



Cisco Unified CallManager New and Changed Information Guide

Release 5.1(1)

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-11473-01



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.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, 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. (0609R)

Cisco Unified CallManager New and Changed Information Guide
Copyright © 2007 Cisco Systems, Inc. All rights reserved.



Preface xxiii

Purpose	xxiii
Audience	xxiii
Organization	xxiv
Related Documentation	xxv
Conventions	xxv
Obtaining Documentation	xxvi
Cisco.com	xxvi
Product Documentation DVD	xxvi
Ordering Documentation	xxvii
Documentation Feedback	xxvii
Cisco Product Security Overview	xxvii
Reporting Security Problems in Cisco Products	xxviii
Obtaining Technical Assistance	xxviii
Cisco Technical Support & Documentation Website	xxix
Submitting a Service Request	xxix
Definitions of Service Request Severity	xxx
Obtaining Additional Publications and Information	xxx

PART 1

About This Guide

CHAPTER 1

About This Guide 1-1

How to Use This Document	1-1
New and Changed Information for Release 5.1(1)	1-2
Cisco Unified CallManager Administration Guide	1-2
Cisco Unified CallManager System Guide	1-2
Cisco Unified CallManager Features and Services Guide	1-3
Cisco Unified CallManager Serviceability Administration Guide	1-3
Cisco Unified CallManager Serviceability System Guide	1-3
Cisco Unified CallManager CDR Analysis and Reporting Administration Guide	1-4
Cisco Unified CallManager Call Detail Record Definitions	1-4
Cisco Unified CallManager Security Guide	1-4
Cisco Unified CallManager Bulk Administration Guide	1-5
Cisco Unified CallManager Developers Guide	1-5

Cisco Unified IP Phones Information	1-5
Release 5.0(4) Documentation Guide	1-5
Cisco Unified CallManager Installation Documentation	1-7
Cisco Unified CallManager Configuration Documentation	1-8
Cisco Unified CallManager Developer Guides	1-10
Related Product Documentation	1-11

PART 2

Cisco Unified CallManager Administration Guide

CHAPTER 2

Region Configuration 2-1

Finding a Region	2-1
Configuring a Region	2-3
Region Configuration Settings	2-5
Deleting a Region	2-7
Related Topics	2-8

CHAPTER 3

License Capabilities Assignment Configuration 3-1

Finding a License Capabilities Assignment	3-1
Configuring the Capabilities Assignments for One User	3-2
Configuring the Capabilities Assignments for Multiple Users	3-3
License Capabilities Assignment Configuration Settings	3-4
Related Topics	3-4

CHAPTER 4

Configuring Non-Cisco SIP Phones 4-1

SIP Phone Configuration Differences	4-1
Migrating from Cisco Unified CallManager Release 5.0(1), and above, to Cisco Unified CallManager, Release 5.1(1)	4-3
Third-Party SIP Phone Configuration Checklist	4-4
Where to Find More Information	4-5

PART 3

Cisco Unified CallManager System Guide

CHAPTER 5

System-Level Configuration Settings 5-1

Server Configuration	5-1
Cisco Unified CallManager Configuration	5-2
Cisco Unified CallManager Groups	5-3

Phone NTP Reference Configuration for SIP Phones	5-4
Date/Time Groups	5-4
Regions	5-5
Device Pools	5-10
Updating Device Pools	5-11
LDAP	5-12
Call Admission Control	5-13
Survivable Remote Site Telephony References	5-13
MLPP Domain	5-15
Enterprise Parameters	5-15
Service Parameters	5-16
Dependency Records	5-16
System Configuration Checklist	5-17
Where to Find More Information	5-18

CHAPTER 6

Cisco TFTP 6-1

TFTP Process Overview for SCCP Devices	6-2
TFTP Process Overview for Cisco SIP IP Phones	6-2
Understanding How Devices Use DHCP and Cisco TFTP	6-4
Understanding How Devices Access the TFTP Server	6-6
Understanding How Devices Identify the TFTP Server	6-6
Configuring a Redundant or Load-Sharing TFTP Server	6-8
Alternate Cisco File Servers	6-8
Centralized TFTP in a Multiple Cluster Environment	6-9
Master TFTP Server	6-9
Sending Files to the Master TFTP Server	6-9
Centralized TFTP with Secure Clusters	6-10
Configuration Tips for Centralized TFTP	6-10
Customizing and Modifying Configuration Files	6-10
TFTP Configuration Checklist	6-11
Where to Find More Information	6-11

CHAPTER 7

Understanding Route Plans 7-1

Automated Alternate Routing	7-1
Automated Alternate Routing Enable Service Parameter	7-3
Automated Alternate Routing and Hunt Pilots	7-3

Route Plan Overview	7-4
Route Groups and Route Lists	7-5
Route Patterns	7-6
Route Pattern Usage	7-6
Line Groups	7-9
Hunt Lists	7-10
Hunt Pilots	7-10
Call Coverage	7-11
Hunting and Call Forwarding	7-11
Internal and External Calls	7-12
Personal Preferences	7-12
Closest Match Routing	7-12
Using the @ Wildcard Character in Route Patterns	7-13
Static Digit Analysis	7-14
Special Characters and Settings	7-16
Wildcards and Special Characters in Route Patterns and Hunt Pilots	7-16
Discard Digits Instructions	7-19
Calling and Called Party Transformations	7-26
Calling Party Number Transformations Settings	7-26
Called Party Number Transformations Settings	7-28
Caller Identification and Restriction	7-29
Calling Party Presentation and Restriction Settings	7-29
Connected Party Presentation and Restriction Settings	7-31
External Route Plan Wizard	7-34
Generated Route Filters	7-35
Generated Route Groups	7-36
Generated Route Lists	7-36
Generated Route Patterns	7-37
Route Plan Report	7-38
Where to Find More Information	7-38

CHAPTER 8

Understanding Directory Numbers	8-1
Characteristics of Directory Numbers	8-1
Shared Line Appearance	8-2
Managing Directory Numbers	8-5
Directory Number Features	8-5
Making and Receiving Multiple Calls Per Directory Number	8-7

Transfer and Conference Behavior	8-7
Direct Transfer and Join Behavior	8-8
Directory Number Search	8-8
Dependency Records	8-9
Directory Number Configuration Checklist	8-10
Where to Find More Information	8-11

CHAPTER 9**Understanding the Directory 9-1**

Cisco Unified CallManager and the Corporate LDAP Directory	9-2
Directory Access	9-3
DirSync Service	9-3
DirSync Service Parameters	9-4
Data Migration Assistant	9-4
Authentication	9-4
Using the Cisco Unified CallManager Database Versus the Corporate LDAP Directory	9-5
Directory Access for Cisco Unified Communications Endpoints	9-5
LDAP Directory Configuration Checklist	9-6
Where to Find More Information	9-7

CHAPTER 10**Understanding Cisco Unified CallManager Voice Gateways 10-1**

Cisco Voice Gateways	10-1
Standalone Voice Gateways	10-2
MGCP BRI Call Connections	10-4
Cisco Catalyst 4000 and 6000 Voice Gateway Modules	10-5
H.323 Gateways	10-7
Voice Gateway Model Summary	10-9
Gateways, Dial Plans, and Route Groups	10-16
Dependency Records for Gateways and their Route Groups and Directory Numbers	10-16
Gateway Failover and Fallback	10-17
MGCP Gateways	10-17
IOS H.323 Gateways	10-17
Cisco VG248 Analog Phone Gateway	10-18
Transferring Calls Between Gateways	10-18
Configuring Transfer Capabilities Using Gateway Configuration	10-18
Configuring Transfer Capabilities by Using Call Classification Service Parameter	10-19
Blocking Transfer Capabilities by Using Service Parameters	10-19
Gateway Configuration Checklist	10-20

MGCP BRI Gateway Configuration Checklist	10-21
Where to Find More Information	10-22

CHAPTER 11

Cisco Unified IP Phones 11-1

Supported Cisco Unified IP Phones	11-2
Cisco SIP IP Phones	11-8
H.323 Clients and CTI Ports	11-8
Cisco IP Communicator	11-9
Cisco Unified Personal Communicator	11-9
Cisco TelePresence	11-9
Phone Button Templates	11-10
Default Phone Button Templates	11-10
Guidelines for Customizing Phone Button Templates	11-14
Softkey Templates	11-16
Add Application	11-17
Configure Softkey Layout	11-18
Softkey Template Operation	11-19
Common Phone Profiles	11-20
Methods for Adding Phones	11-20
Phone Features	11-21
Phone Association	11-27
Phone Administration Tips	11-27
Phone Search	11-27
Messages Button	11-28
Directories Button	11-29
Cisco Unified CallManager User Options	11-29
Maximum Phone Fallback Queue Depth Service Parameter	11-30
Dependency Records	11-30
Phone Failover and Fallback	11-30
Phone Configuration Checklist	11-31
Where to Find More Information	11-35

PART 4

Cisco Unified CallManager Features and Services Guide

CHAPTER 12

Music On Hold 12-1

Understanding Music On Hold	12-1
Music On Hold Definitions	12-2

Music On Hold Characteristics	12-3
Music On Hold Functionality	12-4
Supported Music On Hold Features	12-5
Music On Hold Server	12-8
Music On Hold Audio Sources	12-8
Default Music On Hold Sample	12-9
Creating Audio Sources	12-9
Storing Audio Source Files	12-9
Managing Audio Sources	12-10
Multicast and Unicast Audio Sources	12-10
Multicast Configuration Checklist	12-12
Music On Hold System Requirements and Limits	12-12
Music On Hold Failover and Fallback	12-13
Music On Hold Configuration Checklist	12-14
Monitoring Music On Hold Performance	12-15
Viewing Music On Hold Server Performance	12-15
Checking Service States	12-16
Music On Hold Audio Source Configuration	12-16
Finding a Music On Hold Audio Source	12-17
Configuring a Music On Hold Audio Source	12-18
Deleting a Music On Hold Audio Source	12-19
Music On Hold Audio Source Configuration Settings	12-19
Fixed Music On Hold Audio Source Configuration	12-21
Configuring the Fixed Music On Hold (MOH) Audio Source	12-22
Deleting a Fixed Music On Hold (MOH) Audio Source	12-22
Fixed Music On Hold (MOH) Audio Source Configuration Settings	12-23
Music On Hold Server Configuration	12-23
Finding a Music On Hold Server	12-23
Configuring a Music On Hold Server	12-24
Resetting or Restarting a Music On Hold Server	12-25
Music On Hold Server Configuration Settings	12-26
Music On Hold Audio File Management Configuration	12-28
Displaying Music On Hold Audio Files	12-28
Uploading a Music On Hold Audio File	12-29
Deleting a Music On Hold Audio File	12-30
Related Topics	12-31

CHAPTER 13**Immediate Divert 13-1**

- Introducing Immediate Divert 13-1
- System Requirements for Immediate Divert 13-2
 - Call-Processing Requirements for Immediate Divert 13-2
 - Immediate Divert Phone Display Messages 13-4
 - Using Immediate Divert 13-4
- Interactions and Restrictions 13-6
 - Interactions 13-6
 - Restrictions 13-8
- Installing and Activating Immediate Divert 13-9
- Configuring Immediate Divert 13-9
 - Immediate Divert Configuration Checklist 13-9
 - Setting the Service Parameters for Immediate Divert 13-10
- Where to Find More Information 13-11
- Related Topics 13-11

CHAPTER 14**Cisco Unified CallManager Attendant Console 14-1**

- Introducing Cisco Unified CallManager Attendant Console 14-1
 - Understanding Cisco Unified CallManager Attendant Console Users 14-2
 - Understanding Pilot Points and Hunt Groups 14-2
 - Understanding Call Queuing 14-9
 - Understanding the Cisco Unified CallManager Attendant Console Directory 14-9
 - Understanding the Cisco CallManager Attendant Console Server Service 14-10
 - Cisco Unified CallManager Attendant Console Redundancy 14-11
 - Firewall Support for Attendant Console 14-12
- System Requirements for Cisco Unified CallManager Attendant Console 14-12
 - Attendant PC Requirements 14-12
 - Cisco Unified IP Phone and Voice-Messaging Requirements for Use with the Attendant Console 14-13
- Interactions and Restrictions 14-13
 - Interactions 14-14
 - Restrictions 14-15
- Installing and Activating Cisco Unified CallManager Attendant Console 14-16
- Configuring Cisco Unified CallManager Attendant Console 14-16
 - Configuration Checklist for Cisco Unified CallManager Attendant Console 14-17
 - Configuring Cisco Unified CallManager Attendant Console Users 14-18
 - Enabling Device Security for Cisco Unified CallManager Attendant Console 14-21
 - Enabling the Super Provider Feature for Cisco Unified CallManager Attendant Console 14-22

Configuring Pilot Points	14-23
Associating Devices with the Attendant Console Authorization User	14-28
Configuring Hunt Groups	14-29
Cisco CallManager Attendant Console Server Service Configuration	14-32
Creating and Uploading the CorporateDirectory.txt File	14-33
Deleting the CorporateDirectory.txt File	14-34
Installing the Cisco Unified CallManager Attendant Console Plug-in on an Attendant PC	14-35
Starting Cisco Unified CallManager Attendant Console After Installing Windows XP SP2	14-36
Configuring Cisco Unified CallManager Attendant Console Settings	14-37
Attendant Console Configuration Settings	14-37
Configuring Held Icon Timers	14-39
Dependency Records	14-40
Related Topics	14-40

PART 5

Cisco Unified CallManager Serviceability Administration Guide

CHAPTER 15
Managing Services 15-1

Activating and Deactivating Feature Services	15-1
Starting, Stopping, Restarting, and Refreshing Status of Services in Control Center	15-4
Using a Command Line Interface to Start and Stop Services	15-6
Related Topics	15-6

CHAPTER 16
Alarm Configuration 16-1

Configuring or Updating an Alarm for a Service	16-1
Alarm Destination Settings	16-3
Alarm Event Level Settings	16-4
Related Topics	16-4

CHAPTER 17
Troubleshooting Trace Setting Configuration 17-1

Related Topics	17-2

CHAPTER 18
Real-Time Monitoring Configuration 18-1

Installing the Real-Time Monitoring Tool (RTMT)	18-1
Uninstalling RTMT	18-2
Using RTMT	18-3
Configuring E-mail Notification	18-4
Working with Configuration Profiles	18-5

Using the Default Configuration Profile	18-5
Adding Configuration Profiles	18-5
Restoring Profiles	18-6
Deleting Configuration Profiles	18-6
Working with Predefined Objects	18-7
Viewing/Monitoring a Predefined Object	18-7
Working with Devices	18-10
Finding Specific Devices to Monitor	18-10
Viewing Phone Information	18-12
Viewing Device Properties	18-12
Configuring Polling Rate for Devices and Performance Monitoring Counters	18-13
Working with CTI Applications, Devices, and Lines	18-13
Viewing CTI Manager Information	18-14
Finding CTI Applications to Monitor	18-14
Finding CTI Devices to Monitor	18-14
Finding CTI Lines to Monitor	18-15
Viewing Application Information	18-16
Working with Categories	18-17
Adding a Category	18-17
Renaming a Category	18-17
Deleting a Category	18-18
Where to Find More Information	18-18
Related Topics	18-18

