For the user that you chose, the following information displays:
- User groups to which the user belongs
 - Roles that are assigned to the user
 - Resources to which the user has access. For each resource, the following information displays:
 - Application
 - Resource
 - Permission (*read* and/or *update*)
- Step 5** To return to the user, choose **Back to User** in the Related Links drop-down list box and click **Go**.
-

Additional Topics

See the [“Related Topics” section on page 89-8](#).

Related Topics

- [Finding a User Group, page 89-1](#)
- [Configuring a User Group, page 89-3](#)
- [Deleting a User Group, page 89-3](#)
- [Adding Users to a User Group, page 89-4](#)
- [Deleting Users from a User Group, page 89-6](#)
- [Assigning Roles to a User Group, page 89-6](#)
- [Viewing a User’s Roles, User Groups, and Permissions, page 89-7](#)
- [Roles and User Groups, Cisco Unified CallManager System Guide](#)
- [End User Configuration, Cisco Unified CallManager System Guide](#)
- [Application User Configuration, Cisco Unified CallManager System Guide](#)



User/Phone Add Configuration

The End User, Phone, DN, and LA Configuration window in Cisco Unified CallManager Administration provides a single window that allows the administrator to perform the basic steps that are required to add a new user and assign the user to a new phone. While you add a new end user and associate the end user with a new phone, you can also use this window to configure a new directory numbers (DN) and line appearance (LA) information for the new end phone.



Note

The End User, Phone, DN, and LA Configuration window does not allow you to enter existing end users, phones, or directory numbers.

The End User, Phone, DN, and LA Configuration window adds records of the following types:

- End users
- Phones
- Directory numbers
- Device profiles



Note

You can modify end user information only if synchronization with an LDAP server is not enabled. To check whether synchronization with an LDAP server is enabled, use the **System > LDAP > LDAP System** menu option. In the LDAP System window that displays, ensure that the Enable Synchronizing from LDAP Server check box is not checked. If synchronization is enabled, you can view end user data, but you cannot modify the end user data.

The following topics contain information on adding end users, phones, directory numbers, and line appearances by using the End User, Phone, DN, and LA Configuration window:

- [Adding an End User and Phone, page 90-2](#)
- [User and Device Configuration Settings, page 90-2](#)

Additional Information

See the [“Related Topics” section on page 90-4](#).

Adding an End User and Phone

The following procedure provides instructions on adding an end user and phone and associating the user and phone with a directory number and device profile.

Procedure

Step 1 Choose **User Management > User/Phone Add**.

The End User, Phone, DN, and LA Configuration window displays.



Note

Before you proceed, you can use the links in the Related Links drop-down list box at the top, right of the End User, Phone, DN, and LA Configuration window to determine whether an end user or phone already exists.

To find out which end users already exist, choose **Back to Find List Users** in the Related Links drop-down list box and click **Go**. Use the Find and List Users window that displays to search for the end user ID that you plan to add. If the end user ID already exists, you cannot use the User/Phone Add menu option to add this end user.

To find out which phones already exist, choose **Back to Find List Phones** in the Related Links drop-down list box and click **Go**. Use the Find and List Phones window that displays to search for the phone that you plan to add. If the phone already exists, you cannot use the User/Phone Add menu option to add this phone.

If you use either of the Related Links, repeat [Step 1](#) to return to the End User, Phone, DN, and LA Configuration window.

Step 2 Enter the appropriate settings as described in [Table 90-1](#).

Step 3 When you complete the end user and device addition and have associated the user and device with a directory number, save your changes and add the end user and device by clicking **Save**.

Additional Information

See the [“Related Topics” section on page 90-4](#).

User and Device Configuration Settings

[Table 90-1](#) describes the end user configuration settings. For related procedures, see the [“Related Topics” section on page 90-4](#).

Table 90-1 *User and Device Configuration Settings*

Field	Description
User Information	
LDAP Sync Status	This field displays the LDAP synchronization status, which is set with the System > LDAP > LDAP System menu option.

Table 90-1 **User and Device Configuration Settings (continued)**

Field	Description
User ID	Enter the end user identification name. Cisco Unified CallManager does not permit modifying the user ID after it is created. You may use the following special characters: =, +, <, >, #, ;, \, , "", and blank spaces.
Password	Enter five or more alphanumeric or special characters for the end user password. You may use the following special characters: =, +, <, >, #, ;, \, , "", and blank spaces.
Confirm Password	Enter the end user password again.
PIN	Enter five or more numeric characters for the Personal Identification Number.
Confirm PIN	Enter the PIN again.
Last Name	Enter the end user last name. You may use the following special characters: =, +, <, >, #, ;, \, , "", and blank spaces.
Middle Name	Enter the end user middle name. You may use the following special characters: =, +, <, >, #, ;, \, , "", and blank spaces.
First Name	Enter the end user first name. You may use the following special characters: =, +, <, >, #, ;, \, , "", and blank spaces.
Device Associations	
Product Type	This list box displays the types of devices that are available for association with this end user. From the drop-down list box, choose the type of device to associate with this end user.
MAC Address	Enter a unique MAC address for the new device that you are associating with the new user. The MAC address comprises exactly 12 hexadecimal digits (0 to 9, A to F).
Calling Search Space DN	From the drop-down list box, choose the calling search space for the directory number that you are associating with this user and device.
Calling Search Space Phone	From the drop-down list box, choose the calling search space for the phone that you are associating with this user and device.

Table 90-1 **User and Device Configuration Settings (continued)**

Field	Description
External Phone Number Mask	Specify the mask that is used to format caller ID information for external (outbound) calls that are made from the associated device. - The mask can contain up to 24 characters. Valid characters specify 0 to 9, *, #, and X. - Enter the literal digits that you want to appear in the caller ID information and use Xs to represent the directory number of the associated device. - See the following examples: If you specify a mask of 972813XXXX, an external call from extension 1234 displays a caller ID number of 9728131234 if the Use External Phone Number Mask option is checked on the route pattern that is used to make the external call. If you specify a mask of all literal digits, such as 9728135000 to represent a main attendant number, that literal number (9728135000) displays as the caller ID for an external call from any associated device.
Extension	This field represents the primary directory number for the end user. End users can have multiple lines on their phones. Enter an extension for the new user and phone. You may use the following characters: 0 to 9, ?, [,], +, -, *, ^, #, !.
Partition	From the drop-down list box, choose a partition for the directory number that you specified in the Extension field.
Voice Mail Profile	From the drop-down list box, choose a voice-mail profile for the directory number. Choose <None> to use the system default.
Enable Extension Mobility	Check this check box to enable extension mobility. After you have added the new user, you can use the User Management > End User menu option to choose an Extension Mobility profile.

Additional Information

See the [“Related Topics”](#) section on page 90-4.

Related Topics

- [Adding an End User and Phone, page 90-2](#)
- [User and Device Configuration Settings, page 90-2](#)
- [Application Users and End Users, Cisco Unified CallManager System Guide](#)
- [Cisco Unified IP Phones, Cisco Unified CallManager System Guide](#)
- [Understanding Directory Numbers, Cisco Unified CallManager System Guide](#)
- [Finding an End User, page 87-1](#)
- [Adding an End User, page 87-3](#)

- [End User Configuration Settings](#), page 87-5
- [Changing an End User Password](#), page 87-8
- [Changing an End User PIN](#), page 87-9
- [Associating Devices to an End User](#), page 87-10
- [Associating Cisco Extension Mobility Profiles](#), page 87-12
- [LDAP System Configuration](#), page 12-1
- [Directory Number Configuration](#), page 49-1
- [CTI Route Point Configuration](#), page 67-1
- [Cisco Unified IP Phone Configuration](#), page 70-1
- [Cisco Extension Mobility](#), *Cisco Unified CallManager Features and Services Guide*
- [Associating a User Device Profile to a User](#), *Cisco Unified CallManager Features and Services Guide*



Application User CAPF Profile Configuration

The Application User CAPF Profile Configuration window in Cisco Unified CallManager Administration allows you to issue locally significant certificates to secure application users. After you issue the certificate and perform other security-related tasks, a TLS connection opens between the CTIManager service and the application that is activated on the server.

One Application User CAPF Profile corresponds to a single instance of an application on a server. For example, if you activate an application on two servers in the cluster, you must configure two Application User CAPF Profiles, one for each server. If you activate two different applications on the same server, you must configure two Application User CAPF Profiles, one for each application on the server.

For information on how to configure the Application User CAPF Profile, refer to the *Cisco Unified CallManager Security Guide*.