PART 6

Cisco Unified CallManager Serviceability System Guide

CHAPTER 19

Service Management 19-1

Feature Services	19-1
CM Services	19-2
CTI Services	19-4
CDR Services	19-4
Database and Admin Services	19-5
Performance and Monitoring Services	19-5
Security Services	19-6
Directory Services	19-7
Network Services	19-7
Platform Services	19-7
DB Services	19-8

CCM Services	19-9
Performance and Monitoring Services	19-10
SOAP Services	19-10
Backup and Restore Services	19-11
CDR Services	19-11
Service Activation	19-11
Control Center	19-12
Services Configuration Checklist	19-13
Where to Find More Information	19-14

CHAPTER 20
Alarms 20-1

Understanding Alarms	20-1
Alarm Configuration	20-2
Alarm Definitions	20-2
Viewing Alarm Information	20-2
Alarm Configuration Checklist	20-3
Where to Find More Information	20-4

CHAPTER 21
Trace 21-1

Understanding Trace	21-1
Trace Configuration	21-2
Troubleshooting Trace Setting	21-2
Trace Collection	21-3
Trace Configuration and Collection Checklist	21-4
Where to Find More Information	21-5

CHAPTER 22
Real-Time Monitoring Tool 22-1

Understanding the Real-Time Monitoring Tool	22-1
RTMT Components	22-3
RTMT Services, Servlets and Service Parameters	22-4
RTMT Collector, Alert Manager, and RTMT Reporter	22-4
Viewing a Summary	22-6
Monitoring Server Status	22-6
Understanding Server Logs	22-7
Monitoring Call-Processing Activity	22-7
Understanding Call-Processing Logs	22-9

Monitoring Services	22-10
Understanding Service Logs	22-11
Monitoring Devices	22-11
Understanding Device Logs	22-13
Monitoring CTI Applications, Devices, and Lines	22-13
Where to Find More Information	22-13

CHAPTER 23

Performance Objects and Counters 23-1

Working with Performance Objects and Counters	23-1
Cisco Analog Access	23-3
Cisco Annunciator Device	23-4
Cisco CallManager	23-4
Cisco CallManager Attendant Console	23-11
Cisco CallManager System Performance	23-12
Cisco CTIManager	23-15
Cisco Dual-Mode Mobility	23-16
Cisco Extension Mobility	23-17
Cisco Gatekeeper	23-17
Cisco H.323	23-18
Cisco Hunt Lists	23-19
Cisco HW Conference Bridge Device	23-20
Cisco IP Manager Assistant	23-20
Cisco Lines	23-21
Cisco Locations	23-21
Cisco Media Streaming Application	23-22
Cisco Messaging Interface	23-25
Cisco MGCP FXO Device	23-25
Cisco MGCP FXS Device	23-26
Cisco MGCP Gateways	23-26
Cisco MGCP PRI Device	23-27
Cisco MGCP T1 CAS Device	23-27
Cisco Music On Hold (MOH) Device	23-28
Cisco MTP Device	23-29
Cisco Phones	23-29
Cisco Presence Feature	23-30
Cisco QSIG Features	23-30
Cisco SIP	23-30
Cisco SIP Stack	23-31
Cisco SW Conf Bridge Device	23-39

Cisco TFTP Server	23-40
Cisco Tomcat Connector	23-43
Cisco Tomcat JVM	23-45
Cisco Tomcat Web Application	23-46
Cisco Transcode Device	23-47
Cisco Video Conference Bridge	23-47
Cisco WebDialer	23-48
Cisco WSM Connector	23-48
Database Change Notification Client	23-49
Database Change Notification Server	23-50
Database Change Notification Subscription	23-50
Database Local DSN	23-50
DB User Host Information Counters	23-51
Enterprise Replication DBSpace Monitors	23-51
Enterprise Replication Perfmon Counters	23-51
IP	23-51
Memory	23-52
Network Interface	23-54
Number of Replicates Created and State of Replication	23-55
Partition	23-55
Process	23-56
Processor	23-57
System	23-58
TCP	23-58
Thread	23-59
Using RTMT for Performance Monitoring	23-59
Category Tabs	23-60
Sample Rate	23-61
Adding Counters to Monitor	23-61
Alert Notification for Counters	23-61
Zoom Counter	23-61
Counter Properties	23-61
Understanding Perfmon Logs	23-62
Where to Find More Information	23-63

PART 7**Cisco Unified CallManager CDR Analysis and Reporting Administration Guide****CHAPTER 24****CDR Analysis and Reporting Overview 24-1**

Understanding CDR Data	24-1

Understanding CDR Analysis and Reporting	24-2
CAR Administrators, Managers, and Users	24-5
CAR System Settings	24-6
CAR Reports	24-6
CAR Reports General Information	24-6
User Reports	24-7
System Reports	24-8
Device Reports	24-10
Automatically Generated Reports Schedule	24-11
CDR Search	24-12
Internationalization for CDR Analysis and Reporting	24-14
Web Browsers	24-15
CDR Analysis and Reporting Configuration Checklist	24-15
Related Topics	24-16

CHAPTER 25
CAR System Configuration 25-1

System Parameters Configuration	25-1
Configuring Mail Server Parameters	25-2
Configuring the Dial Plan	25-2
Restoring the Default Values for the CAR Dial Plan	25-4
Gateway Configuration	25-5
Configuring System Preferences	25-6
System Scheduler Configuration	25-7
Configuring the CDR Load Schedule	25-7
Scheduling Daily Reports	25-9
Scheduling Weekly Reports	25-10
Scheduling Monthly Reports	25-11
System Database Configuration	25-12
Manually Purging or Reloading the CAR Database	25-12
Configuring Automatic Database Purge	25-14
System Log Screens	25-15
Generating the Event Log	25-15
Related Topics	25-16

CHAPTER 26
CAR Report Configuration 26-1

Configuring the Rating Engine	26-1
Setting the Base Rate and Duration	26-2
Factoring Time of Day into Call Cost	26-3

Factoring Voice Quality into Call Cost	26-4
Defining the Quality of Service (QoS) Values	26-5
Configuring Automatic Report Generation/Alert	26-6
Enabling or Customizing Reports for Automatic Generation	26-7
Enabling or Disabling Alerts by Mail	26-8
Configuring Notification Limits	26-8
Related Topics	26-9

CHAPTER 27
CDR Search Configuration 27-1

Configuring CDR Search by User Extension	27-1
Configuring CDR Search by Gateway	27-3
Configuring CDR Search by Cause for Call Termination	27-4
Viewing Call Termination Details	27-5
Configuring CDR Search By Call Precedence Levels	27-5
Configuring CDR Search for Malicious Calls	27-7
Related Topics	27-8

CHAPTER 28
CAR Report Results 28-1

Bill Summary Report Results	28-2
Bill Detail Report Results	28-3
Top N By Charge or Duration Report Results	28-4
Top N By Number of Calls Report Results	28-5
Call Usage for Cisco IPMA Assistant—Detail	28-6
Call Usage for Cisco IPMA Assistant—Summary	28-7
Call Usage for Cisco IPMA Manager—Detail	28-8
Call Usage for Cisco IPMA Manager—Summary	28-8
Cisco IP Phone Services Report Results	28-9
QoS Detail Report Results	28-9
QoS Summary Report Results	28-11
QoS by Gateways Report Results	28-11
QoS by Call Types Report Results	28-11
Traffic Summary Report Results	28-12
Authorization Code Name Call Details	28-14
Authorization Level Call Details	28-14
Client Matter Code Details	28-15
Malicious Call Details Report Results	28-15

Precedence Call Summary Report Results	28-15
System Overview Report Results	28-16
CDR Error Report Results	28-17
Gateway Detail Report Results	28-18
Gateway Summary Report Results	28-19
Gateway and Route Utilization Report Results	28-21
Conference Call Detail Report Results	28-21
Conference Bridge Utilization Report Results	28-22
Voice Messaging Utilization Report Results	28-23
Understanding the CDR Search Results	28-23
Understanding the Results for CDR Search	28-23
Media Information	28-25
CDR and CMR Dump Tables	28-25

PART 8

Cisco Unified CallManager Call Detail Record Definitions

CHAPTER 29

Call Detail Record Definitions 29-1

Codec Types	29-1

PART 9

Cisco Unified CallManager Security Guide

CHAPTER 30

Security Overview 30-1

Authentication and Encryption Terminology	30-2
System Requirements	30-4
Features List	30-4
Security Icons	30-5
Interactions and Restrictions	30-5
Interactions	30-5
Restrictions	30-6
Best Practices	30-10
Resetting the Devices, Restarting Services, or Rebooting the Server/Cluster	30-10
Configuring Media Encryption with Barge	30-11
Installation	30-12
TLS and IPSec	30-12
Certificates	30-12
Phone Certificate Types	30-13
Server Certificate Types	30-13

Support for Certificates from External CAs	30-14
Authentication, Integrity, and Authorization Overview	30-15
Image Authentication	30-15
Device Authentication	30-15
File Authentication	30-16
Signaling Authentication	30-16
Digest Authentication	30-17
Authorization	30-18
Encryption Overview	30-19
Signaling Encryption	30-19
Media Encryption	30-20
Configuration File Encryption	30-21
Configuration Checklist Overview	30-21
Where to Find More Information	30-25

CHAPTER 31

Configuring the Cisco CTL Client	31-1
Cisco CTL Client Overview	31-2
Configuration Tips for Cisco CTL Client Configuration	31-2
Cisco CTL Client Configuration Checklist	31-3
Activating the Cisco CTL Provider Service	31-4
Activating the Cisco CAPF Service	31-5
Configuring Ports for the TLS Connection	31-5
Installing the Cisco CTL Client	31-6
Upgrading the Cisco CTL Client and Migrating the Cisco CTL File	31-7
Configuring the Cisco CTL Client	31-8
Updating the CTL File	31-10
Deleting a CTL File Entry	31-12
Updating the Clusterwide Security Mode	31-12
Cisco CTL Client Configuration Settings	31-12
Verifying the Security Mode for the Cisco Unified CallManager Cluster	31-15
Setting the Smart Card Service to Started and Automatic	31-15
Changing the Security Token Password (Etoken)	31-16
Deleting the CTL File on the Cisco Unified IP Phone	31-16
Determining the Cisco CTL Client Version	31-17
Verifying or Uninstalling the Cisco CTL Client	31-18
Where to Find More Information	31-18

CHAPTER 32

Configuring a Phone Security Profile 32-1

- Phone Security Profile Overview 32-1
- Configuration Tips for Phone Security Profiles 32-1
- Finding a Phone Security Profile 32-2
- Configuring a Phone Security Profile 32-3
- Phone Security Profile Configuration Settings 32-4
- Applying a Phone Security Profile 32-9
- Deleting a Phone Security Profile 32-10
- Finding Phones That Use Phone Security Profiles 32-11
- Where to Find More Information 32-11

CHAPTER 33

Configuring Encrypted Phone Configuration Files 33-1

- Understanding Encryption of the Phone Configuration File 33-1
 - Manual Key Distribution 33-2
 - Symmetric Key Encryption with Phone Public Key 33-3
- Supported Phone Models 33-4
- Configuration Tips for Encrypted Configuration Files 33-4
- Encryption Configuration File Configuration Checklist 33-5
- Enabling Phone Configuration File Encryption 33-6
- Configuring Manual Key Distribution 33-6
- Manual Key Distribution Configuration Settings 33-7
- Entering the Symmetric Key on the Phone 33-7
- Verifying That an LSC or MIC Certificate Is Installed 33-8
- Verifying That the Phone Configuration File Is Encrypted 33-8
- Disabling Encryption for the Phone Configuration Files 33-9
- Excluding Digest Credentials from Phone Configuration File Download 33-9
- Where to Find More Information 33-10

PART 10

Cisco Unified CallManager Bulk Administration Guide

CHAPTER 34

Working with Licenses 34-1

- Using the CUPS Menu 34-1
 - Export CUPS/CUPC Users 34-1
 - Update CUPS/CUPC Users 34-2

CHAPTER 35**Updating the Region Matrix 35-1**

Populating and Depopulating the Region Matrix 35-1

PART 11**Cisco Unified CallManager Developers Guide****CHAPTER 36****AXL Programming 36-1**

Introduction 36-1

Target Audience for this Chapter 36-2

New and Changed Information 36-2

AXL APIs 36-2

New Service Parameter 36-2

AXL API 36-3

AXL Compliance 36-3

AXL Error Codes 36-3

Example AXL Requests 36-5

C or C++ Example 36-6

Java Example 36-10

Throttling of Requests 36-12

The AXL Schema Documentation 36-12

Example XML Structure 36-13

Authentication 36-14

Data Encryption 36-14

Integration Considerations and Interoperability 36-14

CHAPTER 37**WebDialer API Programming 37-1**

Definitions 37-1

Overview 37-2

WebDialer Servlet 37-2

Redirector Servlet 37-2

Changes in Release 5.1 37-4

Cisco WebDialer Security Support 37-4

SIP Phone Support in Cisco WebDialer 37-6

Call Flows 37-6

Interfaces 37-9

HTML over HTTPS Interfaces 37-15

Cisco WebDialer WSDL 37-16

Sample JavaScript 37-19

PART 12

Cisco Unified IP Phone Information

CHAPTER 38

Enhanced Immediate Divert Behavior 38-1

CHAPTER 39

Arabic Support 39-1

INDEX



Preface

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

The preface covers these topics:

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

Purpose

The *Cisco Unified CallManager New and Changed Information Guide* provides new or changed information for Cisco Unified CallManager Release 5.1(1) components.

Audience

The *Cisco Unified CallManager New and Changed Information 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 shows the organization of this guide:

Part	Description
Part 1	“About This Document” Describes how to use this document as a supplement to the Cisco Unified CallManager 5.0(4) document set.
Part 2	“Cisco Unified CallManager Administration Guide” Provides new and changed information for the <i>Cisco Unified CallManager Administration Guide</i> .
Part 3	“Cisco Unified CallManager System Guide” Provides new and changed information for the <i>Cisco Unified CallManager System Guide</i> .
Part 4	“Cisco Unified CallManager Features and Services Guide” Provides new and changed information for the <i>Cisco Unified CallManager Features and Services Guide</i> .
Part 5	“Cisco Unified CallManager Serviceability Administration Guide” Provides new and changed information for the <i>Cisco Unified CallManager Serviceability Administration Guide</i> .
Part 6	“Cisco Unified CallManager Serviceability System Guide” Provides new and changed information for the <i>Cisco Unified CallManager Serviceability System Guide</i> .
Part 7	“Cisco Unified CallManager CDR Analysis and Reporting Administration Guide” Provides new and changed information for the <i>Cisco Unified CallManager CDR Analysis and Reporting Administration Guide</i> .
Part 8	“Cisco Unified CallManager Call Detail Record Definitions” Provides new and changed information for <i>Cisco Unified CallManager Call Detail Record Definitions</i> .
Part 9	“Cisco Unified CallManager Security Guide” Provides new and changed information for the <i>Cisco Unified CallManager Security Guide</i> .
Part 10	“Cisco Unified CallManager Bulk Administration Guide” Provides new and changed information for the <i>Cisco Unified CallManager Bulk Administration Guide</i> .
Part 11	“Cisco Unified CallManager Developers Guide” Provides new and changed information for the <i>Cisco Unified CallManager Developers Guide</i> .
Part 12	“Cisco Unified IP Phones Information” Provides new and changed information for Cisco Unified IP Phones.

Related Documentation

Refer to the “[Release 5.0\(4\) Documentation Guide](#)” in the “[About This Guide](#)” chapter for further information about related Cisco Unified Communications applications and products.

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 screen font.
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.
^	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

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML 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= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Ordering Documentation

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 submit comments about Cisco documentation 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 will find information about how to:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at 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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only — 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.

- For 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 (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.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.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

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)—An existing 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 operations 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 the network is impaired, while 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.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

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

- 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

About This Guide





About This Guide

This section covers these topics:

- [How to Use This Document, page 1-1](#)
- [New and Changed Information for Release 5.1\(1\), page 1-2](#)
- [Release 5.0\(4\) Documentation Guide, page 1-5](#)

How to Use This Document

The *Cisco Unified CallManager New and Changed Information Guide* provides new or changed information for Cisco Unified CallManager Release 5.1(1) software components. Much of the functionality and feature content for this release remains the same as Cisco Unified CallManager Release 5.0(4).

This document acts as a supplement to the Cisco Unified CallManager Release 5.0(4) document set. Content in this guide supersedes information that the Cisco Unified CallManager Release 5.0(4) documents contain; however, chapters in this guide may contain references to Cisco Unified CallManager 5.0(4) documents for additional information.



Note

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

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

You can find both PDF versions of entire chapters and PDF versions of entire books at this URL. PDF versions of entire chapters may contain later information than whole-book PDFs.

The 5.0(4) release online help provides the basis for the online help that was provided with your system for this release.

New and Changed Information for Release 5.1(1)

This section provides new and changed information for Release 5.1(1).

Cisco Unified CallManager Administration Guide

The chapters in this part include the following new and changed information:

- Release 5.1(1) of Cisco Unified CallManager adds support for the Advanced Audio Codec (AAC) when configuring regions (see the [“Region Configuration”](#) chapter for more information).
- The System menu in Cisco Unified CallManager Administration include the License Capabilities option (see the [“License Capabilities Assignment Configuration”](#) chapter for more information).
- The Basic and Advanced Third-Party SIP Phone Configuration windows includes a check box called Require DTMF Reception (see the [Configuring Non-Cisco SIP Phones, page 4-1](#) chapter for more information).
- The TFTP Service Parameter no longer offers the Enable Caching of Configuration Files option (see the [“Cisco TFTP”](#) chapter for more information).
- Release 5.1(1) of Cisco Unified CallManager adds support for the DirSync service to synchronize information from additional types of corporate directories to the Cisco Unified CallManager database (see the [“DirSync Service”](#) section on page 9-3 in the [“Understanding the Directory”](#) chapter for more information).

Cisco Unified CallManager System Guide

The chapters in this part include the following new and changed information:

- Release 5.1(1) of Cisco Unified CallManager adds support for the Advanced Audio Codec (AAC) for calls between SIP phones (see the [“System-Level Configuration Settings”](#) chapter for more information).
- Release 5.1(1) of Cisco Unified CallManager adds Enhanced Immediate Divert feature (see the [“Cisco Unified IP Phones”](#) chapter for more information).
- Release 5.1(1) of Cisco Unified CallManager adds Call Forward All (CFA) override feature (see the [“Cisco Unified IP Phones”](#) and [“Understanding Directory Numbers”](#) chapters for more information).
- Directory/LDAP supports Sun Java Directory Server 5.2 (see the [“Understanding the Directory”](#) chapter for more information).
- This chapter provides supported voice gateways, protocols, trunk interfaces, and port updates (see the [“Understanding Cisco Unified CallManager Voice Gateways”](#) chapter for more information).

Cisco Unified CallManager Features and Services Guide

The chapters in this part include the following new and changed information:

- The enhanced Immediate Divert (iDivert) feature adds these new service parameters: Use Legacy iDivert, Allow QSIG During iDivert, iDivert User Response Timer (see the [“Setting the Service Parameters for Immediate Divert”](#) section on page 13-10 of the [“Immediate Divert”](#) chapter for more information). The chapter also describes the changed functionality of the Immediate Divert feature in the enhanced and legacy modes.
- The Music On Hold feature adds the following service parameter: Multicast MOH Direction Mode for SIP (see the [“Multicast and Unicast Audio Sources”](#) section on page 12-10 for more information).
- Checking the Allow Control of Device from CTI check box on the Phone Configuration window ensures call control comes up for the attendant console (see the [“Cisco Unified CallManager Attendant Console”](#) chapter for more information).

Cisco Unified CallManager Serviceability Administration Guide

The chapters in this part include the following new and changed information:

- An updated procedure on how to configure troubleshooting trace settings in Cisco Unified CallManager Serviceability (see the [“Troubleshooting Trace Setting Configuration”](#) chapter for more information).
- New information on how to zoom in on an area of a chart for a predefined object in RTMT (see the [“Real-Time Monitoring Configuration”](#) chapter for more information).
- An updated procedure on how to install the Cisco Unified CallManager Real-Time Monitoring Tool plug-ins; that is, Cisco Unified CallManager Real-Time Monitoring Tool-Linux or Cisco Unified CallManager Real-Time Monitoring Tool-Windows (see the [“Real-Time Monitoring Configuration”](#) chapter for more information).
- Updated information on viewing the Database Summary window in the Cisco Unified CallManager Real-Time Monitoring Tool (see the [“Real-Time Monitoring Configuration”](#) chapter for more information).
- Updated multiserver service activation recommendations for the Cisco SOAP-CDRonDemand Service, Cisco CAR Scheduler service, Cisco CAR Web Service, and Cisco TAPS Service (see the [“Managing Services”](#) chapter for more information).
- Updated information on configuring a remote syslog server as the alarm destination (see the [“Alarm Configuration”](#) chapter for more information).

Cisco Unified CallManager Serviceability System Guide

The chapters in this part include the following new and changed information:

- Updated information on how troubleshooting trace works (see the [“Trace”](#) chapter for more information).
- Updated information on configuring a remote syslog server as the alarm destination (see the [“Alarms”](#) chapter for more information).

- New information on the Cisco SOAP-CDRonDemand Service, Cisco TAPS Service, and A Cisco DB Replicator service; updated information on the Cisco CAR Scheduler service and the Cisco CAR Web Service (see the [“Service Management”](#) chapter for more information).
- Updated information on viewing the Database Summary window in the Cisco Unified CallManager Real-Time Monitoring Tool (see the [“Real-Time Monitoring Tool”](#) chapter for more information).
- Updated information on accessing log files through the Cisco Unified CallManager Real-Time Monitoring Tool (see the [“Real-Time Monitoring Tool”](#) chapter for more information).
- New information on the performance counter, ThreadsBusy, which supports the Cisco Tomcat Connector object (see the [“Performance Objects and Counters”](#) chapter for more information).
- Updated information on the performance counter, CallsInProgress, which supports the Cisco CallManager object (see the [“Performance Objects and Counters”](#) chapter for more information).
- Updated information on the performance counter, Process Status, which supports the Process object (see the [“Performance Objects and Counters”](#) chapter for more information).

Cisco Unified CallManager CDR Analysis and Reporting Administration Guide

The chapters in this part include the following new and changed information:

- Updated information on how CAR database purging works (see the [“CDR Analysis and Reporting Overview”](#) and the [“CAR System Configuration”](#) chapters for more information).
- Updated information on how CDR search works (see the [“CDR Analysis and Reporting Overview”](#) and the [“CDR Search Configuration”](#) chapters for more information).
- New information on how CAR generates e-mail addresses when it sends automatically generated reports to CAR administrators (see the [“CAR Report Configuration”](#) chapter for more information).
- New information on when _unspecifieduser displays in CAR reports (see the [“CAR Report Results”](#) chapter for more information).

Cisco Unified CallManager Call Detail Record Definitions

Cisco Unified CallManager Release 5.1(1) adds a single new codec type, Media_Payload_AAC = 42 (see the [“Call Detail Record Definitions”](#) chapter for more information). This chapter contains an updated table only; it is not replacement chapter.

Cisco Unified CallManager Security Guide

The chapters in this part include the following new and changed information:

- Securing a Cisco PIX Firewall as part of a secure Cisco Unified CallManager system (see the [“Configuring the Cisco CTL Client”](#) chapter for more information).
- Updated information for Cisco Unified IP SIP Phone support for the Exclude Digest Credentials option for encrypted files (see the [“Configuring Encrypted Phone Configuration Files”](#) chapter for more information).
- Upgrading Cisco Unified IP Phones to use LSCs for TLS connection to Cisco Unified CallManager and removing MIC root certificates from the CallManager trust store to avoid possible future compatibility issues (see the [“Security Overview”](#) and [“Configuring a Phone Security Profile”](#) chapters for more information).

Cisco Unified CallManager Bulk Administration Guide

The chapters in this part include the following new and changed information:

- New menus in BAT: CUPS menu to update and export licenses (see the [“Working with Licenses”](#) chapter for more information).
- New menu in BAT: Region Matrix menu to populate and depopulate the region matrix (see the [“Updating the Region Matrix”](#) chapter for more information).

Cisco Unified CallManager Developers Guide

The chapters in this part include the following new and changed information:

- WebDialer requires HTTPS (see the [“WebDialer API Programming”](#) chapter for more information).
- See [“AXL Programming”](#) for new AXL API calls, a new AXL service parameter, and an updated C / C++ example.

Cisco Unified IP Phones Information

The chapters in this part include the following new and changed information:

- Transfer to voicemail with iDivert softkey (see the [“Enhanced Immediate Divert Behavior”](#) chapter for more information)
- Arabic support (see the [“Arabic Support”](#) chapter for more information)

These chapters contain only introductory information for these features. The Cisco Unified IP Phone administration and user guides provide more information.

Release 5.0(4) Documentation Guide

The documentation that supports Cisco Unified CallManager Release 5.1(1) comprises existing release 5.0(4) documentation that is listed in this documentation guide, as well as the following new release 5.1(1) documents (also listed in this documentation guide):

- *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*
- *Release 5.1(1) Release Notes for Cisco Unified CallManager*
- *Upgrading Cisco Unified CallManager, Release 5.1(1)*
- *Installing Cisco Unified CallManager, Release 5.1(1)*
- *Data Migration Assistant Administration Guide, Release 5.1(1)*
- *Cisco Unified Communications Operating System Administration Guide, Release 5.1(1)*
- *Cisco Unified Communications Locale Installer Release Notes for Cisco Unified CallManager, Release 5.1*

The *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)* is a new document that is specific to release 5.1(1). See the [“Cisco Unified CallManager New and Changed Information Guide, Release 5.1\(1\)”](#) section on page 1-8 for more information.

This document lists and describes the documents that make up the Cisco Unified CallManager suite of installation and configuration documents. It contains the following sections:

- [Cisco Unified CallManager Installation Documentation, page 1-7](#)
- [Cisco Unified CallManager Configuration Documentation, page 1-8](#)
- [Cisco Unified CallManager Developer Guides, page 1-10](#)
- [Related Product Documentation, page 1-11](#)

**Note**

This documentation guide represents the only printed document that ships with Cisco Unified CallManager Release 5.1(1). Because all the available documentation is online, this document provides the online URLs.

Cisco Unified CallManager Installation Documentation

This section lists Cisco Unified CallManager install-related documentation.



Tip

The documents in this section post to www.cisco.com and Cisco Connection Online (CCO).

Data Migration Assistant (DMA) User Guide, Release 5.1(1)

This document describes the data migration tool that you must install and run on your existing Cisco Unified CallManager system prior to upgrading to Cisco Unified CallManager 5.1.

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_1/install/upgrade/index.htm

Disaster Recovery System Administration Guide, Release 5.0(4)

This document provides an overview of the Disaster Recovery System and provides procedures for performing various backup- and restore-related tasks.

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_0/drs/index.htm

Installing Cisco Unified CallManager, Release 5.1(1)

This document provides procedures for installing Cisco Unified CallManager on the publisher database and subscriber servers.

To obtain copies of this document, refer to the URL

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_1/install/instcall/index.htm

Installing Cisco Security Agent for Unified CallManager

This document provides installation instructions and information about Cisco Security Agent (CSA) for Cisco Unified CallManager Release 4.1, 4.2, 5.0, and 5.1.

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/csa/index.htm

Upgrading Cisco Unified CallManager, Release 5.1(1)

This document provides procedures for upgrading from previous versions of Cisco Unified CallManager to Cisco Unified CallManager 5.1(1).

This document also provides information on replacing hardware while you perform the upgrade.

To obtain copies of this document, refer to the URL

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_1/install/upgrade/index.htm

Cisco Unified CallManager Configuration Documentation

This section lists Cisco Unified CallManager configuration documentation that is available only on www.cisco.com and CCO. Cisco does not print the documentation that is in this section, and you cannot order the documentation through Manufacturing.

Cisco Unified CallManager CDR Analysis and Reporting Administration Guide, Release 5.0(4)

This document describes how to configure and use Cisco Unified CallManager CDR Analysis and Reporting (CAR), a tool that is used to create user, system, device, and billing reports.

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_0/service/serv504/car/index.htm

Cisco Unified CallManager Administration Guide, Release 5.0(4)

This document provides step-by-step instructions for configuring, maintaining, and administering the Cisco Unified CallManager voice over IP network.

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_0/sys_ad/5_0_4/ccmcfg/index.htm

Cisco Unified CallManager Attendant Console User Guide, Release 5.0(4)

This document provides reference and procedural information for users who are operating the Cisco Unified CallManager Attendant Console. This release provides localized versions of the *Cisco Unified CallManager Attendant Console User Guide* in multiple languages.

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/attendant/call_att/index.htm

Cisco Unified CallManager Bulk Administration Guide, Release 5.0(4)

This document provides step-by-step instructions for adding, updating, or deleting large numbers of users, devices, and ports on specific devices.