End User CAPF Profile Configuration

The End User CAPF Profile Configuration window in Cisco Unified CallManager Administration allows you to issue locally significant certificates to CTI clients. After you issue the certificate and perform other security-related tasks, the CTI client communicates with the CTIManager service via a TLS connection.

For information on how to configure the End User CAPF Profile, refer to the *Cisco Unified CallManager Security Guide*.



SIP Realm Configuration

When you configure digest authentication for SIP trunks, Cisco Unified CallManager challenges the identity of the SIP user agent that connects to the trunk every time the trunk sends a SIP request to Cisco Unified CallManager; the SIP user agent, in turn, can challenge the identity of Cisco Unified CallManager. For Cisco Unified CallManager to respond to the SIP user agent, you must configure the SIP realm for Cisco Unified CallManager.

For information on how to configure SIP realm for Cisco Unified CallManager, refer to the *Cisco Unified CallManager Security Guide*.



PART 9

Cisco Unified CallManager Bulk Administration





Bulk Administration Tool

The Cisco Unified CallManager Bulk Administration Tool (BAT), a web-based application, performs bulk transactions to the Cisco Unified CallManager database. BAT lets you add, update, or delete a large number of similar phones, users, or ports at the same time. When you use Cisco Unified CallManager Administration, each database transaction requires an individual manual operation, while BAT automates the process and achieves faster add, update, and delete operations.

You can use BAT to work with the following types of devices and records:

- Add, update, and delete Cisco Unified IP Phones including voice gateway chalice (VGC) phones, computer telephony interface (CTI) ports, and H.323 clients
- Add, update, and delete users
- Add, update, and delete User Device Profiles
- Add, update, and delete Cisco Unified CallManager Assistant managers and assistants
- Add, update, and delete ports on a Cisco Catalyst 6000 FXS Analog Interface Module
- Add or delete Cisco VG200 analog gateways and ports
- Add or delete Forced Authorization Codes
- Add or delete Client Matter Codes
- Add or delete Call Pickup Groups

You can also work with these devices in combination with the user information. For example, when you add CTI ports and users, BAT allows you to “Enable CTI Application Use.” This saves time when you are adding users who have applications that require a CTI port, such as Cisco IP SoftPhone.

An optional component of BAT, the Tool for Auto-Registered Phones Support (TAPS), further reduces the manual labor that is involved in administering a large system. When you need to add a large block of new phones, you can use BAT to add the devices with dummy media access control (MAC) addresses instead of entering each MAC address in the data input file. After the phones are installed, the phone users or the administrator can call the TAPS directory number, follow the voice prompts, and download the correct user device profiles for their phones.

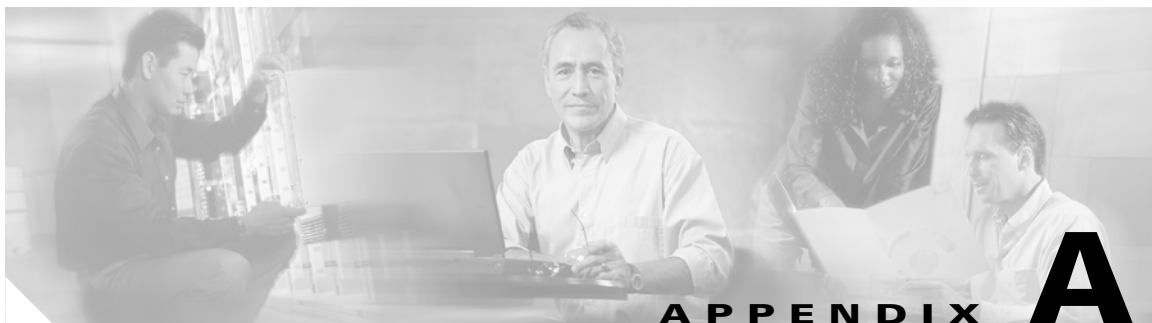
For more information about the BAT and TAPS, refer to the *Cisco Unified CallManager Bulk Administration Guide*.



PART 10

Appendixes





Dependency Records

This appendix provides information about the dependency record windows in Cisco Unified CallManager Administration. These windows help you to determine which records in the database use other records. For example, you can determine which devices (such as CTI route points or phones) use a particular calling search space.

If you need to delete a record from Cisco Unified CallManager, you can use dependency records to show which records are associated with the record that you want to delete. You can then reconfigure those records, so they are associated with a different record.

This appendix contains the following sections:

- [Enabling Dependency Records, page A-1](#)
- [Disabling Dependency Records, page A-2](#)
- [Accessing Dependency Records, page A-2](#)
- [Dependency Records Buttons, page A-4](#)

Enabling Dependency Records

To access dependency records, you must first enable them. The system disables dependency records by default. To enable the dependency records, perform the following procedure.



Caution

Enabling the dependency records functionality causes high CPU usage. This task executes at below-normal priority and may take time to complete due to dial plan size and complexity, CPU speed, and the CPU requirements of other applications.

Procedure

-
- Step 1** Choose **System > Enterprise Parameters**
 - Step 2** Scroll to the CCMAAdmin Parameters area of the window.
 - Step 3** From the Enable Dependency Records drop-down list box, choose True.

A dialog box displays with a message about the consequences of enabling the dependency records. Read the information carefully before clicking OK.

- Step 4** Click **OK**.
The field displays True.
- Step 5** Click **Save**.
-

Disabling Dependency Records

If you have dependency records enabled and your system is experiencing CPU usage issues, you can disable dependency records. (The system disables dependency records by default.) To disable the dependency records, perform the following procedure.

Procedure

- Step 1** Choose **System > Enterprise Parameters**.
- Step 2** Scroll to the CCMAAdmin Parameters area of the window.
- Step 3** From the Enable Dependency Records drop-down list box, choose False.
A dialog box displays with a message about dependency records. Read the information carefully before clicking OK.
- Step 4** Click **OK**.
The field displays False.
- Step 5** Click **Save**.
-

Accessing Dependency Records

To access dependency records from Cisco Unified CallManager configuration windows, choose **Dependency Records** from the Related Links box and click **Go**. The Dependency Records—Summary window displays. This window displays the number and type of records that use the record that is shown in the Cisco Unified CallManager configuration window.



Note

If the dependency records are not enabled, the Dependency Records—Summary window displays a message, not the information about the record. To enable dependency records, see the [“Enabling Dependency Records”](#) section on page A-1.

For example, if you display a the Default device pool in the Device Pool Configuration window and click the Dependency Records link, the Dependency Records Summary window displays all the records that use that device pool, as shown in [Figure A-1](#).

Figure A-1 **Dependency Records—Summary Example**

To display detailed dependency records information, click the record about which you want more information; for example, click the trunk record. The Dependency Records Detail window displays, as shown in [Figure A-2](#). If you want to return to the original configuration window, choose Back to Summary from the Related List Box and click **Go**, then choose Back to <configuration window name> and click **Go** or click the **Close and go Back** button.

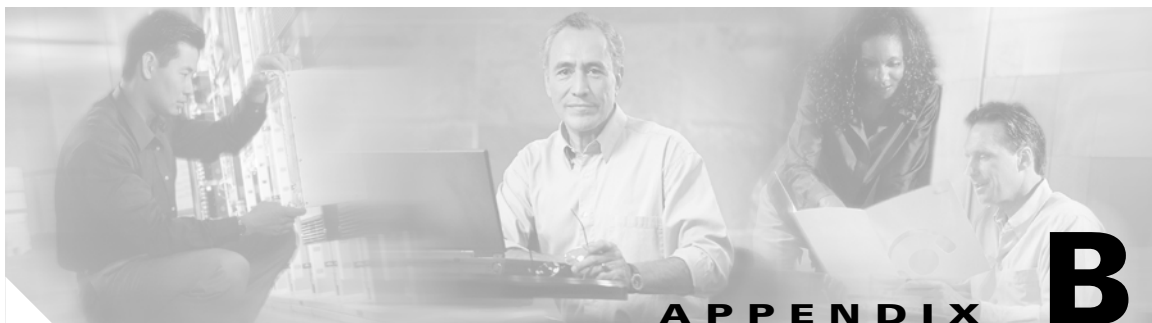
Figure A-2 *Dependency Records—Detail Example*

To display the configuration window of the record that is displayed in the Dependency Records Detail window, click the record. The configuration window for that record displays. For example, if you click the h225trunk record that is shown in [Figure A-2](#), the Trunk Configuration window displays with information about the h225trunk.

Dependency Records Buttons

Three buttons display in the Dependency Records Summary window:

- Refresh—Updates the window with current information.
- Close—Closes the window but does not return to the Cisco Unified CallManager configuration window in which you clicked the Dependency Records link.
- Close and Go Back—Closes the window and returns to the Cisco Unified CallManager configuration window in which you clicked the Dependency Records link.