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_0/bulk_adm/5_0_4/index.htm

Cisco Unified CallManager Features and Services Guide, Release 5.0(4)

This document provides key concepts, terminology, and descriptive information about features and high-level administrative tasks that involve Cisco Unified CallManager.

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_0/sys_ad/5_0_4/ccmfeat/index.htm

Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)

The *Cisco Unified CallManager New and Changed Information Guide* provides new or changed information for Cisco Unified CallManager Release 5.1(1) software components. Much of the functionality and feature content for this release remains the same as Cisco Unified CallManager Release 5.0(4).

This document acts as a supplement to the Cisco Unified CallManager Release 5.0(4) document set. Content in this guide supersedes information that the Cisco Unified CallManager Release 5.0(4) documents contain; however, chapters in this guide may contain references to Cisco Unified CallManager 5.0(4) documents for additional information.

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_1/doc_gd/index.htm

Cisco Unified CallManager Security Guide, Release 5.0(4)

This document provides step-by-step instructions on how to configure authentication and encryption for Cisco Unified CallManager, Cisco Unified IP Phones, SRST references, Cisco MGCP gateways, and Cisco Unity voice-messaging ports. This guide also discusses authorization for SIP trunk messages.

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/ae/sec504/index.htm

Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)

This document provides step-by-step instructions for configuring alarms, traces, and other reporting for Cisco Unified CallManager serviceability and remote serviceability.

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_0/service/serv504/ccmsrva/index.htm

Cisco Unified CallManager Serviceability System Guide, Release 5.0(4)

This document provides descriptions of Cisco Unified CallManager serviceability and remote serviceability as well as links to associated *Cisco Unified CallManager Serviceability Administration Guide* procedures.

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_0/service/serv504/ccmsrvs/index.htm

Cisco Unified CallManager System Guide, Release 5.0(4)

This document provides descriptions of the Cisco Unified CallManager system and its components, configuration checklists, and links to associated *Cisco Unified CallManager Administration Guide* and *Cisco Unified CallManager Features and Service Guide* procedures.

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_0/sys_ad/5_0_4/ccmsys/index.htm

Cisco Unified Communications Locale Installer Release Notes for Cisco Unified CallManager, Release 5.1

The *Cisco Unified Communications Locale Installer Release Notes for Cisco Unified CallManager* is used in conjunction with the *Cisco Unified Communications Operating System Administration Guide* and the readme document that accompanies the Locale Installer on cisco.com.

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/locinst/index.htm

Cisco Unified Communications Operating System Administration Guide, Release 5.1(1)

The *Cisco Unified Communications Operating System Guide* provides information about using the Cisco Unified Communications Platform graphical user interface (GUI) and the command line interface (CLI) to perform many common system- and network-related tasks.

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_1/cucos/511/index.htm

Release Notes for Cisco Unified CallManager Release 5.1(1)

This document lists and describes the system requirements, new features, changed information, documentation updates, and open caveats for Cisco Unified CallManager Release 5.1(1).

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_1/rel_note/index.htm

Troubleshooting Guide for Cisco Unified CallManager, Release 5.0(4)

This document provides troubleshooting procedures for solving Cisco Unified CallManager system and configuration problems.

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_0/trouble/trbl_504/index.htm

Cisco Unified CallManager Developer Guides

This section lists Cisco Unified CallManager third-party developer documentation that is available only on www.cisco.com and CCO. Cisco does not print the documentation that is in this section, and you cannot order the documentation through Manufacturing.

Cisco Unified CallManager JTAPI Developers Guide, Release 5.0(4)

This guide describes the Cisco implementation of JTAPI for the Cisco Unified CallManager platform. Cisco conforms as closely as possible to the JTAPI specification while providing extensions that enhance JTAPI and expose the advanced features of Cisco Unified CallManager to applications.

http://www.cisco.com/univercd/cc/td/doc/product/voice/vpdd/cdd/5_0/index.htm

Cisco Unified CallManager TAPI Developers Guide, Release 5.0(4)

This guide describes the Cisco TAPI Service Provider (TSP), which allows developers to create customized IP telephony applications for Cisco users. The Cisco TAPI implementation uses the Microsoft TAPI v2.1 specification and supplies extension functions to support Cisco Unified Communications Solutions.

http://www.cisco.com/univercd/cc/td/doc/product/voice/vpdd/cdd/5_0/index.htm

Cisco Unified CallManager Call Detail Record Definitions, Release 5.0(4)

This document describes the format and logic of the call detail records (CDRs) and call management records (CMRs) that the Cisco Unified CallManager Release 5.0(4) system generates.

http://www.cisco.com/univercd/cc/td/doc/product/voice/vpdd/cdd/5_0/index.htm

Cisco Unified CallManager Data Dictionary, Release 5.1(1)

This document describes the data that the primary Cisco Unified CallManager database stores for Release 5.1(1). This document automatically generates from the actual development data dictionary that is used to create the SQL scripts for installing the Cisco Unified CallManager database.

http://www.cisco.com/univercd/cc/td/doc/product/voice/vpdd/cdd/5_1/index.htm

Cisco Unified CallManager Developers Guide, Release 5.0(4)

This guide includes the AXL, AXL Serviceability, Extension Mobility, and WebDialer APIs.

The Cisco Unified CallManager AXL implementation allows applications to modify the Cisco Unified CallManager system database.

Cisco Unified CallManager Real-Time information, Performance Counters, and Database information exposure occurs through the AXL Serviceability API.

The Cisco Extension Mobility Service provides a rich API, which enables extension mobility on IP phones and allows application control over authentication, scheduling, and availability.

The Cisco WebDialer application enables click-to-dial functionality by creating hyperlinked telephone numbers in a company directory.

http://www.cisco.com/univercd/cc/td/doc/product/voice/vpdd/cdd/5_0/index.htm

Cisco Unified IP Phone Service Application Development Notes for Cisco Unified CallManager 5.0(4)

This document provides the information that is needed for programmers and system administrators to develop and deploy new Cisco Unified IP Phone services with Cisco Unified CallManager 5.0, using eXtensible Markup Language (XML) objects and the Hypertext Transfer Protocol (HTTP) with standard web servers. Cisco conforms as closely as possible to the XML and HTTP standards while providing maximum service functionality for Cisco Unified IP Phones.

http://www.cisco.com/univercd/cc/td/doc/product/voice/vpdd/cdd/5_0/index.htm

Related Product Documentation

This section lists additional documentation that is available on the World Wide Web at www.cisco.com.



Note

For voice product documentation that is not specified in this section, refer to <http://www.cisco.com/univercd/cc/td/doc/product/ipcvoice.htm>.

Cisco Unified CallManager 5.1 TCP and UDP Port Usage

This document provides a list of the TCP and UDP ports that Cisco Unified CallManager 5.1 uses for intracluster connections and for communications with external applications or devices. It provides important information for the configuration of firewalls, Access Control Lists (ACLs), and quality of service (QoS) on a network when an IP Communications solution is implemented.

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/udp_tcp/index.htm

Cisco Unified CallManager Attendant Console Keyboard Shortcuts

This quick-reference guide lists keyboard shortcuts that are used with the Cisco Unified CallManager Attendant Console. The attendant can attach this document to the monitor or place it on the keyboard.

To access copies of this document online, refer to the URL

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/attendnt/call_att/index.htm

You can order copies of this document by using the following customer order number:

DOC-7817425=

Cisco Unified CallManager Compatibility Matrix

You can find which application versions and third-party components are compatible with Cisco Unified CallManager release 5.1(1) by referring to the *System Release Notes for IP Telephony: Cisco Unified Communications Release 5.1* at

<http://www.cisco.com/univercd/cc/td/doc/systems/unified/uc511/relnotes/rnpt511.htm>

Cisco Unified CallManager Security Token Advisory

This document describes the purpose of the Cisco System Administrator Security Token.

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/ae/etoken/index.htm

Cisco Unified Communications SRND Based on Cisco Unified CallManager 5.0

This Solution Reference Network Design (SRND) document provides design considerations and guidelines for deploying the following components of the Cisco Unified Communications System: Cisco Unified CallManager, Cisco Unified MeetingPlace, Cisco Unity, and Cisco Unified Video Advantage.

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_0/srnd5_0/index.htm

Cisco Unified IP Phones and Services

The following location provides documentation for administering and using the Cisco IP Phones and services:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm



PART 2

Cisco Unified CallManager Administration Guide





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 2-8](#) 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 2-1](#)
- [Configuring a Region, page 2-3](#)
- [Related Topics, page 2-8](#)
- [Deleting a Region, page 2-7](#)

Refer to the [“Regions”](#) section in the *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*, 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, 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 > 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 2-8.

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 that are to be used within the same region, and you also define audio codec values that are to be used between regions.
- **Video Call Bandwidth**—You define video call bandwidth values that are to be used within the same region, and you also define video call bandwidth values that are 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 2-1](#) 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 2-2](#) 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 2-2](#) 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 in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*, for information on configuring device pools.

Additional Information

See the [“Related Topics” section on page 2-8](#).

Region Configuration Settings

[Table 2-1](#) 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 2-8](#).

Table 2-1 **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 2-1 *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 2-3. - 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 2-2](#) apply for 30-ms data packets and include IP headers. Each call comprises two call streams.

**Note**

The codecs that [Table 2-2](#) specifies 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 2-2 *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 2-2 **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. Use this audio codec if you want to configure the Advanced Audio Codec (AAC) for calls between SIP phones. Advanced Audio Codec (AAC) specifies a wideband voice codec that provides improved voice fidelity and equal or better sound quality over older codecs.
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 in the *Cisco Unified CallManager System Guide, Release 5.0(4)*.

If you attempt to delete a region that is in use, Cisco Unified CallManager displays a 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 in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.
- Delete the device pools that use the region that you want to delete. See the “Deleting a Device Pool” section in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

Procedure

-
- Step 1** Find the region by using the procedure in the [“Finding a Region” section on page 2-1](#).
- 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 2-8](#).

Related Topics

- [Region Configuration, page 2-1](#)
- [Finding a Region, page 2-1](#)
- [Configuring a Region, page 2-3](#)
- [Region Configuration Settings, page 2-5](#)
- [Deleting a Region, page 2-7](#)



License Capabilities Assignment Configuration

Capabilities Assignment allows system administrators to enable the Cisco Unified Presence Server (CUPS) and Cisco Unified Personal Communicator (CUPC) capabilities for users. You must ensure that licenses for CUPS and CUPC are available.

Make license capabilities assignments to existing users. Before you begin, ensure that users exist on your system by choosing **User Management > End User** and clicking **Find**.

Before you begin configuring the capabilities assignments for users, determine how many CUPS (servers and clients) and CUPC licenses are required for your system by choosing **Licensing > License Unit Calculator**. Acquire the required licenses by using **Licensing > License File Upload**. Verify the total licenses by using **Licensing > License Unit Report**.

Use the following topics to add or update a license capabilities assignment:

- [Finding a License Capabilities Assignment, page 3-1](#)
- [Configuring the Capabilities Assignments for One User, page 3-2](#)
- [Configuring the Capabilities Assignments for Multiple Users, page 3-3](#)
- [License Capabilities Assignment Configuration Settings, page 3-4](#)
- [Related Topics, page 3-4](#)

Finding a License Capabilities Assignment

Because you might have several license capabilities assignments for users in your network, Cisco Unified CallManager Administration lets you locate specific capabilities assignments 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 > Licensing > Capabilities Assignment**.

The Find and List Capabilities Assignment window displays. Use the two drop-down list boxes to search for a capabilities assignment.

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

- User ID
- Last Name
- Manager
- Department

From the second Find capabilities assignment 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 locations that are registered in the database, click **Find** without entering any search text.

A list of discovered capabilities assignments displays by

- User ID
- Last Name
- Manager
- Department
- UPS Enabled
- UPC Enabled

Step 4 From the list of records, click the user name for whom you want to make capabilities assignments. The Capabilities Assignments Configuration window displays.

Additional Information

See the [“Related Topics”](#) section on page 3-4.

Configuring the Capabilities Assignments for One User

This section describes how to add or update a capabilities assignment for a user to the Cisco Unified CallManager database.

Before You Begin

Before configuring a capabilities assignment, you must obtain licenses from Cisco Systems by using the License File Upload under the System menu.

Procedure

-
- Step 1** Choose **System > Licensing > Capabilities Assignment**.
- The Find and List Capabilities Assignment window displays.
- Step 2** To add a new capabilities assignment or update an existing capabilities assignment, locate the appropriate capabilities assignment as described in the [“Finding a License Capabilities Assignment” section on page 3-1](#) and continue with [Step 3](#).
- The Capabilities Assignments Configuration window displays.
- Step 3** Check the appropriate check box as described in [Table 3-1](#).
- Step 4** To save the capabilities assignment information in the database, click **Save**.
-

Additional Information

See the [“Related Topics” section on page 3-4](#).

Configuring the Capabilities Assignments for Multiple Users

This section describes how to add or update capabilities assignments for multiple users to the Cisco Unified CallManager database.

Before You Begin

Before configuring a capabilities assignment, you must obtain licenses from Cisco Systems by using the License File Upload under the System menu.



Note Up to 250 users can be assigned licenses when using the Bulk Assignment capability.

Procedure

-
- Step 1** Choose **System > Licensing > Capabilities Assignment**.
- The Find and List Capabilities Assignment window displays.
- Step 2** To add a new capabilities assignment or update an existing capabilities assignment, locate the appropriate capabilities assignment as described in the [“Finding a License Capabilities Assignment” section on page 3-1](#) and continue with [Step 3](#).
- Step 3** To enable a new capabilities assignment or to update an existing capabilities assignment for multiple users, check the check boxes next to the users or click the **Select All** button.
- Step 4** Click the **Bulk Assignment** button.
- The Capabilities Assignments Configuration window displays.

- Step 5** Check the appropriate check box as described in [Table 3-1](#).
- Step 6** To save the capabilities assignment information in the database, click **Save**.

Additional Information

See the “[Related Topics](#)” section on page 3-4.

License Capabilities Assignment Configuration Settings

[Table 3-1](#) describes the license capabilities assignment configuration settings. For related procedures, see the “[Related Topics](#)” section on page 3-4.

Table 3-1 License Capabilities Assignment Configuration Settings

Field	Description
User Information	
User ID	Displays the name of the user for which you are enabling capabilities assignment.
Capabilities Assignment Information	
Enable UPS (Unified Presence Server)	To enable CUPS for this user, check the Enable UPS (Unified Presence Server) check box.
Enable UPC (Unified Personal Communicator)	To enable CUPC for this user, check the Enable UPC (Unified Personal Communicator) check box. You can enable both CUPS and CUPC; however, if you want CUPC, you must also enable CUPS.