Cisco Unity Voice-Mail Port Adjustments

Migration from Cisco CallManager 3.3(3) to Cisco Unified CallManager 4.0(1) required adjustments to the voice-mail port settings. This appendix describes the changes required to Cisco Unity voice-mail ports upon upgrade to Cisco Unified CallManager, Release 4.0 or later. The appendix covers the following topics:

- [Cisco Unity Voice-Mail Port Changes, page B-1](#)
- [Changes After Upgrading to Cisco Unified CallManager 4.0 or Later Releases, page B-1](#)
- [Before Upgrading to Cisco Unified CallManager 4.0 or Later Releases, page B-3](#)
- [Cisco Unity Failover Voice-Mail Port Setup, page B-3](#)

Cisco Unity Voice-Mail Port Changes

This section describes various voice-mail port configurations in Cisco Unified CallManager. Use the scenarios and procedures that follow to ensure that migration from Cisco CallManager 3.3(x) to Cisco Unified CallManager 4.0 or later releases properly migrates the voice-mail port settings. This section describes voice-mail port configurations in Cisco CallManager 3.3(x) as well as the expected configuration after migration to Cisco Unified CallManager 4.0 or later releases. This section also describes the voice-messaging system changes that take place after you upgrade your system to Cisco Unified CallManager 4.0 or later releases.

This section contains the following topics:

- [Changes After Upgrading to Cisco Unified CallManager 4.0 or Later Releases, page B-1](#)
- [Before Upgrading to Cisco Unified CallManager 4.0 or Later Releases, page B-3](#)
- [Cisco Unity Failover Voice-Mail Port Setup, page B-3](#)

Changes After Upgrading to Cisco Unified CallManager 4.0 or Later Releases

You will need to reconfigure a few items to maintain your original voice-mail port functionality, depending on what type of scenario you have set up. You must also change your setup as described in this section.

Things That May Affect Your Setup

If your last voice-mail port is forwarded to a route pattern (gateway or intercluster trunk [ICT]), this configuration will no longer exist after the upgrade. You will need to add the intercluster trunk or gateway to a route group, then add the route group to the corresponding route/hunt list of the route patterns that are attached to the voice-mail pilot number. The route group represents the last member of the route/hunt list.

**Note**

Cisco does not recommend use of the Broadcast distribution algorithm in conjunction with the implementation of voice-mail ports for Cisco Unity.

Line Group Forwarding and Cisco Unity Failover

If you are using the recommended Cisco Unity failover voice-mail port setup, you need to configure the following values for the line groups that are used for the voice-mail ports:

- No Answer: Skip Remaining members and go directly to next group.
- Busy: Try Next member, but do not go to next group.
- Not Available: Skip Remaining members and go directly to next group.

The descriptions of the various scenarios throughout this document provide specific information about these values.

If your final voice-mail port is configured to go to an operator, and the operator is set up to Call Forward No Answer (CFNA) and Call Forward Busy (CFB) back to the voice-mail pilot, you will no longer be able to CFB or CFNA back to the same voice-messaging system. You can add an additional line group that contains the operator line to the voice-mail hunt list.

After an upgrade, the system places the line group where the failover voice-mail ports reside in the route/hunt list that is associated with the hunt list pilot number. You need to manually select the hunt options on the basis of your original configuration.

Changes That You Will Notice After the Upgrade

After the upgrade from previous versions of Cisco Unified CallManager to Cisco Unified CallManager 4.0 or later releases, you will notice the following changes:

- The Cisco Voice Mail Port Configuration window no longer has forwarding fields.
- Voice-mail ports now use line groups, route/hunt lists, and hunt pilot numbers. The system creates these entities automatically after the upgrade if the database contained an existing voice-mail port setup. You need to select the hunt options on the basis of your original configurations.
- The pilot number now represents a route pattern that is assigned to the hunt list where the line group of the ports resides.
- Ports in the same server should be in the same line group for the ports to work correctly. Thus, when you add additional ports to an existing server, the system uses the same line group that was used for the first port for the additional ports.
- The system places voice-mail ports in a newly created partition during the upgrade process.
- The system places voice-mail ports that are used for MWI and for outbound calls on their own separate line groups, route/hunt lists, and hunt list pilot numbers.

Before Upgrading to Cisco Unified CallManager 4.0 or Later Releases

Perform the following step on the voice-mail ports to ensure proper migration:

1. **Important:** Remove any call forwarding that is set on voice-mail ports that are used only for outbound calls and message waiting indication.

Cisco Unity Failover Voice-Mail Port Setup

Two supported failover configurations exist. The following white paper discusses these failover configurations: *Cisco Unified CallManager Port Configuration for Cisco Unity Failover (Cisco Unity Versions 4.0 and 3.1(2) and Later)*.

This section provides example configurations in Cisco CallManager 3.3(x) and then outlines what each configuration should resemble after an upgrade to Cisco Unified CallManager 4.0 or later releases occurs. Some manual configuration needs to take place after an upgrade to Cisco Unified CallManager version 4.0 or later releases. This section also outlines these changes.

This section covers the following topics:

- [Cisco Unity Failover Configuration 1 in Cisco CallManager 3.3\(x\) \(Recommended\)](#), page B-3
- [Cisco Unity Failover Configuration 1 After Migration to Cisco Unified CallManager 4.0 or Later Releases \(Recommended\)](#), page B-4
- [Single Cisco Unity Server with Single Cisco Unified CallManager Cluster](#), page B-5
- [Single Cisco Unity Server with Single Cisco Unified CallManager Cluster in Cisco CallManager 3.3\(x\)](#), page B-5
- [Single Cisco Unity Server with Single Cisco Unified CallManager Cluster After Migration to Cisco Unified CallManager 4.0 or Later Releases](#), page B-6

Cisco Unity Failover Configuration 1 in Cisco CallManager 3.3(x) (Recommended)

In this example, on each server, four ports handle incoming calls, and two ports handle outbound calls and MWI. PhoneCSS contains partition(s) that are assigned to subscriber phones, as well as VMPilotNumberPT. VMRestrictedCSS contains only VMRestrictedPT, which is assigned only to VM ports.

Primary Cisco Unity server VM ports configuration:

```
Port 1: (Line: 2001) Device Settings - CSS = PhoneCSS
Port 1: (Line: 2001) Directory Number Settings - Partition = VMPilotNumberPT, CSS =
VMRestrictedCSS
Ports 2 to 6: (Lines: 2002-2006) Device Settings - CSS = PhoneCSS
Ports 2 to 6: (Lines: 2002-2006) Directory Number Settings - Partition = VMRestrictedPT,
CSS = VMRestrictedCSS
Ports 1 to 6: (Lines: 2001-2006) Call Forwarding Settings on Busy and No Answer CSS =
VMRestrictedCSS
Line: 2001, CFNA = 3001, CFB = 2002
Line: 2002, CFNA = 3001, CFB = 2003
Line: 2003, CFNA = 3001, CFB = 2004
Line: 2004, CFNA = 3001, CFB = 2001
Line: 2005, CFNA = 2001, CFB = Blank (for outbound calls and MWI)
Line: 2006, CFNA = 2001, CFB = Blank (for outbound calls and MWI)
```

The following example shows secondary Cisco Unity server VM ports (call does not get sent to operator if all ports are busy or ring no answer [RNA]) configuration:

```
Ports 1 to 6: (Lines: 3001-3006) Device Settings - CSS = PhoneCSS
Ports 1 to 6: (Lines: 3001-3006) Directory Number Settings - Partition = VMRestrictedPT,
CSS = VMRestrictedCSS
Ports 1 to 6: (Lines: 3001-3006) Call Forwarding Settings on Busy and No Answer CSS =
VMRestrictedCSS
Line: 3001, CFNA = 3002, CFB = 3002
Line: 3002, CFNA = 3003, CFB = 3003
Line: 3003, CFNA = 3004, CFB = 3004
Line: 3004, CFNA = 3001, CFB = 3001
Line: 3005, CFNA = 3001, CFB = Blank (for outbound calls and MWI)
Line: 3006, CFNA = 3001, CFB = Blank (for outbound calls and MWI)
```

The following example shows secondary Cisco Unity server VM ports (call gets sent to operator if all ports are busy or RNA) configuration:

```
Ports 1 to 6: (Lines: 3001-3006) Device Settings - CSS = PhoneCSS
Ports 1 to 6: (Lines: 3001-3006) Directory Number Settings - Partition = VMRestrictedPT,
CSS = VMRestrictedCSS
Ports 1 to 6: (Lines: 3001-3006) Call Forwarding Settings on Busy and No Answer CSS =
VMRestrictedCSS
Line: 3001, CFNA = 3002, CFB = 3002
Line: 3002, CFNA = 3003, CFB = 3003
Line: 3003, CFNA = 3004, CFB = 3004
Line: 3004, CFNA = operator DN, CFB = operator DN
Line: 3005, CFNA = 3001, CFB = Blank (for outbound calls and MWI)
Line: 3006, CFNA = 3001, CFB = Blank (for outbound calls and MWI)
```

Cisco Unity Failover Configuration 1 After Migration to Cisco Unified CallManager 4.0 or Later Releases (Recommended)

In this example, on each server, four ports handle incoming calls, and two ports handle outbound calls and MWI. PhoneCSS contains partition(s) that are assigned to subscriber phones, as well as VMPilotNumberPT. VMRestrictedCSS contains only VMRestrictedPT, which is assigned only to VM ports. The VMPilotPartition gets created automatically and gets assigned to the voice-mail ports.