Related Topics

- [License Capabilities Assignment Configuration, page 3-1](#)
- [Finding a License Capabilities Assignment, page 3-1](#)
- [Configuring the Capabilities Assignments for One User, page 3-2](#)
- [Configuring the Capabilities Assignments for Multiple Users, page 3-3](#)
- [License Capabilities Assignment Configuration Settings, page 3-4](#)
- *Cisco Unified CallManager Bulk Administration Guide*



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 chapter describes how to configure the third-party SIP phones by using Cisco Unified CallManager Administration.

This chapter contains the following sections:

- [SIP Phone Configuration Differences, page 4-1](#)
- [Migrating from Cisco Unified CallManager Release 5.0\(1\), and above, to Cisco Unified CallManager, Release 5.1\(1\), page 4-3](#)
- [Third-Party SIP Phone Configuration Checklist, page 4-4](#)
- [Where to Find More Information, page 4-5](#)

SIP Phone Configuration Differences

[Table 4-1](#) provides a comparison overview of the configuration differences between Cisco SIP IP Phones and third-party SIP phones.

Table 4-1 *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

Use Cisco Unified CallManager Administration to configure third-party SIP phones (see the [“Third-Party SIP Phone Configuration Checklist”](#) section on page 4-4). The administrator must also perform configuration steps on the third-party SIP phone; see following examples:

- Ensure proxy address in the phone is the IP or Fully Qualified Domain Name (FQDN) of Cisco Unified CallManager
- Ensure directory number(s) in the phone match the directory number(s) that are configured for the device in Cisco Unified CallManager Administration
- Ensure digest user ID (sometimes referred to as Authorization ID) in the phone matches the Digest User ID in Cisco Unified CallManager Administration

Consult the documentation that came with the third-party SIP phone for more information.

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 in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*). 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, in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*).



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 gets 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 Phone Security Profile. (See Phone Security Profile Configuration in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.) On the 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.

DTMF Reception

To require DTMF reception, check the Require DTMF Reception check box that displays on the Phone Configuration window in Cisco Unified CallManager Administration.

Migrating from Cisco Unified CallManager Release 5.0(1), and above, to Cisco Unified CallManager, Release 5.1(1)

In Cisco Unified CallManager, Release 5.1(1) and above, certain characteristics for Basic and Advanced Third-Party SIP Phones changed. These characteristics include changes to the Maximum Number of Calls per Device, Default Maximum number of calls per DN, and Default Busy Trigger per DN fields that display on the Directory Number Configuration window in Cisco Unified CallManager Administration. See [Table 4-2](#) and [Table 4-3](#) for more information.

Table 4-2 *Directory Number Migration Changes for Basic Third-Party SIP Phones*

Field Name	Old Value	New Value
Maximum Number of Calls Per Device	8	2
Default Maximum Number of Calls per DN	4	2
Default Busy Trigger per DN	2	2

Table 4-3 *Directory Number Migration Changes for Advanced Third-Party SIP Phones*

Field Name	Old Value	New Value
Maximum Number of Calls Per Device	64	16
Default Maximum Number of Calls per DN	4	2
Default Busy Trigger per DN	2	2

For users that have third-party SIP phones that are configured on release 5.0(1) and above that are migrating/upgrading to release 5.1(1) or above, be aware after the upgrade, these devices retain their release 5.0 configured values. However, if users need to make changes to DN configuration values, users must change Maximum Number of Calls and Default Busy Trigger values on each DN.

For basic third-party SIP phones, only one line value needs to be modified. However, for advanced third-party SIP phones, users potentially must disassociate lines on the device before they can make any DN-related configuration changes. This situation potentially can happen if more than four lines are configured. An example scenario follows:

- Advanced phone configured with 6 lines with Maximum number of calls = 4 and Busy Trigger = 2 for each of the lines.
- After upgrade to release 5.1 or above, ensure maximum number of calls on the device is reduced to 16 or below before any DN changes. The current value on this phone equals 24 (6 lines * 4). The device essentially exists in a negative zone (16-24).
- User would disassociate two lines from the device.
- After the user disassociates those lines from the device, you can modify the DN characteristics for the remaining four lines by setting Maximum Number of Calls and Busy Trigger to an appropriate value.
- User reassociates the disassociated lines.

Third-Party SIP Phone Configuration Checklist

Table 4-4 provides steps to manually configure a third-party SIP phone by using Cisco Unified CallManager Administration.

Table 4-4 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, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
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, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> Configuring Cisco Unified IP Phones, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>

Table 4-4 Third-Party SIP Phone Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 4	Configure the Phone Security Profile. To use digest authentication, you must configure a new phone security profile. If you use one of the standard, nonsecure SIP profiles that are provided for auto-registration, you cannot enable digest authentication.	Enabling Digest Authentication for Third-Party SIP Phones, page 4-2 Phone Security Profile Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> <i>Cisco Unified CallManager Security Guide, Release 5.0(4)</i>
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, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 6	Add and configure lines (DNs) on the phone.	Directory Number Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
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, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
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, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
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, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Cisco Unified IP Phone Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- SIP Profile Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- End User Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Cisco Unified IP Phones, *Cisco Unified CallManager System Guide, Release 5.0(4)*



PART 3

Cisco Unified CallManager System Guide





System-Level Configuration Settings

Configure system-level settings before you add devices and configure other Cisco Unified CallManager features. This section covers the following topics:

- [Server Configuration, page 5-1](#)
- [Cisco Unified CallManager Configuration, page 5-2](#)
- [Cisco Unified CallManager Groups, page 5-3](#)
- [Phone NTP Reference Configuration for SIP Phones, page 5-4](#)
- [Date/Time Groups, page 5-4](#)
- [Regions, page 5-5](#)
- [Device Pools, page 5-10](#)
- [LDAP, page 5-12](#)
- [Call Admission Control, page 5-13](#)
- [Survivable Remote Site Telephony References, page 5-13](#)
- [MLPP Domain, page 5-15](#)
- [Enterprise Parameters, page 5-15](#)
- [Service Parameters, page 5-16](#)
- [System Configuration Checklist, page 5-17](#)
- [Dependency Records, page 5-16](#)
- [Where to Find More Information, page 5-18](#)

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.

Adding a Server

The following guidelines apply to adding a server:

- 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** and then configure the server. After you add the subsequent server, you can then install the Cisco Unified CallManager software on that server.
- Add each server only once on the Server Configuration window. If you add a server by using the host name and add the same server by 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 the system.
- Any changes that you make to the server configuration do not take effect until you restart Cisco Unified CallManager.

Deleting a Server



Note

You cannot delete a server that has a specific Cisco Unified CallManager that is running on it.

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

Before deleting a server that is currently in use, you must perform the following tasks:

- Update the Cisco Unified CallManager in question and assign it to a different server or delete the Cisco Unified CallManager that is assigned to that server.
- Delete the conference bridges, MTPs, and MOH servers that use the server that you want to delete.



Note

The system may automatically delete some devices, such as MOH servers, when you delete a server.

- Deactivate the services that are running on that server.

For more information, refer to the *Cisco Unified CallManager Administration Guide*, the *Cisco Unified CallManager Serviceability Administration Guide*, and the *Cisco Unified CallManager Features and Services Guide*.

Cisco Unified CallManager Configuration

The Cisco Unified CallManager servers get added to Cisco Unified CallManager at installation time. Use Cisco Unified CallManager configuration to update fields such as 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.

Any changes that you make to the settings for auto-registration partition, external phone number mask, and voice message box mask do not take effect until you restart Cisco Unified CallManager.

**Note**

When you perform a fresh installation of Cisco Unified CallManager, you must activate the Cisco Unified CallManager service. For information about activating the Cisco Unified CallManager service, refer to the *Cisco Unified CallManager Serviceability Administration Guide*.

Cisco Unified CallManager Groups

A Cisco Unified CallManager group comprises 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 (backup) Cisco Unified CallManagers.

Cisco Unified CallManager groups associate with devices through device pools. Each device belongs to a device pool, and each device pool specifies the Cisco Unified CallManager group for all of its devices.

**Note**

Some Media Gateway Control Protocol (MGCP) devices, such as gateways and route/hunt lists, can associate directly with Cisco Unified CallManager groups.

Cisco Unified CallManager groups provide two important features for your system:

- **Prioritized failover list for backup call processing**—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. Each device pool has one Cisco Unified CallManager group that is assigned to it.
- **Call processing load balancing**—You can configure device pools and Cisco Unified CallManager groups to distribute the control of devices across multiple Cisco Unified CallManagers. See the “Balanced Call Processing” section of the *Cisco Unified CallManager System Guide, Release 5.0(4)*, for more information.

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

Adding a Cisco Unified CallManager Group

- Cisco Unified CallManagers automatically get installed and configured.
- 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.
- You must reset the devices that use the updated Cisco Unified CallManager group to apply any changes that you make.

Deleting a Cisco Unified CallManager Group

**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**.

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.
- Create or choose a different Cisco Unified CallManager group to be the Auto-registration Cisco Unified CallManager Group.

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

Phone NTP Reference Configuration for SIP Phones

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 an NTP server. If a SIP phone cannot get its date/time from the provisioned “Phone NTP Reference,” the phone will receive this information when it registers with Cisco Unified CallManager.

Adding a Phone NTP Reference

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 window.

Deleting a Phone NTP Reference

Before you can delete a phone NTP reference from Cisco Unified CallManager Administration, you must delete the server 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**.

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 “Dependency Records” section in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

Date/Time Groups

Use Date/Time Groups to define time zones for the various devices that are connected to Cisco Unified CallManager.

Cisco Unified CallManager provides a default Date/Time Group that is called CMLocal that configures automatically when you install Cisco Unified CallManager; however, Cisco recommends that you configure a group for each local time zone. CMLocal synchronizes to the active date and time of the operating system on the Cisco Unified CallManager server. After installing Cisco Unified CallManager, you can change the settings for CMLocal as desired. Normally, you adjust the 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 a Date/Time Group for each of the 24 time zones.

Adding a Date/Time Group

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.

You must reset devices to apply any changes that you make.

Deleting a Date/Time Group**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**.

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 device pools that use the Date/Time Group that you want to delete.
- Delete the device pools that use the Date/Time Group that you want to delete.

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

Regions

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.

When you create a region, you specify the codec that can be used for calls between devices within that region, and between that region and other regions. The system uses regions also for applications that only support a specific codec; for example, an application that only uses G.711.

The audio codec type specifies the technology that is used to compress and decompress voice signals. The choice of audio codec determines the compression type and amount of bandwidth that is used per call. See [Table 5-1](#) for specific information about bandwidth usage for available audio codecs.

**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.

Cisco Unified CallManager supports video stream encryption and various audio/video codecs, such as G.722.

Regions provide capacity controls for Cisco Unified CallManager multisite deployments where you may need to limit the bandwidth for individual calls that are sent across a WAN link, but where you want to use a higher bandwidth for internal calls.

Adding a Region

To specify audio codec usage for devices that are using regions, you must perform the following tasks:

- Configure the default values for audio codec and video call bandwidth in the Cisco Unified CallManager Administration Service Parameters Configuration window.
- Create regions and specify the audio codecs to use for calls within those regions and between other regions.
- Create or modify device pools to use the regions that you created.
- Assign devices to device pools that specify the appropriate region.

**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 uses fewer resources.

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

- Regions have default values for use within a region—The recommended default value specifies G.711.
- Regions have default values for use between regions—The recommended default value specifies G.729.

**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.

For more information about configuring regions, refer to the Region Configuration chapter in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

See the “[Device Pools](#)” section on page 5-10 for more information about device pool settings. For information about codes and video calls, see the Understanding Video Telephony chapter of the *Cisco Unified CallManager System Guide, Release 5.0(4)*.

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.

**Note**

To apply any changes that you make to all devices that use the updated region, you must restart the devices.

Supported Audio Codecs and Bandwidth Usage

Cisco Unified CallManager supports the following audio codecs for use with the regions feature:

- **G.711**—Default codec for all calls through Cisco Unified CallManager.
- **G.722**—Audio codec often used in video conferences.
- **G.723**—Low-bit-rate codec with 6-kbps compression for Cisco IP Phone model 12 SP+ and Cisco IP Phone model 30 VIP devices.
- **G.728**—Low-bit-rate codec that video endpoints support.
- **G.729**—Low-bit-rate codec with 8-kbps compression supported by Cisco Unified IP Phone 7900 models. Typically, you would use low-bit-rate codecs for calls across a WAN link because they use less bandwidth. For example, a multisite WAN with centralized call processing can set up a G.711 and a G.729 region per site to permit placing intrasite calls as G.711 and placing intersite calls as G.729.
- **GSM**—The global system for mobile communications (GSM) codec. GSM enables the MNET system for GSM wireless handsets to operate with Cisco Unified CallManager. Assign GSM devices to a device pool that specifies GSM as the audio codec for calls within the GSM region and between other regions. Depending on device capabilities, this includes GSM EFR (enhanced full rate) and GSM FR (full rate).
- **Wideband**—Supported for calls from IP phone to IP phone. The wideband audio codec, uncompressed with a 16-bit, 16-kHz sampling rate, works with phones with handsets, acoustics, speakers, and microphones that can support high-quality audio bandwidth, such as Cisco Unified IP Phone 7900 model phones.

Use this audio codec if you want to configure the Advanced Audio Codec (AAC) for calls between SIP phones.

**Tip**

Regions that specify wideband as the codec type must have a large amount of network bandwidth that is available because wideband uses four times as much bandwidth as G.711.

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), as indicated in [Table 5-1](#). (The bandwidth information in [Table 5-1](#) applies to Ethernet.)

**Note**

Each call includes two streams, one in each direction.

**Note**

The codecs that [Table 5-1](#) specifies correlate to an approximate bandwidth usage per call. For more information on bandwidth usage for each codec, refer to the *Cisco Unified Communications Solution Reference Network Design (SRND)* for the current release of Cisco Unified CallManager.