The following example shows primary Cisco Unity server VM ports configuration:

```
Ports 1 to 6: (Lines: 2001-2006) Device Settings - CSS = PhoneCSS
Ports 1 to 6: (Lines: 2001-2006) Directory Number Settings - Partition = VMPilotPartition,
CSS = VMRestrictedCSS
```

The following example shows secondary Cisco Unity server VM ports configuration:

```
Ports 1 to 6: (Lines: 3001-3006) Device Settings - CSS = PhoneCSS
Ports 1 to 6: (Lines: 3001-3006) Directory Number Settings - Partition = VMPilotPartition,
CSS = VMRestrictedCSS
```

The following example shows Line Groups (calls not sent to operator if all ports are busy or RNA) configuration:

1. Line Group Name: LG2001 includes 2001-2004, with the following settings:

```
No Answer: Skip remaining members, and go directly to next group (Because this setting
is not the default, you must set it manually.)
Busy: Try next member, but do not go to next group (Because this setting is not the
default, you must set it manually.)
Not Available: Skip remaining members, and go directly to next group (Because this
setting is not the default, you must set it manually.)
```


2. Line Group Name: LG3001 includes 3001-3004, with the following settings:

No Answer: Try next member, but do not go to next group
 Busy: Try next member, but do not go to next group
 Not Available: Try next member, but do not go to next group

Ensure that these values are set manually after the upgrade.

The following example shows Line Groups (calls sent to the operator if all ports are busy or RNA) configuration:



Note Configure only incoming line groups; line groups that dial out remain the same.

1. Line Group Name: LG2001 includes 2001-2004, with the following settings:

No Answer: Skip remaining members, and go directly to next group
 Busy: Try next member, but do not go to next group
 Not Available: Skip remaining members, and go directly to next group

Ensure that these values are set manually after the upgrade.

2. Line Group Name: LG3001 includes 3001-3004 with the following settings:

No Answer: Try next member, but do not go to next group
 Busy: Try next member, but do not go to next group
 Not Available: Skip remaining members, and go directly to next group

Ensure that these values are set manually after the upgrade.

3. Line Group Name: Operator includes Operator extension (example 1000):

No Answer: Try next member, but do not go to next group
 Busy: Try next member, but do not go to next group
 Not Available: Try next member, but do not go to next group

After an upgrade, a hunt list automatically gets configured as follows:

Hunt List Name: HL2001, includes Line Groups LG2001 and LG3001, and operator LG if used, in this order.

After an upgrade, a hunt pilot automatically gets configured as follows:

Hunt Pilot: 2001, Partition: VMPilotNumberPT, Hunt List: HL2001

Single Cisco Unity Server with Single Cisco Unified CallManager Cluster

This section outlines the voice-mail port configurations with a single Cisco Unity server and a single Cisco Unified CallManager cluster. The examples describe following configurations:

- [Single Cisco Unity Server with Single Cisco Unified CallManager Cluster in Cisco CallManager 3.3\(x\), page B-5](#)
- [Single Cisco Unity Server with Single Cisco Unified CallManager Cluster After Migration to Cisco Unified CallManager 4.0 or Later Releases, page B-6](#)

Single Cisco Unity Server with Single Cisco Unified CallManager Cluster in Cisco CallManager 3.3(x)

In this example, voice-mail ports get configured as follows:

Port 1: (Line: 2001) Device Settings - CSS = PhoneCSS

Port 1: (Line: 2001) Directory Number Settings - Partition = VMPilotNumberPT, CSS = VMRestrictedCSS

Ports 2 to 6: (Lines: 2002-2006) Device Settings - CSS = PhoneCSS

Ports 2 to 6: (Lines: 2002-2006) Directory Number Settings - Partition = VMRestrictedPT,
 CSS = VMRestrictedCSS
 Ports 1 to 6: (Lines: 2001-2006) Call Forwarding Settings on Busy and No Answer CSS =
 VMRestrictedCSS
 Line: 2001, CFNA = 2002, CFB = 2002
 Line: 2002, CFNA = 2003, CFB = 2003
 Line: 2003, CFNA = 2004, CFB = 2004
 Line: 2004, CFNA = 2001, CFB = 2001
 Line: 2005, CFNA = 2001, CFB = Blank (for outbound calls and MWI)
 Line: 2006, CFNA = 2001, CFB = Blank (for outbound calls and MWI)

Single Cisco Unity Server with Single Cisco Unified CallManager Cluster After Migration to Cisco Unified CallManager 4.0 or Later Releases

In this example, voice-mail ports get configured as follows:

Ports 1 to 6: (Lines: 2001-2006) Device Settings - CSS = PhoneCSS
 Ports 1 to 6: (Lines: 2001-2006) Directory Number Settings - Partition = VMPilotPartition,
 CSS = VMRestrictedCSS

Line groups get configured as follows:

Line Group Name: LG2001 includes 2001-2004 with the following settings:

No Answer: Try next member, but do not go to next group
 Busy: Try next member, but do not go to next group
 Not Available: Try next member, but do not go to next group

Create the following line groups for outbound ports:

LG2005, include 2005 and 2006

Configure these line groups with the following settings:

No Answer: Stop hunting. **(Because this setting is not the default, you must set it manually.)**
 Busy: Stop hunting. **(Because this setting is not the default, you must set it manually.)**
 Not Available: Stop hunting. **(Because this setting is not the default, you must set it manually.)**

Hunt lists get configured as follows:

Hunt List Name: HL2001, includes Line Groups LG2001
 Hunt List Name: HL2004, includes Line Groups LG2004 and LG2001, in that order
 Hunt List Name: HL2005, includes Line Groups LG2005 and LG2001, in that order

Hunt pilot gets configured as follows:

Hunt Pilot: 2001, Partition: VMPilotNumberPT, Hunt List: HL2001



Configuring Non-Cisco SIP Phones

Cisco Unified CallManager Release 5.0 supports Cisco SIP IP Phones as well as RFC3261-compliant SIP phones from third-party companies. This appendix describes how to configure the third-party SIP phones by using Cisco Unified CallManager Administration.

This appendix contains the following sections:

- [SIP Phone Configuration Differences, page C-1](#)
- [Third-Party SIP Phone Configuration Checklist, page C-3](#)
- [Where to Find More Information, page C-4](#)

SIP Phone Configuration Differences

[Table C-1](#) provides a comparison overview of the configuration differences between Cisco SIP IP Phones and third-party SIP phones.

Table C-1 *SIP Phone Model Configuration Comparison*

SIP Phone	Integrated with Centralized TFTP	Sends MAC Address	Downloads Softkey File	Downloads Dial Plan File	Supports Cisco Unified CallManager Failover and Fallback	Supports Reset and Restart
Cisco SIP IP Phone model 7911, 7941, 7961, 7970, 7971	Yes	Yes	Yes	Yes	Yes	Yes
Cisco SIP IP Phone model 7940, 7960	Yes	Yes	No	Yes	Yes	Yes
Cisco SIP IP Phone model 7905, 7912	Yes	Yes	No	No	Yes	Yes
Third-party SIP Phone	No	No	No	No	No	No

When third-party SIP phones get configured, the Cisco Unified CallManager database gets updated when the administrator uses Cisco Unified CallManager Administration. The administrator must also perform configuration steps on the third-party SIP phone; see following examples:

- Proxy address in the phone should be the IP or Fully Qualified Domain Name (FQDN) of Cisco Unified CallManager
- Directory number(s) in the phone should match the directory number(s) that are configured for the device in Cisco Unified CallManager Administration
- Digest user ID (sometimes referred to as Authorization ID) in the phone should match the Digest User ID in Cisco Unified CallManager Administration

Consult the documentation that came with the third-party SIP phone for more information. See the [“Third-Party SIP Phone Configuration Checklist”](#) section on page C-3 for Cisco Unified CallManager Administration configuration steps.