Table 5-1 **Bandwidth Used Per Call by Each Codec Type**

Audio Codec	Bandwidth Used for Data Packets Only (Fixed Regardless of Packet Size)	Bandwidth Used Per Call (Including IP Headers) With 30-ms Data Packets	Bandwidth Used Per Call (Including IP Headers) With 20-ms Data Packets
G.711	64 kbps	80 kbps	88 kbps
G.722	24 kbps	80 kbps	88 kbps
G.723	6 kbps	24 kbps	Not applicable
G.729	8 kbps	24 kbps	32 kbps
Wideband ¹	256 kbps	272 kbps	280 kbps
GSM ²	13 kbps	29 kbps	37 kbps

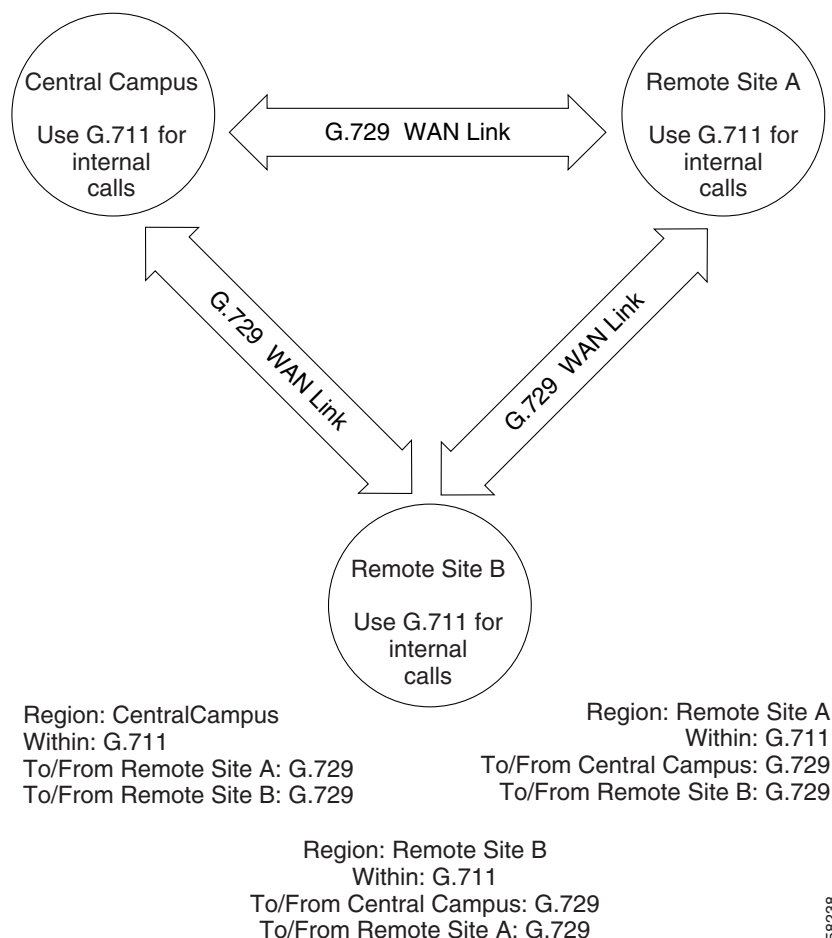
1. Uncompressed. Cisco Unified CallManager supports wideband audio from IP phone to IP phone for Cisco Unified IP Phone 7900 Family model phones only.
2. Global system for mobile communications.

Example

[Figure 5-1](#) shows a very simple region configuration example for deployment with a central site and two remote branches. In the example, an administrator configures a region for each site. The G.711 codec equals the maximum bandwidth codec that is used for calls within each site, and the G.729 codec equals the maximum bandwidth codec that is used for calls between sites across the WAN link.

After region configuration, the administrator assigns devices to the following sites:

- The Central Campus site to device pools that specify CentralCampus as the region setting
- Remote Site A to device pools that specify RemoteSiteA as the region setting
- Remote Site B to device pools that specify RemoteSiteB for the region setting

Figure 5-1 Simple Region Example

Locations and Regions

In Cisco Unified CallManager, locations-based call admission control works in conjunction with regions to define the characteristics of a network link.

- Regions define the type of codec that is used on the link (and therefore, the amount of bandwidth that is used per call).
- Locations define the amount of available bandwidth for the link.

You must assign each device on the network to both a region (by means of a device pool) and a location. See the [“Call Admission Control” section on page 5-13](#).

Deleting a Region

**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**.

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.
- Delete the device pools that use the region that you want to delete.

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

Device Pools

Device pools provide a convenient way to define a set of common characteristics that can be assigned to devices. You can specify the following device characteristics for a device pool:

- **Device Pool Name**—Specifies the name for the new device pool.
- **Cisco Unified CallManager group**—Specifies a prioritized list of up to three Cisco Unified CallManagers to facilitate redundancy. 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 (backup) Cisco Unified CallManagers. See the [“Cisco Unified CallManager Groups” section on page 5-3](#) for more details.
- **Date/Time group**—Specifies the date and time zone for a device. See the [“Date/Time Groups” section on page 5-4](#) for more details.
- **Region**—Specifies the audio and video codecs that are used within and between regions. Use regions only if you have different types of codecs within the network. See the [“Regions” section on page 5-5](#) for more details.
- **Softkey template**—Manages the softkeys that are associated with applications on Cisco Unified IP Phones. See the [“Softkey Template Configuration” section in the Cisco Unified CallManager Administration Guide, Release 5.0\(4\)](#), for more details.
- **Survivable Remote Site Telephony (SRST) reference**—Specifies the gateway that provides SRST functionality for the devices in a device pool. See the [“Survivable Remote Site Telephony References” section on page 5-13](#) for more details.
- **Calling search space for auto-registration (optional)**—Specifies the partitions that an auto-registered device can reach when a call is placed. See the [“Partitions and Calling Search Spaces” section of the Cisco Unified CallManager System Guide, Release 5.0\(4\)](#), for more details.
- **Media resource group list (optional)**—Specifies a prioritized list of media resource groups. An application chooses 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 the media resource group list. See the [“Media Resource Group Lists” section of the Cisco Unified CallManager System Guide, Release 5.0\(4\)](#), for more details.
- **Network hold music on hold (MOH) audio sources (optional)**—Specifies the audio source for network hold. See the [“Music On Hold Audio Sources” section in the Cisco Unified CallManager New and Changed Information Guide, Release 5.1\(1\)](#), for more details.
- **User hold music on hold (MOH) audio source (optional)**—Specifies the audio source for user hold. See the [“Music On Hold Audio Sources” section in the Cisco Unified CallManager New and Changed Information Guide, Release 5.1\(1\)](#), for more details.
- **Network locale**—Contains a definition of the tones and cadences that the phones and gateways use in a device pool in a specific geographic area.

**Note**

You must 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.

- User locale—Identifies a set of detailed information to support users, including language and font. This characteristic associates with the phones and gateways in a device pool.
- Connection Monitor Duration—Resolves WAN link flapping issues between Cisco Unified CallManager and SRST. See the [“Survivable Remote Site Telephony References”](#) section on [page 5-13](#) for more information.
- MLPP Precedence and Preemption Information—Manages MLPP settings:
 - MLPP Indication—Specifies whether devices in the device pool that are capable of playing precedence tones will use the capability when the devices plan an MLPP precedence call.
 - MLPP Preemption—Specifies whether devices in the device pool that are capable of preempting calls in progress will use the capability when the devices plan an MLPP precedence call.
 - MLPP Domain—Specifies a hexadecimal value for the MLPP domain that is associated with the device pool. Device pools refer to the configured MLPP domain.

**Note**

You must configure the preceding items before you configure a device pool if you want to choose the items for the device pool.

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, and CTI route points.

If using auto-registration, you can assign all devices of a given type to a device pool by using the Device Defaults window in Cisco Unified CallManager Administration.

For more information, refer to the “Updating Device Defaults” section in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

Updating Device Pools

If you make changes to a device pool, you must reset the devices in that device pool before the changes will take effect.

You cannot delete a device pool that has been assigned to any devices or one that is used for Device Defaults configuration.

To find out which devices are using the device pool, choose **Dependency Records** from the Related Links drop-down list box on the Device Pool Configuration window and click **Go**.

If you try to delete a device pool that is in use, a 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.
- Delete the devices that are assigned to the device pool that you want to delete.

LDAP

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

The LDAP directory provides applications with a standard method for accessing and modifying the information that is stored in the directory. This capability provides the benefit of enabling companies to centralize all user information in a single repository that is available to several applications, thereby reducing maintenance costs through the ease of adds, moves, and changes.

Cisco Unified CallManager provides support for an optional, external LDAP directory. When used, Cisco Unified CallManager and related applications store all application data in a local database instead of in the directory. Cisco Unified CallManager supports integration with the customer directory, and it provides default user authentication with the database as well as user authentication with the customer directory.

To use the LDAP directory with Cisco Unified CallManager, modify information directly from the LDAP server and then configure the following LDAP parameters by using Cisco Unified CallManager Administration.

- **LDAP System**—Configure this parameter to enable synchronization from the LDAP server. Choose the LDAP server type, such as Microsoft Active Directory (AD) or Netscape LDAP Server, and the LDAP attribute for the user ID.
- **LDAP Directory**—Use this parameter to find and list LDAP directories and to add information to the LDAP directory, such as LDAP configuration name, LDAP directory synchronization schedule, user fields to be synchronized, and LDAP server information. You must enable synchronization from the LDAP server on the LDAP System window before you can make any changes to this information.
- **LDAP Authentication**—Configure this parameter to enable LDAP authentication for end users. When the LDAP authentication is turned on, the system authenticates the user password against the LDAP server instead of the Cisco Unified CallManager database, and it synchronizes the end user information from the LDAP server to the Cisco Unified CallManager database. You must enable synchronization from the LDAP server on the LDAP System window before you can make any changes to this information.



Note

You can switch between LDAP parameters by choosing the menu option that you want to configure from the Related Links drop-down list box on the LDAP Configuration windows.

If you want to use your Active Directory or Netscape corporate directory with Cisco Unified CallManager, you must synchronize the directory with the Cisco Unified CallManager database by accessing **System > LDAP > LDAP System**. You set up the directory synchronization agreements by accessing **System > LDAP > LDAP Directory**.

You must activate the Cisco DirSync service from Cisco Unified CallManager Serviceability to synchronize the AD/Netscape directories. The Cisco DirSync service interacts with these directories by synchronizing the data, reading the customer directory information, and updating the Cisco Unified CallManager database.

To activate Cisco DirSync, access **Control Center > Feature Services** and navigate to Directory Services.

- Set up the directory synchronization agreements by accessing **System > LDAP > LDAP Directory**.
- Set up the configuration used by Cisco DirSync by accessing **System > LDAP > LDAP System** and **System > LDAP > LDAP Directory**.

See “[Understanding the Directory](#)” for more information about using directories with Cisco Unified CallManager.

Call Admission Control

Use call admission control to maintain a desired level of voice quality over a WAN link. For example, you can use call admission control to regulate the voice quality on a 56-kbps frame relay line that connects your main campus and a remote site.

Voice quality can begin to degrade when too many active calls exist on a link and the amount of bandwidth is oversubscribed. Call admission control regulates voice quality by limiting the number of calls that can be active at the same time on a particular link. Call admission control does not guarantee a particular level of audio quality on the link, but it does allow you to regulate the amount of bandwidth that active calls on the link consume.

Cisco Unified CallManager supports two types of call admission control:

- **Locations**—Use locations to implement call admission control in a centralized call-processing system. Call admission control lets you regulate voice quality by limiting the amount of bandwidth that is available for calls over links between the locations.
- **H.323 Gatekeeper**—Use an H.323 gatekeeper, also known as a Cisco Multimedia Conference Manager (MCM), to provide call admission control in a distributed system with a separate Cisco Unified CallManager or Cisco Unified CallManager cluster at each site.



Note

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

See the “Call Admission Control” section in the *Cisco Unified CallManager System Guide, Release 5.0(4)*, for more information.

Survivable Remote Site Telephony References

Survivable Remote Site Telephony (SRST) gets used at sites that depend on a centralized Cisco Unified CallManager cluster that is accessible via a WAN connection. SRST provides telephony service to IP phones at the remote site in the event of a WAN outage. An SRST-enabled router has features that allow calls between IP phones at the remote site to call each other, allow calls from the PSTN to reach the IP phones, and allow calls from the IP phones to reach the external world through the PSTN. Intelligence in the SRST router that can accept registrations from the IP phones and route calls based on the directory numbers that are registered, and based on the routing that is configured for the PSTN link, accomplishes that.

Survivable remote site telephony (SRST) references, a configurable option in Cisco Unified CallManager Administration, provide limited call capability in the event of a WAN outage. Using SRST references, IP gateways can take over limited Cisco Unified CallManager functionality. When phones lose connectivity to all associated Cisco Unified CallManagers, the phones in a device pool attempt to make a Cisco Unified CallManager connection to the SRST reference IP gateway.

The status line indication on the IP phone that shows the phone has failed over to the backup proxy (SRST gateway) provides the only user interactions with SRST.

Device Pool Settings for SRST

The system administrator can configure the SRST configuration for a device pool of phones. The following list gives Device Pool configuration options that are available:

- **Disable**—If a phone cannot reach any Cisco Unified CallManagers, it does not try to connect to an SRST gateway.
- **Use Default Gateway**—If a phone cannot reach any Cisco Unified CallManagers, it tries to connect to its IP gateway as an SRST gateway.
- **User-defined**—If a phone cannot reach any Cisco Unified CallManagers, it tries to connect to an administrator-specified SRST gateway. The SRST Reference field of the Device Pool Configuration lists user-defined SRST references.

The administrator defines SRST configurations in the SRST Reference Configuration window. Any preceding SRST configuration option can apply to a device pool. The Cisco TFTP reads the SRST configuration and provides it to the IP phone in a .cnf.xml file. The IP phone reacts appropriately to the SRST configuration.

Connection Monitor Duration

An IP phone that connects to the SRST over a Wide Area Network (WAN) reconnects itself to Cisco Unified CallManager as soon as it can establish a connection with Cisco Unified CallManager over the WAN link. However, if the WAN link is unstable, the IP phone switches back and forth between the SRST and Cisco Unified CallManager. This situation causes temporary loss of phone service (no dial tone). These reconnect attempts, known as WAN link flapping issues, continue until the IP phone successfully reconnects itself to Cisco Unified CallManager. These WAN link disruptions fit into two classifications: infrequent random outages that occur on an otherwise stable WAN and the sporadic, frequent disruptions that last a few minutes.

To resolve the WAN link flapping issues between Cisco Unified CallManager and SRST, Cisco Unified CallManager provides an enterprise parameter and a setting in the Device Pool Configuration window that is called Connection Monitor Duration. Depending upon system requirements, the administrator decides which parameter to use. The value of the parameter gets delivered to the IP phone in the XML configuration file.

- The default for the enterprise parameter specifies 120 seconds. Use the enterprise parameter to change the connection duration monitor value for all IP phones in the Cisco Unified CallManager cluster.
- Use the Device Pool Configuration window to change the connection duration monitor value for all IP phones in a specific device pool.

SRST Reference Configuration Options for SIP Phones

A remote site may have a mix of SCCP and SIP endpoints in addition to PSTN gateway access. For calls to be routed between the different protocols and the PSTN, three different features will get configured in one SRST router that will allow calls to be routed between SCCP phones, SIP phones, and the PSTN during a WAN outage. In addition, the SRST Reference Configuration window in Cisco Unified CallManager Administration provides two fields:

- SIP Network/IP Address—The SIP network/IP address applies for SIP SRST. This address notifies the SIP phone where to send SIP Register message for SIP SRST.
- SIP Port—SIP port of the SRST gateway. Default specifies 5060.

For more information, refer to the “SRST Reference Configuration Settings” section in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

For information about configuring security for the SRST reference and the SRST-enabled gateway, refer to *Cisco Unified CallManager Security Guide*.