How Cisco Unified CallManager Identifies a Third-Party Phone

Because third-party SIP phones do not send a MAC address, they must identify themselves by using digest authentication.

The REGISTER message includes the following header:

```
Authorization: Digest
username="swhite",realm="ccmsipline",nonce="GBauADss2qoWr6k9y3hGGVDAqnLfoLk5",uri
="sip:172.18.197.224",algorithm=MD5,response="126c0643a4923359ab59d4f53494552e"
```

The username, swhite, must match an end user that is configured in the End User Configuration window of Cisco Unified CallManager Administration (see [Adding an End User](#), page 87-3). The administrator configures the SIP third-party phone with the user; for example, swhite, in the Digest User field of Phone Configuration window (see [Configuring Cisco Unified IP Phones](#), page 70-2).



Note

You can assign each end user ID to only one third-party phone (in the Digest User field of the Phone Configuration window). If the same end user ID is assigned as the Digest User for multiple phones, the third-party phones to which they are assigned will not successfully register.

Third-Party SIP Phones and TFTP

Third-party SIP phones do not get configured by using the Cisco Unified CallManager TFTP server. The customer configures them by using the native phone configuration mechanism (usually a web page or tftp file). The customer must keep the device and line configuration in the Cisco Unified CallManager database synchronized with the native phone configuration (for example, extension 1002 on the phone and 1002 in Cisco Unified CallManager). Additionally, if the directory number of a line is changed, ensure that it is changed in both Cisco Unified CallManager Administration and in the native phone configuration mechanism.

Enabling Digest Authentication for Third-Party SIP Phones

To enable digest authentication for third-party SIP phones, the administrator must create a SIP Phone Security Profile. (See [SIP Phone Security Profile Configuration](#) in the *Cisco Unified CallManager Administration Guide*.) On the SIP Phone Security Profile Configuration window, check the Enable Digest Authentication check box. After the security profile is configured, the administrator must assign that security profile to the SIP phone by using the Phone Configuration window. If this check box is not

checked, Cisco Unified CallManager will use digest authentication for purposes of identifying the phone by the end user ID, and it will not verify the digest password. If the check box is checked, Cisco Unified CallManager will verify the password.

**Note**

Cisco Unified CallManager does not support Transport Layer Security (TLS) from third-party SIP phones.

Third-Party SIP Phone Configuration Checklist

Table C-2 provides steps to manually configure a third-party SIP phone by using Cisco Unified CallManager Administration.

Table C-2 *Third-Party SIP Phone Configuration Checklist*

Configuration Steps		Procedures and Related Topics
Step 1	Gather the following information about the phone: • MAC address • Physical location of the phone • Cisco Unified CallManager user to associate with the phone • Partition, calling search space, and location information, if used • Number of lines and associated DNs to assign to the phone	
Step 2	Configure the end user that will be the Digest User. Note If the third-party SIP phone does not support an authorization ID (digest user), create a user with a user ID that matches the DN of the third-party phone. For example, create an end user named 1000 and create a DN of 1000 for the phone. Assign this user to the phone (see Step 8).	Adding an End User, page 87-3
Step 3	Configure the SIP Profile or use the default profile. The SIP Profile gets added to the SIP phone by using the Phone Configuration window. Note Third-party SIP phones use only the SIP Profile Information section of the SIP Profile Configuration window.	Configuring SIP Profiles, page 79-2 Configuring Cisco Unified IP Phones, page 70-2
Step 4	Use one of the pre-defined Non-Secure SIP Profiles, the Standard SIP Profile for Autoregistration, or configure a SIP phone security profile. Enable digest authentication if required.	Enabling Digest Authentication for Third-Party SIP Phones, page C-2 SIP Phone Security Profile Configuration, Cisco Unified CallManager Administration Guide Cisco Unified CallManager Security Guide

Table C-2 Third-Party SIP Phone Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 5	Add and configure the third-party SIP phone by choosing Third-party SIP Device (Advanced) or (Basic) from the Add a New Phone Configuration window. Note Third-party SIP Device (Basic) supports one line and consumes three license units, and Third-party SIP Device (Advanced) supports up to eight lines and video, and consumes six license units.	Configuring Cisco Unified IP Phones, page 70-2
Step 6	Add and configure lines (DNs) on the phone.	Directory Number Configuration, page 49-1
Step 7	In the End User Configuration window, associate the third-party SIP phone with the user by using Device Association and choosing the SIP phone.	Associating Devices to an End User, page 87-10
Step 8	In the Digest User field of the Phone Configuration window, choose the end user that you created in Step 2 .	Phone Configuration Settings, page 70-6
Step 9	Provide power, install, verify network connectivity, and configure network settings for the third-party SIP phone.	Refer to the administration guide that was provided with your SIP phone.
Step 10	Make calls with the third-party SIP phone.	Refer to the user guide that came with your third-party SIP phone.

Where to Find More Information

- [Directory Number Configuration, page 49-1](#)
- [Cisco Unified IP Phone Configuration, page 70-1](#)
- [SIP Profile Configuration, page 79-1](#)
- [End User Configuration, page 87-1](#)
- [Cisco Unified IP Phones](#), *Cisco Unified CallManager System Guide*



A

AAR

- overview [28-1](#)

abbreviated dial

- configuration settings (table) [70-23](#)

accessibility

- accessing buttons and icons [1-7](#)

admission control

- implementing with locations [15-1](#)

analog access gateways and ports

- adding [69-11](#)

Annunciator

- updating [3-2](#)

annunciator [53-1](#)

- configuration settings (table) [53-3](#)

- configuring [53-1](#)

- resetting [53-4](#)

- updating [53-2](#)

application dial rules

- adding [29-2](#)

- configuring [29-1](#)

- deleting [29-4](#)

- finding [29-1](#)

- reprioritizing [29-4](#)

- updating [29-2](#)

application server

- configuration [23-1](#)

- configuration settings (table) [23-3](#)

- configuring [23-1](#)

- deleting [23-2](#)

- finding [23-3](#)

application user

- adding [86-3](#)

- application profiles [86-7](#)

- associating devices to an application user [86-8](#)

- changing password [86-7](#)

- configuration [86-1](#)

- configuration settings (table) [86-3](#)

- finding [86-1](#)

autogenerated device profiles

- configuring directory numbers [75-7](#)

automated alternate routing groups

- configuration settings (table) [28-3](#)

- configuring [28-2](#)

- deleting [28-4](#)

- finding [28-1](#)

- overview [28-1](#)

auto-registration

- configuration settings (table) [27-3](#)

- configuring [27-1](#)

- disabling [27-2](#)

- enabling [27-1](#)

- reusing auto-registration numbers [27-4](#)

B

BAT

- application overview [94-1](#)

BLF/SpeedDial

- configuration settings [70-24](#)

BRI

- gateway configuration [69-33](#)

- ports, adding [69-8](#)

browsing

Cisco Unified CallManager 1-2

security

hypertext transfer protocol 1-4

C

call display restrictions

configuring in translation pattern 46-7

configuring in user device profile 75-3

phone configuration 70-11

calling search spaces

adding 43-2

configuration settings (table) 43-3

configure display in drop-down list box 49-23

configuring 43-1

deleting 43-5

finding 43-1

updating 66-2

call routing

directory numbers

configuration overview 49-1

call waiting

configuration settings 49-22

Cisco SIP IP Phones

third-party SIP device differences C-1

Cisco Unified CallManager

benefits 1-1

browsing into 1-2

configuration settings (table) 3-3

configuring 3-1

finding 3-1

groups

adding 4-3

configuration overview 4-1

configuration settings (table) 4-3

deleting 4-4

finding 4-1

introduction 1-1

key features 1-1

log off 1-3

logon 1-3

more information 1-7

overview 1-1

server configuration 2-1

Cisco Unified CallManager Administration

navigating 1-6

Cisco Unified CallManager Administration Guide

audience xxiv

conventions xxv

organization xxiv

purpose xxiii

related documentation xxv

Cisco Unified CallManager Assistant

configuration wizard 81-1

Cisco Unified CallManager server configuration

software conference bridge 54-3

Cisco Unified IP Phones

configuration overview 70-1

configuring 70-2

deleting 70-5

directory numbers 49-1

displaying MAC address 70-4

finding and listing 70-29

resetting 70-4

templates, phone button

configuring 76-1

Cisco Unified IP Phone Services

adding a service parameter 78-5

configuration settings (table) 78-4

configuring 70-24, 78-1

configuring a service 78-3

deleting a service 78-5

deleting a service parameter 78-7

dependency records 78-5

finding a service 78-2

parameter settings (table) 78-7

subscribing 70-25

- unsubscribing [70-26](#)
- updating [70-26](#)
- updating a service parameter [78-5](#)
- Cisco Unity
 - upgrading to Cisco Unified CallManager 4.0 or later [B-1, B-3](#)
 - user configuration voice mailbox [87-3](#)
 - voice-mail port adjustments [B-1](#)
 - voice-mail port changes [B-1](#)
 - voice-mail port failover [B-3](#)
 - voice-mail port setup [B-3](#)
- Cisco Unity Connection
 - user configuration voice mailbox [87-3](#)
- Cisco Unity or Cisco Unity Connection voice mailbox
 - directory numbers [49-4](#)
- Cisco uOne
 - MWI device, configuring [64-3](#)
- Cisco voice mail
 - adding a new server and ports [63-1](#)
 - adding ports [62-3](#)
 - adding ports with the wizard [63-5](#)
 - configuring [62-1](#)
 - configuring message waiting [64-1](#)
 - configuring port wizard [63-1](#)
 - configuring profile [66-1](#)
 - copying ports [62-3](#)
 - deleting ports [62-6](#)
 - deleting ports with the wizard [63-6](#)
 - finding a message waiting number [64-1](#)
 - finding ports [62-1](#)
 - port configuration settings (table) [62-4](#)
 - port wizard device information configuration settings [63-2](#)
 - port wizard directory number configuration settings [63-3](#)
 - updating ports [62-3](#)
- Cisco voice-mail pilot
 - configuring [65-1, 65-3](#)
 - deleting [65-4](#)
 - finding [65-1](#)
- CMLocal date/time group [6-1](#)
- common phone profiles
 - configuration settings (table) [80-3](#)
 - configuring [80-1, 80-2](#)
 - deleting [80-3](#)
 - dependency records [80-3](#)
 - finding [80-1](#)
- conference bridges
 - adding a Cisco IOS device [54-5](#)
 - adding a Cisco Unified CallManager Conference Bridge (WS-SVC-CMM) [54-8](#)
 - adding a Cisco video conference bridge device [54-6](#)
 - adding a hardware device [54-4](#)
 - Cisco IOS configuration settings (table) [54-6](#)
 - Cisco Unified CallManager Conference Bridge (WS-SVC-CMM) configuration settings (table) [54-9](#)
 - Cisco video configuration settings (table) [54-7](#)
 - configuring [54-1](#)
 - copying a meet-me number pattern [50-2](#)
 - deleting a conference device [54-10](#)
 - deleting a meet-me number pattern [50-4](#)
 - finding [54-2](#)
 - finding a meet-me number pattern [50-1](#)
 - hardware configuration settings (table) [54-5](#)
 - software configuration settings (table) [54-3](#)
 - updating a conference device [54-10](#)
- conventions [xxv](#)
- CTI
 - route points
 - adding [67-2](#)
 - configuration settings (table) [67-3](#)
 - configuring [67-1](#)
 - deleting [67-4](#)
 - finding [67-1](#)
 - resetting [67-5](#)
- custom phone button templates
 - adding [76-2](#)
 - creating 7914 expansion module [76-4](#)

deleting [76-5](#)
 finding [76-1](#)

D

date/time groups

adding [6-3](#)
 configuration settings (table) [6-4](#)
 configuring [6-1](#)
 deleting [6-5](#)
 finding [6-1](#)
 using NTP server configuration with [21-1, 22-1, 91-1, 92-1, 93-1](#)
 using phone NTP reference configuration with [8-1](#)

defaults

devices

configuration settings (table) [72-2](#)
 configuring [72-1, 73-1](#)
 updating [72-1](#)
 with non-firmware loads [73-1](#)

dependency records

accessing [A-2](#)
 buttons [A-4](#)
 Cisco Unified IP Phone Services [78-5](#)
 common phone profile [80-3](#)
 disabling [A-2](#)
 enabling [A-1](#)
 enterprise parameter [A-1](#)
 overview [A-1](#)
 route filters [32-5](#)
 user device profile [75-5](#)
 voice-mail pilot numbers [65-4](#)
 voice-mail ports [62-6](#)
 voice-mail profile [66-3](#)

device defaults

configuration settings (table) [72-2](#)
 configuring [72-1, 73-1](#)
 updating [72-1](#)

device pools

adding [9-3](#)
 configuration settings (table) [9-4](#)
 configuring [9-1](#)
 deleting [9-7](#)
 finding [9-1](#)

device profile defaults

adding [74-1](#)
 configuration settings [74-2](#)
 configuring [74-1](#)
 deleting [74-5](#)
 subscribing a service [74-5](#)

device profiles

adding a user [75-2](#)
 configuring [75-1](#)
 configuring directory numbers for autogenerated device profiles [75-7](#)
 deleting a user profile [75-5](#)
 finding [75-2](#)
 updating a user profile [75-2](#)
 updating autogenerated profile [75-6](#)

devices

Cisco Unified IP Phones

configuration overview [70-1](#)
 configuring [70-2](#)
 defining common characteristics [9-1](#)
 gatekeepers, configuring [68-1](#)
 gateways [69-1](#)
 MWI configuration settings (table) [64-3](#)
 trunks, configuring [71-1](#)
 with non-default firmware loads [73-1](#)

DHCP

activating DHCP monitor service [10-1](#)
 server
 configuration settings (table) [10-4](#)
 configuring [10-4](#)
 deleting [10-5](#)
 finding [10-2](#)
 starting DHCP monitor service [10-2](#)

- subnet
 - configuration settings (table) [11-3](#)
 - configuring [11-2](#)
 - deleting [11-4](#)
 - finding [11-1](#)
 - dial plans
 - configuring route pattern details for a non-NANP dial plan [52-4](#)
 - editing [52-3](#)
 - finding [52-2](#)
 - installing [52-3](#)
 - restarting Cisco CallManager Service [52-6](#)
 - uninstalling [52-6](#)
 - upgrading [52-4](#)
 - dial rules
 - configuring a directory lookup rule [30-2](#)
 - deleting a directory lookup rule [30-4](#)
 - directory lookup configuration settings [30-3](#)
 - directory lookup rule configuration [30-1](#)
 - pattern formats [31-5](#)
 - updating a directory lookup rule [30-2](#)
 - digest authentication
 - enabling for SIP third-party phones [C-2](#)
 - Digital Access PRI ports [69-7](#)
 - Digital Access T1
 - ports [69-7](#)
 - directory
 - Cisco Unity or Cisco Unity Connection voice mailbox [87-3](#)
 - directory lookup dial rules
 - configuration [30-1](#)
 - configuration settings [30-3](#)
 - configuring [30-2](#)
 - deleting [30-4](#)
 - updating [30-2](#)
 - directory numbers
 - calling search space list [49-23](#)
 - call waiting configuration settings [49-22](#)
 - configuration overview [49-1](#)
 - configuration settings (table) [49-6](#)
 - configuring [49-1](#), [49-2](#)
 - creating Cisco Unity or Cisco Unity Connection voice mailbox [49-4](#)
 - deleting unassigned [51-3](#)
 - finding [49-2](#)
 - related topics [49-23](#)
 - removing from phone [49-4](#)
 - updating unassigned [51-3](#)
 - document
 - audience [xxiv](#)
 - conventions [xxv](#)
 - organization [xxiv](#)
 - purpose [xxiii](#)
 - documentation
 - related [xxv](#)
 - Domain Name System (DNS) [2-1](#)
 - domains, MLPP
 - overview [17-1](#)
-
- ## E
- end user
 - adding [87-3](#)
 - adding with phone [90-2](#)
 - associating devices to an end user [87-10](#)
 - changing password [87-8](#)
 - changing PIN [87-9](#)
 - configuration [87-1](#)
 - configuration settings (table) [87-5](#)
 - configuring with phone [90-1](#)
 - deleting [87-13](#)
 - extension mobility [87-12](#)
 - finding [87-1](#)
 - user-related information [87-9](#)
 - end user and device
 - configuration settings (table) [90-2](#)
 - enterprise parameters
 - configuring [18-1](#)

dependency records [A-1](#)

extension mobility

end user [87-12](#)

external phone number mask [27-4](#)

F

firmware loads, devices with non-default [73-1](#)