MLPP Domain

Because the MLPP service applies to a domain, Cisco Unified CallManager only marks a precedence level to connections and resources that belong to calls from MLPP users in a given domain. The MLPP domain subscription of the originating user determines the domain of the call and its connections. Only higher precedence calls in one domain can preempt connections that calls in the same domain are using.

To define an MLPP domain, configure the following MLPP domain information:

- Domain Name—Name of the MLPP domain.
- Domain Identifier—Configure the MLPP domain identifier as a hexadecimal value of zero or greater (the default value specifies zero).

The MLPP domain identifier comprises the collection of devices and resources that are associated with an MLPP subscriber. When an MLPP subscriber (who belongs to a particular domain) places a precedence call to another MLPP subscriber (who belongs to the same domain), the MLPP service can preempt the existing call that the called MLPP subscriber is on for a higher precedence call. The MLPP service availability does not cross domains. Device pools refer to the configured MLPP domain.

**Note**

You must reset all devices for a change to this setting to take effect.

Enterprise Parameters

Enterprise parameters provide default settings that apply to all devices and services in the same cluster. When you install a new Cisco Unified CallManager, it uses the enterprise parameters to set the initial values of its device defaults.

You cannot add or delete enterprise parameters, but you can update existing enterprise parameters. Cisco Unified CallManager Administration divides enterprise parameters by categories; for example, CCMAAdmin parameters, CCMUser parameters, and CDR parameters.

You can display additional descriptions for enterprise parameters by using the question mark button on the Enterprise Parameters Configuration window.

Service Parameters

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 that displays on 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.

**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) requests that you make changes.

Dependency Records

To find specific information about system-level settings such as servers, device pools, and date/time groups, choose **Dependency Records** from the Related Links drop-down list box on the Cisco Unified CallManager Administration configuration windows for each system-level setting and click **Go**.

If the dependency records are not enabled for the system, the dependency records summary window displays a message.

**Note**

You cannot view Dependency Records from the Device Defaults and Enterprise Parameters Configuration windows.

The Cisco Unified CallManager Configuration Dependency Records window provides information about Cisco Unified CallManager groups that it accesses. The Date/Time Group Configuration Dependency Records window provides information about Device Pools that it accesses.

For more information about Dependency Records, refer to “Accessing Dependency Records” in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

System Configuration Checklist

Table 5-2 lists the general steps for configuring system-level settings.

Table 5-2 System Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Configure the server to specify the address of the server where Cisco Unified CallManager is installed.	Server Configuration, page 5-1 Server Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 2	Specify the ports and other properties for each Cisco Unified CallManager that is installed in the same cluster.	Cisco Unified CallManager Configuration, page 5-2 Cisco Unified CallManager Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 3	Configure Cisco Unified CallManager groups for redundancy.	Cisco Unified CallManager Groups, page 5-3 Redundancy, <i>Cisco Unified CallManager System Guide, Release 5.0(4)</i> Cisco Unified CallManager Group Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 4	Configure phone NTP references, so SIP phones can get the date and time from the NTP server (optional).	Phone NTP Reference Configuration for SIP Phones, page 5-4 Phone NTP Reference Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 5	Configure Date/Time groups to define time zones for the various devices that are connected to Cisco Unified CallManager.	Date/Time Groups, page 5-4 Date/Time Group Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 6	Configure regions to specify the codec that can be used for calls between devices within that region, and between that region and other regions, if needed. Tip You do not need to configure regions if you are using only the default G.711 audio codec.	Regions, page 5-5 Region Configuration, Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)
Step 7	Configure device pools to define a set of common characteristics that can be assigned to devices.	Device Pools, page 5-10 Device Pool Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>

Table 5-2 System Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 8	Configure media resource groups and media resource group lists.	Media Resource Management, <i>Cisco Unified CallManager System Guide, Release 5.0(4)</i> Media Resource Group Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 9	Configure LDAP to store authentication and authorization information about users who interface with Cisco Unified CallManager.	LDAP, page 5-12 Understanding the Directory
Step 10	Configure locations or gatekeepers for call admission control.	Locations and Regions, page 5-9 Call Admission Control, <i>Cisco Unified CallManager System Guide, Release 5.0(4)</i>
Step 11	Configure survivable remote site telephony (SRST) references to preserve rudimentary call capability.	Survivable Remote Site Telephony References, page 5-13 Survivable Remote Site Telephony Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 12	Configure the MLPP domain.	MLPP Domain, page 5-15 Multilevel Precedence and Preemption, <i>Cisco Unified CallManager Features and Services Guide, Release 5.0(4)</i>
Step 13	Update enterprise parameters, if necessary.	Enterprise Parameters, page 5-15 Enterprise Parameters Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 14	Update service parameters, if necessary. For example, configure the DRF backup and restore master agent in the Cisco Unified CallManager Administration Service Parameters Configuration window.	Service Parameters, page 5-16 Dependency Records, page 5-16 Service Parameters Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>

Where to Find More Information

Related Topics

- [Server Configuration, page 5-1](#)
- [Cisco Unified CallManager Configuration, page 5-2](#)
- [Cisco Unified CallManager Groups, page 5-3](#)
- [Date/Time Groups, page 5-4](#)
- [Regions, page 5-5](#)

- [Device Pools, page 5-10](#)
- [LDAP, page 5-12](#)
- [Call Admission Control, page 5-13](#)
- [Survivable Remote Site Telephony References, page 5-13](#)
- [MLPP Domain, page 5-15](#)
- [Enterprise Parameters, page 5-15](#)
- [Service Parameters, page 5-16](#)
- [Dependency Records, page 5-16](#)
- Redundancy, *Cisco Unified CallManager System Guide, Release 5.0(4)*

Additional Cisco Documentation

- *Cisco Unified CallManager Administration Guide*



Cisco TFTP

The Cisco TFTP service builds and serves files that are consistent with the Trivial File Transfer Protocol (TFTP). Cisco TFTP builds configuration files and serves embedded component executables, ringer files, and device configuration files.

A configuration file contains a prioritized list of Cisco Unified CallManagers for a device (SCCP and SIP phones and gateways), the TCP ports on which the device connects to those Cisco Unified CallManagers, and an executable load identifier. Configuration files for selected devices contain locale information and URLs for the phone buttons: messages, directories, services, and information. Configuration files for gateways contain all their configuration information.

You can find configuration files in a .cnf, a .cnf.xml, or an .xml format, depending on the device type and your TFTP service parameter settings. When you set the BuildCNFType service parameter to Build All, the TFTP server builds both .cnf.xml and .cnf format configuration files for all devices. When you set this service parameter to Build None, the TFTP server builds only .cnf.xml files for all devices. When this parameter is set to Build Selective, which is the default value, the TFTP server builds .cnf.xml files for all devices and, in addition, builds .cnf files only for a select list of device types that are provided in [Table 6-1](#):

Table 6-1 **Devices with Build Selective BuildCNFType**

Device Type	Device Name
MODEL_30SPP	Cisco 30 SP+
MODEL_12SPP	Cisco 12 SP+
MODEL_12SP	Cisco 12 SP
MODEL_12S	Cisco 12 S
MODEL_30VIP	Cisco 30 VIP or DPA
MODEL_IP_CONFERENCE_PHONE	Cisco 7935
MODEL_SCCP_PHONE	SCCP Phone
MODEL_VEGA	Analog Access
MODEL_UONE	Voice Mail Port

This section describes the relationship among Cisco Unified CallManager, TFTP, and Dynamic Configuration Protocol (DHCP) as well as the relationship between devices and the TFTP server. This section contains the following topics:

- [TFTP Process Overview for SCCP Devices, page 6-2](#)
- [TFTP Process Overview for Cisco SIP IP Phones, page 6-2](#)

- [Understanding How Devices Use DHCP and Cisco TFTP](#), page 6-4
- [Understanding How Devices Access the TFTP Server](#), page 6-6
- [Understanding How Devices Identify the TFTP Server](#), page 6-6
- [Configuring a Redundant or Load-Sharing TFTP Server](#), page 6-8
- [Centralized TFTP in a Multiple Cluster Environment](#), page 6-9
- [Alternate Cisco File Servers](#), page 6-8
- [Configuration Tips for Centralized TFTP](#), page 6-10
- [Customizing and Modifying Configuration Files](#), page 6-10
- [TFTP Configuration Checklist](#), page 6-11
- [Where to Find More Information](#), page 6-11

TFTP Process Overview for SCCP Devices

The TFTP server can handle simultaneous requests for configuration files. This section describes the request process.

When a device boots, it queries a DHCP server for its network configuration information. The DHCP server responds with an IP address for the device, a subnet mask, a default gateway, a Domain Name System (DNS) server address, and a TFTP server name or address. (Some devices, such as the Cisco Unified IP Phone 7960 model, support up to two TFTP servers. If the primary TFTP server is not reached, such devices attempt to reach the fallback TFTP server.)

**Note**

If DHCP is not enabled on a device, you must assign it an IP address and configure the TFTP server locally on the device.

The device requests a configuration file from the TFTP server. The TFTP server searches an internal cache, then primary and alternate paths (if specified) for the configuration file. If the TFTP server finds the configuration file, it sends it to the device. If the device receives the Cisco Unified CallManager name, it resolves the name by using DNS and opens a Cisco Unified CallManager connection. If the device does not receive an IP address or name, it uses the default server name.

If the TFTP server cannot find the configuration file, it sends a “file not found” message to the device.

Devices that are requesting a configuration file while the TFTP server is rebuilding configuration files or while processing the maximum number of requests receive a message from the TFTP server, which causes the device to request the configuration file later. The Maximum Serving Count service parameter, which can be configured, specifies 200 as the maximum number of requests.

For a more detailed description of how devices boot, see the [“Understanding How Devices Use DHCP and Cisco TFTP”](#) section on page 6-4.

TFTP Process Overview for Cisco SIP IP Phones

Unlike SCCP phones, SIP phones get all their configurations from the TFTP server. From initial startup, the SIP phone contacts the configured TFTP server (either manually configured or configured through the DHCP server) to get the configuration files; it then registers itself to its configured Cisco Unified CallManager.

When the SIP phone configuration gets changed, the Cisco Unified CallManager database notifies the TFTP server to rebuild all the configuration files or to rebuild selectively. The TFTP server retrieves information from the Cisco Unified CallManager database and converts it into the proper output format, according to the device type, and saves the output in TFTP cache. When the TFTP server gets a request, it searches either the cache or Alternate File Server locations disk to serve the requested configuration file or default files.

The TFTP support for SIP phones builds and serves different formats of SIP configuration files from the Cisco Unified CallManager database for the following Cisco Unified SIP IP Phones:

- Cisco Unified IP Phone 7970/71, 7961, 7941, 7911 (These phones share the same SIP configuration file format.)
- Cisco Unified IP Phone 7960, 7940 (These phones share the same SIP configuration file format.)
- Cisco Unified IP Phone 7905, 7912
- SIP dial plans on the preceding phone models
- Softkey templates on the preceding phone models

The TFTP server generates the following files from the Cisco Unified CallManager database for SIP phone configuration:

- Systemwide default configuration files and per-device configuration files.
- List of systemwide dial plans for Cisco Unified IP Phones 7970/71, 7960/61, 7940/41, and 7911.
- List of systemwide softkey template files.

Table 6-2 lists the configuration files that get generated based on the SIP phone type.

Table 6-2 SIP Configuration Files That the TFTP Server Generates

SIP Configuration File Type	Model 7970/71, 7961, 7941, 7911	Model 7960/40	Model 7905	Model 7912
SIP IP Phone	SEP<mac>.cnf.xml	SIP<mac>.cnf	ld<mac>	gk<mac>
Dial Plan	DR<dialplan>.xml	<dialplan>.xml	Parameter in ld<mac>	Parameter in gk<mac>
Softkey Template	SK<softkey_template>.xml	Not configurable	Not configurable	Not configurable

The system derives filenames from the MAC Address and Description fields in the Phone Configuration window of Cisco Unified CallManager Administration and the devicename field in the Cisco Unified CallManager database. The MAC address uniquely identifies the phone.

SIP Phone Configuration Sequence

The SIP phone configuration sequence performs the following steps:

1. The administrator makes a change to the SIP phone (for example, by using Phone Configuration, SIP Profile Configuration, or SIP Security Configuration in Cisco Unified CallManager Administration) and presses Save.
2. The Cisco Unified CallManager database sends a change notification to the TFTP server and to Cisco Unified CallManager. The TFTP server then rebuilds all the configuration files for the selected phone. The configuration file name and format depend on the device type and protocol (see Table 6-2).
3. The administrator presses the reset/restart button to reset/restart the phones that are affected by the changes.

4. Upon notification (automatically, by the administrator, or by the user), Cisco Unified CallManager notifies the phone to get the configuration files again.
5. The SIP phone requests the configuration files from the TFTP server, and the server sends the requested files to the phone.
6. After getting the necessary configuration files, the phone registers its configured lines with Cisco Unified CallManager.

SIP Phone Dial Plan Configuration Sequence

The SIP phone dial plan configuration sequence performs the following steps:

1. The administrator configures the SIP dial plan and associates the dial plan with the SIP phone.
2. The Cisco Unified CallManager database sends a change notification to the TFTP server, which triggers the TFTP server to build a new set of files for the SIP phone.
3. The TFTP server rebuilds the Dial Plan configuration file and/or the configuration file for the SIP phone.
4. When all the updates to the dial rules have been made to the Cisco Unified CallManager database, the administrator clicks the Reset or Restart button to apply the change to the phone.

SIP Phone Softkey Template Configuration Sequence

The SIP phone softkey template configuration sequence performs the following steps:

1. The administrator configures the SIP softkey template and associates the softkey template with the SIP phone.
2. The Cisco Unified CallManager database sends a change notification to the TFTP server, which triggers the TFTP server to build a new set of files for the SIP phone.
3. The TFTP server rebuilds the softkey template configuration file and/or the configuration file for the SIP phone.
4. When all the updates to the softkeys have been made to the Cisco Unified CallManager database, the administrator presses the Reset or Restart button to apply the change to the phone.

Interaction with Cisco Extension Mobility

When a user logs in to a device by using Cisco Extension Mobility, the Cisco Unified CallManager database notifies the TFTP server to rebuild the SEP<mac>.cnf.xml file to include the new dial plan filenames that are defined for the lines on the device profile.

Serviceability Counters

The TFTP server provides counters in Cisco Unified CallManager Serviceability for troubleshooting purposes. See the *Cisco Unified CallManager Serviceability System Guide, Release 5.0(4)* and the *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)* for more information.

Understanding How Devices Use DHCP and Cisco TFTP

Cisco telephony devices require IP addresses that are assigned manually or by using DHCP. Devices also require access to a TFTP server that contains device loads and device configuration files.