FXO ports [69-5](#)

FXS ports [69-4](#)

G

gatekeepers

configuration settings (table) [68-3](#)

configuring [68-1](#)

configuring a gatekeeper [68-3](#)

deleting [68-4](#)

finding [68-1](#)

resetting [68-5](#)

gateways

adding [69-1](#)

analog access configuration settings (table) [69-53](#)

analog access gateway, adding [69-11](#)

BRI configuration settings (table) [69-33](#)

Cisco IOS SCCP gateway configuration settings
(table) [69-57](#)

Cisco VG224/VG248 analog gateway, adding [69-12](#)

Cisco VG224/VG248 analog ports, adding [69-12](#)

Cisco VG248 configuration settings (table) [69-56](#)

configuration settings (table) [69-13](#)

configuring [69-1](#)

deleting [69-74](#)

Digital Access PRI configuration settings (table) [69-20](#)

E & M port configuration settings (table) [69-63](#)

finding and listing [69-66](#)

FSX/FXO configuration settings (table) [69-16](#)

ground start port configuration settings (table) [69-63](#)

H.323, adding [69-10](#)

H.323 configuration settings (table) [69-44](#)

ISDN [69-21](#)

ISDN BRI [69-33](#)

loop start port configuration settings (table) [69-62](#)

MGCP

BRI, configuring [69-33](#)

BRI ports, adding [69-8](#)

Cisco IOS, adding [69-2](#)

configuration settings (table) [69-14](#)

Digital Access PRI ports, adding [69-7](#)

FXO ports, adding [69-5](#)

FXS ports, adding [69-4](#)

ports, adding [69-4](#)

T1 ports, adding [69-7](#)

modifying [69-74](#)

non-IOS, adding [69-9](#)

port configuration settings (table) [69-59](#)

ports, adding [69-11](#)

POTS port configuration settings (table) [69-60](#)

PRI [69-21](#)

resetting [69-75](#)

restarting [69-75](#)

SCCP

Cisco IOS, adding [69-8](#)

searching

by calling search space [69-69](#)

by description [69-67](#)

by device name [69-66](#)

by device pool [69-70](#)

by device type [69-72](#)

by directory number [69-68](#)

by route group [69-71](#)

by route pattern [69-68](#)

updating [69-76](#)

groups

Cisco Unified CallManager

configuration settings (table) [4-3](#)

configuring [4-1](#)

date/time
 configuration settings (table) [6-4](#)
 overview [6-1](#)
 presence, configuring [5-1](#)

H

H.323, adding gateways [69-10](#)
 HTTPS
 HTTP over secure sockets layer [1-4](#)
 hunt lists
 adding [37-3](#)
 adding line groups [37-4](#)
 changing the order of line groups [37-5](#)
 configuring [37-1](#)
 deleting [37-6](#)
 finding [37-1](#)
 removing line groups [37-5](#)
 hunt pilots
 configuration settings (table) [38-4](#)
 configuring [38-1, 38-3](#)
 deleting [38-4](#)
 finding [38-1](#)

I

introduction to Cisco Unified CallManager [1-1](#)
 IP address [2-1](#)
 IP Phone Services
 See Cisco Unified IP Phone Services
 ISDN, gateway configuration [69-21](#)
 ISDN BRI, gateway configuration [69-33](#)

K

keypad templates, configuring [76-1](#)

L

LDAP

authentication
 configuration settings (table) [14-2](#)
 configuring [14-1](#)
 directory
 configuration settings (table) [13-3](#)
 configuring [13-1, 13-2](#)
 deleting [13-5](#)
 finding [13-1](#)
 system
 configuration settings (table) [12-2](#)
 configuring [12-1](#)
 updating LDAP authentication information [14-1](#)
 updating LDAP System information [12-1](#)
 licensing
 calculating license units [25-1](#)
 generating license unit report [24-1](#)
 license file
 contents [26-2](#)
 obtaining license file [26-1](#)
 sample license files [26-2](#)
 uploading [26-3](#)
 line groups
 adding devices [36-8](#)
 configuration settings (table) [36-3](#)
 configuring [36-2](#)
 deleting [36-9](#)
 finding [36-1](#)
 overview [36-1](#)
 removing devices [36-9](#)
 locations
 adding [15-3](#)
 configuration settings (table) [15-4](#)
 configuring [15-1](#)
 copying [15-3](#)
 deleting [15-5](#)
 finding [15-1](#)

resynchronizing bandwidth [15-6](#)

updating [15-3](#)

log off

Cisco Unified CallManager [1-3](#)

logon

Cisco Unified CallManager [1-3](#)

M

max list box enterprise parameter

calling search space [49-23](#)

media resource group lists

adding [61-2](#)

configuration settings (table) [61-3](#)

configuring [61-1](#)

copying [61-2](#)

deleting [61-4](#)

finding [61-1](#)

updating [61-2](#)

media resource groups

adding [60-3](#)

configuration settings (table) [60-4](#)

configuring [60-1](#)

copying [60-3](#)

deleting [60-5](#)

finding [60-1](#)

updating [60-3](#)

Media Termination Point (MTP) [55-1](#)

meet-me number patterns

configuration settings (table) [50-3](#)

configuring [50-1](#)

copying [50-2](#)

deleting [50-4](#)

finding [50-1](#)

MGCP

BRI

gateway configuration settings (table) [69-33](#)

Cisco IOS, adding [69-2](#)

Digital Access PRI ports, adding [69-7](#)

Digital Access T1 ports [69-7](#)

FXO ports, adding [69-5](#)

FXS ports, adding [69-4](#)

gateways, adding [69-2](#)

non-IOS gateway, adding [69-9](#)

ports, adding [69-4](#)

MLPP domains

configuration settings (table) [17-3](#)

configuring [17-2](#)

deleting [17-3](#)

finding [17-1](#)

overview [17-1](#)

MTP

adding [55-3](#)

configuring [55-1](#)

deleting [55-4](#)

finding [55-2](#)

IOS MTP configuration settings (table) [55-4](#)

multilevel administration access (MLA)

assigning privileges to user groups [89-6](#)

deleting users from user groups [89-6](#)

MWI

MWI device configuration settings (table) [64-3](#)

MWI device for uOne [64-3](#)

N

navigating

Cisco Unified CallManager Administration [1-6](#)

nonstandard softkey templates

adding [77-2](#)

adding application softkeys [77-3](#)

finding [77-1](#)

softkey positions [77-4](#)

NTP server [21-1, 22-1, 91-1, 92-1, 93-1](#)

number patterns, meet-me

copying [50-2](#)

deleting [50-4](#)

finding [50-1](#)

O

organization [xxiv](#)
 overview
 BAT application [94-1](#)
 overview of Cisco Unified CallManager [1-1](#)

P

parameters
 configuring [19-1](#)
 configuring for a service [19-2](#)
 displaying for a service [19-3](#)
 enterprise [18-1](#)
 partitions
 adding [42-2](#)
 configuring [42-1](#)
 deleting [42-3](#)
 finding [42-1](#)
 searching [42-6](#)
 phone button templates
 adding [76-2](#)
 configuration settings (table) [76-4](#)
 configuring [76-1](#)
 creating 7914 expansion module [76-4](#)
 deleting [76-5](#)
 finding [76-1](#)
 modifying button items [70-28](#)
 phone NTP reference [8-1](#)
 configuration settings (table) [8-3](#)
 configuring [8-2](#)
 deleting [8-4](#)
 phones
 adding with end user [90-2](#)
 Cisco Unified IP Phone Services
 adding a service parameter [78-5](#)
 configuration settings (table) [78-4](#)
 configuring [78-1](#)
 configuring a service [78-3](#)
 deleting a service [78-5](#)
 deleting a service parameter [78-7](#)
 finding a service [78-2](#)
 parameter settings (table) [78-7](#)
 updating a service parameter [78-5](#)
 configuration settings (table) [70-6](#)
 configuring with end user [90-1](#)
 deleting [70-5](#)
 directory numbers, configuring [49-1](#)
 displaying MAC address [70-4](#)
 finding and listing [70-29](#)
 resetting [70-4](#)
 plugins
 configuring [85-1](#)
 installing [85-1](#)
 ports
 adding [62-3](#)
 copying [62-3](#)
 deleting [62-6](#)
 Digital Access T1 configuration settings (table) [69-40](#)
 finding [62-1](#)
 modifying [69-74](#)
 updating [69-76](#)
 updating Cisco voice mail [62-3](#)
 presence groups
 configuring [5-1](#)
 PRI, gateway configuration [69-21](#)
 privileges
 assigning to user groups [89-6](#)

R

regions
 adding [7-2](#)
 configuration settings (table) [7-5](#)
 configuring [7-1](#)
 deleting [7-7](#)
 finding [7-1](#)
 related documentation [xxv](#)

roles

- configuration settings (table) [88-4](#)
- configuring [88-3](#)
- deleting [88-4](#)
- described [88-1](#)
- finding [88-2](#)
- viewing a user's [89-7](#)

route filters

- adding clauses [32-4](#)
- configuration settings (table) [32-4](#)
- configuring [32-3](#)
- deleting [32-5](#)
- dependency records [32-5](#)
- finding [32-1](#)
- operators
 - described (table) [32-8](#)
 - explained [32-8](#)
- overview [32-1](#)
- removing clauses [32-5](#)
- tags
 - described (table) [32-7](#)
 - explained [32-6](#)

route groups

- adding devices [33-5](#)
- configuration settings (table) [33-3](#)
- configuring [33-2](#)
- deleting [33-6](#)
- finding [33-1](#)
- overview [33-1](#)
- removing devices [33-6](#)

route lists

- adding [34-3](#)
- adding route groups [34-4](#)
- changing the order of route groups [34-6](#)
- configuring [34-1](#)
- deleting [34-6](#)
- finding [34-1](#)
- removing route groups [34-5](#)

route patterns

- configuration settings (table) [35-4](#)
- configuring [35-3](#)
- configuring a SIP pattern [39-3](#)
- deleting [35-10](#)
- deleting a SIP pattern [39-6](#)
- finding [35-1](#)
- finding a SIP pattern [39-1](#)
- overview [35-1](#)

route plans

- report
 - configuring [51-1](#)
 - deleting unassigned directory numbers [51-3](#)
 - updating unassigned directory numbers [51-3](#)
 - viewing in a file [51-4](#)
 - viewing records [51-1](#)

S

SCCP

- Cisco IOS, adding [69-8](#)
- gateways, adding [69-8](#)

servers

- configuration settings (table) [2-4](#)
- configuring [2-1, 2-2](#)
- deleting [2-3](#)
- finding [2-1](#)
- updating [2-2](#)

service parameters

- configuring [19-1](#)
 - adding Cisco Unified IP Phone Services [78-5](#)
 - deleting Cisco Unified IP Phone Services [78-7](#)
 - updating Cisco Unified IP Phone Services [78-5](#)
- configuring for a service [19-2](#)
- displaying for a service [19-3](#)

services

- Cisco Unified IP Phone configuration settings (table) [78-4](#)
- Cisco Unified IP Phone parameter settings (table) [78-7](#)

- configuring
 - Cisco Unified IP Phone Services [78-3](#)
 - deleting Cisco Unified IP Phone Services [78-5](#)
 - finding Cisco Unified IP Phone Services [78-2](#)
 - service URL button
 - adding [70-27](#)
 - SIP
 - configuration differences [C-1](#)
 - configuring third-party devices [C-1](#)
 - third-party SIP phone configuration checklist (table) [C-3](#)
 - third-party SIP phones and TFTP [C-2](#)
 - SIP dial rules
 - configuration settings [31-3](#)
 - configuring [31-1, 31-3](#)
 - deleting [31-6](#)
 - dial plan examples [31-6](#)
 - finding [31-1](#)
 - pattern formats [31-5](#)
 - resetting [31-7](#)
 - updating [31-3](#)
 - SIP phones
 - enabling digest authentication
 - third-party phones [C-2](#)
 - SIP profiles
 - adding [79-2](#)
 - configuration settings [79-2](#)
 - configuring [79-1](#)
 - copying [79-2](#)
 - deleting [79-8](#)
 - finding [79-1](#)
 - resetting [79-9](#)
 - updating [79-2](#)
 - SIP route patterns
 - configuration settings (table) [39-3](#)
 - configuring [39-1, 39-3](#)
 - deleting [39-6](#)
 - finding [39-1](#)
 - related topics [39-7](#)
 - softkey templates
 - assigning [77-8](#)
 - configuring [77-1](#)
 - deleting [77-6](#)
 - renaming [77-5](#)
 - updating [77-7](#)
 - software conference bridge
 - configuring [54-3](#)
 - speed dial
 - configuration settings (table) [70-23, 70-24](#)
 - speed-dial buttons
 - configuring [70-23](#)
 - SRST
 - configuration settings (table) [16-4](#)
 - configuring [16-1, 16-2](#)
 - deleting [16-3](#)
 - finding [16-1](#)
 - Survivable Remote Site Telephony (SRST)
 - configuring [16-1](#)
-
- ## T
- T1 ports, adding [69-7](#)
 - TFTP
 - third-party SIP phones [C-2](#)
 - time periods
 - configuration settings (table) [40-4](#)
 - configuring [40-1, 40-2](#)
 - deleting [40-3](#)
 - finding [40-1](#)
 - time schedules
 - configuration settings (table) [41-4](#)
 - configuring [41-1, 41-2](#)
 - deleting [41-3](#)
 - finding [41-1](#)
 - time zones [6-1](#)
 - transcoders
 - configuration settings (table) [59-5](#)
 - configuring [59-1, 59-3](#)

- deleting [59-4](#)
 - overview [59-1](#)
 - resetting [59-3](#)
 - translation patterns
 - configuration settings (table) [46-4](#)
 - configuring [46-3](#)
 - deleting [46-9](#)
 - finding [46-1](#)
 - overview [46-1](#)
 - trunks
 - adding [71-2](#)
 - configuration settings (table) [71-3](#)
 - configuring [71-1](#)
 - deleting [71-27](#)
 - finding and listing [71-1](#)
 - modifying [71-2](#)
 - resetting [71-27](#)
-
- ## U
- unassigned directory numbers
 - deleting [51-3](#)
 - updating [51-3](#)
 - uOne, Cisco
 - MWI device, configuring [64-3](#)
 - user
 - application
 - adding [86-3](#)
 - application profiles [86-7](#)
 - associating devices to an application user [86-8](#)
 - changing password [86-7](#)
 - configuration [86-1](#)
 - configuration settings (table) [86-3](#)
 - finding [86-1](#)
 - configuring Cisco Unity or Cisco Unity Connection
 - voice mailbox [87-3](#)
 - end
 - adding [87-3](#)
 - adding with phone [90-2](#)
 - associating devices to an end user [87-10](#)
 - changing password [87-8](#)
 - changing PIN [87-9](#)
 - configuration [87-1](#)
 - configuration settings (table) [87-5](#)
 - configuring with phone [90-1](#)
 - deleting [87-13](#)
 - extension mobility [87-12](#)
 - finding [87-1](#)
 - user-related information [87-9](#)
 - user/phone add
 - adding [90-2](#)
 - configuration [90-1](#)
 - user and device
 - configuration settings (table) [90-2](#)
 - user device profile
 - dependency records [75-5](#)
 - user groups
 - adding [89-3](#)
 - adding users [89-4](#)
 - assigning privileges [89-6](#)
 - deleting [89-3](#)
 - deleting users [89-6](#)
 - described [89-1](#)
 - finding [89-1](#)
 - viewing a user's roles [89-7](#)
 - user information
 - configuration settings (table) [85-3](#)
-
- ## V
- video
 - conference bridges [54-6](#)
 - voice gateways [69-1](#)
 - voice mail
 - adding a new server and ports [63-1](#)
 - adding ports [62-3](#)
 - adding ports with the wizard [63-5](#)
 - configuring [62-1](#)

- configuring message waiting [64-1](#)
- configuring port wizard [63-1](#)
- configuring profile [66-1](#)
- copying ports [62-3](#)
- deleting ports [62-6](#)
- deleting ports with the wizard [63-6](#)
- finding a message waiting number [64-1](#)
- finding ports [62-1](#)
- port configuration settings (table) [62-4](#)
- port wizard device information configuration settings [63-2](#)
- port wizard directory number configuration settings [63-3](#)
- updating ports [62-3](#)
- voice-mail pilot
 - configuration settings (table) [65-3](#)
 - configuring [65-1](#), [65-3](#)
 - deleting [65-4](#)
 - finding [65-1](#)
- voice-mail pilot numbers
 - dependency records [65-4](#)
- voice-mail ports
 - adjustments for Cisco Unity [B-1](#)
 - changes for Cisco Unity [B-1](#)
 - dependency records [62-6](#)
- voice-mail profiles
 - configuration settings (table) [66-3](#)
 - copy [66-2](#)
 - delete [66-3](#)
 - dependency records [66-3](#)
 - find [66-1](#)
 - list [66-1](#)