Obtaining an IP Address

If DHCP is enabled on a device, DHCP automatically assigns IP addresses to the device when you connect it to the network. The DHCP server directs the device to a TFTP server (or to a second TFTP server, if available for the device). For example, you can connect multiple Cisco Unified IP Phones anywhere on the IP network, and DHCP automatically assigns IP addresses to them and provides them with the path to the appropriate TFTP server.

If DHCP is not enabled on a device, you must assign it an IP address and configure the TFTP server locally on the device.

The default DHCP setting varies depending on the device:

- Cisco Unified IP Phones stay DHCP-enabled by default. If you are not using DHCP, you need to disable DHCP on the phone and manually assign it an IP address.
- DHCP remains always enabled for Cisco Access Analog and Cisco Access Digital Gateways.
- For Cisco Catalyst 6000 8 Port Voice T1/E1 and Services Modules, the Network Management Processor (NMP) on the Cisco Catalyst 6000 may or may not have DHCP enabled. If DHCP is not enabled, you will need to configure the IP address through the Cisco CATOS command-line interface on the Cisco Catalyst 6000.

Requesting the Configuration File

After a device obtains an IP address (through DHCP or manual assignment), it requests a configuration file from the TFTP server.

If a device has been manually added into the Cisco Unified CallManager database, the device accesses a configuration file that corresponds to its device name. If a phone is not manually configured and auto-registration is enabled, the phone requests a default configuration file from the TFTP server and starts the auto-registration procedure with Cisco Unified CallManager.

**Note**

Phones represent the only device type that can auto-register and that have default configuration files. You must manually add all other devices to the Cisco Unified CallManager database.

If a phone has an XML-compatible load, it requests a .cnf.xml format configuration file; otherwise, it requests a .cnf file.

**Note**

When you set the Build CNF Type service parameter to Build All, the TFTP server builds both .cnf.xml and .cnf format configuration files for all devices. When you set this service parameter to Build None, the TFTP server builds only .cnf.xml files for all devices. When this parameter is set to Build Selective, which is the default value, the TFTP server builds .cnf.xml files for all devices and, in addition, builds .cnf files only for a select list of devices that do not support .cnf.xml. [Table 6-1](#) provides a list of these devices.

Contacting Cisco Unified CallManager

After obtaining the configuration file from the TFTP server, a device attempts to make a TCP connection to the highest priority Cisco Unified CallManager in the list that is specified in the configuration file. If the device was manually added to the database, Cisco Unified CallManager identifies the device. If auto-registration is enabled in Cisco Unified CallManager, phones that were not manually added to the database attempt to auto-register in the Cisco Unified CallManager database.

Cisco Unified CallManager informs devices that are using .cnf format configuration files of their load ID. Devices that are using .xml format configuration files receive the load ID in the configuration file. If the device load ID differs from the load ID that is currently executing on the device, the device requests

the load that is associated with the new load ID from the TFTP server and resets itself. For more information on device loads, refer to Device Support in the *Cisco Unified CallManager System Guide, Release 5.0(4)*.

A phone gets the Ring Tones list after it performs its booting process, when the user wants to modify the Default Phone Ring setting, and when the user loads new ring tones.

Understanding How Devices Access the TFTP Server

You can enable the IP phones and gateways to discover the TFTP server IP address in one or more of the following ways, depending on the device type:

- Gateways and phones can use DHCP custom option 150.
Cisco recommends this method. With this method, you configure the TFTP server IP address as the option value.
- Gateways and phones can use DHCP option 066.
You may configure either the host name or IP address of the TFTP server as the option value.
- Gateways and phones can query CiscoCM1.
Ensure the Domain Name System (DNS) can resolve this name to the IP address of the TFTP server. Cisco does not recommend this option because it does not scale.
- You can configure phones with the IP address of the TFTP server. If DHCP is enabled on the phone, you can still configure an alternate TFTP server IP address locally on the phone that will override the TFTP address that was obtained through DHCP.
- Gateways and phones also accept the DHCP Optional Server Name (sname) parameter.
- The phone or gateway can use the value of Next-Server in the boot processes (siaddr).

Devices save the TFTP server address in nonvolatile memory. If one of the preceding methods was available at least once, but is not currently available, the device uses the address that is saved in memory.

You can configure the TFTP service on the first node or a subsequent node, but usually you should configure it on the first node. For small systems, the TFTP server can coexist with a Cisco Unified CallManager on the same server.

Understanding How Devices Identify the TFTP Server

The following sections describe how gateways and Cisco Unified IP Phones identify the TFTP server.

Gateways

When gateways receive conflicting or confusing information from the DHCP server, they have an order of precedence that they use for selecting the address of the TFTP server. The basis for the order of precedence depends on the method that is used to specify the TFTP server (method 1 in the following list has the highest precedence).

1. Catalyst 6000 gateway uses a locally configured TFTP server address. This address overrides any TFTP address that the DHCP server sends.
2. The gateway queries the DNS name CiscoCM1, and it is resolved. The gateway always tries to resolve the DNS name CiscoCM1. If this name is resolved, it overrides all information that the DHCP server sends.

You do not need to name the TFTP server CiscoCM1, but you must enter a DNS CName record to associate CiscoCM1 with the address or name of the TFTP server.

3. The gateway uses the value of Next-Server in the boot processes. The address of the TFTP server traditionally uses this DHCP configuration parameter. When BOOTP servers are configured, this field typically serves as the address of the TFTP server.

This information gets returned in the siaddr (server IP address) field of the DHCP header. Use this option, if available, because some DHCP servers will place their own IP address in this field when it is not configured.

4. The gateway uses the site-specific option 150. This option resolves the issue in which some servers do not allow the Next-Server configuration parameter. Some servers allow access to the Next-Server parameter only when IP addresses are statically assigned.
5. The gateway uses the Optional Server Name parameter. This DHCP configuration parameter designates the host name of a TFTP server. Currently, you can configure only a host name in this parameter; do not use a dotted decimal IP address.
6. The gateway uses the 066 option, which is the name of the boot server. Option 066 normally replaces the sname (server name) field when option overloading occurs. This name field can contain a host name or a dotted decimal IP address. Do not use the 066 option with the 150 option. The device prefers the IP address over the name that is given by the 066 option if they are sent together. If both a dotted decimal IP address and a 150 option are sent, order of preference depends on the order in which they appear in the option list. The device chooses the last item in the option list because option 066 and option 150 remain mutually exclusive.

Cisco Unified IP Phones

Similar to gateways, Cisco Unified IP Phones 7971, 7970, 7961, 7941, 7931, 7911, 7906, 7960, and 7940 (that are using release 8.0(4) firmware and later) also have an order of precedence that they use for selecting the address of the TFTP server when they receive conflicting or confusing information from the DHCP server. The method that is used to specify the TFTP server (method 1 in the following list has the highest precedence) provides basis for the order of precedence.

1. Cisco Unified IP Phones use a manually configured Alternate TFTP option in their Settings Menu. When Alternate TFTP option is set to Yes locally on IP phones, both TFTP Server 1 and TFTP Server 2 address values override any TFTP addresses that the DHCP server sent.
2. Cisco Unified IP Phones use the option 150 value as the TFTP server IP address when Alternate TFTP option is set to No. You can assign only dotted IP addresses as Option 150 values. A maximum of two IP addresses get used, and only the first two IP addresses that the DHCP server provides get accepted.
3. Cisco Unified IP Phones use 066 option, which could be either a name (option 66 = DNS name) or dotted-decimal IP address (option 66 = dotted-decimal IP address) of the TFTP server. Option 066 normally replaces the sname (server name) field when option overloading occurs. This name field can contain a DNS name or a dotted decimal IP address. You cannot use multiple entries as part of this option values.
4. Cisco Unified IP Phones use the value of Next-Server IP Address in the boot-up processes as its TFTP server IP address. This DHCP configuration parameter traditionally gives the address of the TFTP server. When you configure BOOTP servers, this field typically gets referred to as the address of the TFTP server. The siaddr (server IP address) field of the DHCP header returns this information.
5. Cisco Unified IP Phones use the Optional Server Name parameter sname as the TFTP server name. This DHCP configuration parameter represents the DNS name of a TFTP server. Currently you can configure only a DNS name in this parameter; do not use a dotted decimal IP address.

Cisco recommends that you use DHCP custom option 150. With this method, TFTP server dotted decimal IP address gets configured as the option 150 value. DHCP server can send multiple values or dotted decimal IP addresses as part of option 150 to the phone. Phones will only support two dotted decimal IP addresses for Option 150 values as TFTP Server 1 and TFTP Server 2 entries.

**Note**

Be aware that option 66 is defined to be a string type, option 150 is defined as an array of 32-bit dotted decimal IP address(es), and both TFTP Server 1 and TFTP Server 2 are 32 bit dotted decimal IP addresses

Configuring a Redundant or Load-Sharing TFTP Server

You must have one TFTP server that is configured in a cluster; however, you may want to configure a redundant or load-sharing TFTP server. If a device (phone or gateway) gets no response from the first TFTP server or if the server is busy and returns a Process Allocation Exceeded message (and if a redundant TFTP server is configured), the device will try to connect to the second TFTP server. Configure the second TFTP server in option 150 in the DHCP scope.

If the TFTP servers that are in the middle of rebuilding all configuration files return a Disk Full message to the requesting device, the device will not attempt to use the second TFTP server; instead, it will wait and retry the first TFTP server from which it received the Disk Full message.

Alternate Cisco File Servers

You can specify alternate Cisco file servers if you have multiple clusters, if you want to configure only one server for many DHCP scopes, or if you want to have one DHCP scope. You can specify up to 10 alternate servers by entering a value in any of the Alternate Cisco File Server fields of the Cisco TFTP service parameter. For more information on service parameters, refer to Service Parameters Configuration in the *Cisco Unified CallManager Administration Guide*.

You can use either of the following syntax examples:

- `host://<IP of the off-cluster TFTP server>` (for example, `host://10.10.134.24`)
- `HOST://<IP of the off-cluster TFTP server>` (for example, `HOST://10.10.134.24`)

If DNS is also supported, you can also use one of the following syntax examples:

- `host://<name of the off-cluster TFTP server>` (for example, `HOST://tftp-prim`)
- `HOST://<name of the off-cluster TFTP server>` (for example, `HOST://tftp-second`)

You cannot use any other syntax.

The primary TFTP server should have the Alternate Cisco File Server (1 to 10) values set for external Cisco Unified CallManager clusters. The primary TFTP server serves configuration files from these servers for phones and devices in the external clusters. To avoid creating a loop, ensure that the TFTP servers on the external clusters do not point to each other.

Centralized TFTP in a Multiple Cluster Environment

Centralized TFTP supports multiple Cisco Unified CallManager clusters within one regional, or site-specific environment, such as a large campus. Centralized TFTP allows devices (phones and gateways) to be moved, such as from one building to another, without requiring the administrator to reconfigure the device's IP settings (for example, DHCP, VLAN/DHCP).

Another example would be when several T1s terminate at the same demarcation point, but the T1s are to be distributed to several clusters, the administrator needs only to configure the T1s in the appropriate clusters and have the DHCP scope point the TFTP requests to the Master TFTP Server. The Centralized TFTP solution will provide the appropriate cluster-specific information to the individual T1s.

Centralized TFTP also supports multiple clusters that are running different operating systems. Devices that are registered and configured in any cluster can be directed to use a single TFTP server (the Master TFTP Server) that then serves cluster-specific files to those devices. The following sections describe how Centralized TFTP works in a Cisco Unified CallManager multicluster environment:

- [Master TFTP Server, page 6-9](#)
- [Sending Files to the Master TFTP Server, page 6-9](#)
- [Centralized TFTP with Secure Clusters, page 6-10](#)
- [Configuration Tips for Centralized TFTP, page 6-10](#)

Master TFTP Server

Each cluster must have at least one TFTP server. The primary function of the TFTP server is to build endpoint configuration files and to serve all files (such as configuration, security, firmware) to the endpoints.

In the Centralized TFTP environment, the Master TFTP Server represents a name that is applied to a single TFTP server, which gets designated to serve all files including security, firmware, and configuration files from the Cisco Unified CallManager clusters. Make this designation by directing all requests at the Master TFTP Server, either by hard-coding or by DHCP configuration at the endpoints.

If the Master TFTP Server does not find the requested file in its local cache, it begins a sequential search of each of the configured Alternate Cisco File Server service parameters. If the file is found in one of these off-cluster locations, the file gets sent to the Master TFTP Server via HTTP. The Master TFTP Server then serves the file to the endpoint via TFTP. If the alternate file server does not respond, the request eventually times out if the response is not received within a set time. The Master TFTP Server will then inform the endpoint.

Cisco strongly recommends that the Master TFTP Server belong to the cluster that has the most devices configured. In general, the system assumes that this configuration will provide the greatest chance for files to be found in the TFTP server cache and, therefore, will reduce the number of off-cluster searches.

Sending Files to the Master TFTP Server

When an off-cluster TFTP server receives a request from the Master TFTP Server, it searches for the file and, if found, sends the requested file back to the Master TFTP Server by using HTTP. The Master TFTP Server then uses TFTP to send the requested file to the device that originally requested the file. Should the off-cluster TFTP server not have the requested file, it will respond to the Master TFTP Server with File Not Found (HTTP Error 404). The Master TFTP Server continues the process with the next off-cluster TFTP server until either the file is located or no remaining options exist.

When the off-cluster server is busy, it sends HTTP Error 503 to the Master TFTP Server, so it should try the request again later. This message will also get sent to the endpoint device that made the original request.

Centralized TFTP with Secure Clusters

All off-cluster servers that are operating in mixed mode must add the Master TFTP Server or Master TFTP Server IP address to the off-clusters CTL file. (Without this updated CTL file, phones that register to a cluster where security is enabled and that attempt to download their config files will fail.) After the CTL file is updated, reboot the servers, so they can participate in the secure multicluster centralized TFTP network.

To update the CTL file for the TFTP servers, download the CTL Client plug-in by using **Application > Install Plugins** from Cisco Unified CallManager Administration. For more information about the CTL client and how to configure TFTP for security, refer to the *Cisco Unified CallManager Security Guide, Release 5.0(4)* and the Configuring the Cisco CTL Client chapter in the *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*.

Configuration Tips for Centralized TFTP

The following list comprises tips to remember when you are configuring a centralized TFTP environment:

- Only the master TFTP server gets configured with the Alternate Cisco File Server values.
- Ensure all off-cluster TFTP servers do not have Alternate Cisco File Server values configured. Refer to Service Parameters Configuration in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*, for information on how to configure the TFTP service.
- You can configure 1 to 10 Alternate Cisco File Servers in the Cisco TFTP Service Parameters Configuration window. If Alternate Cisco File Server 1 contains an empty parameter value, TFTP will stop searching for alternate servers. For example, if Alternate Cisco File Servers 2 through 10 are configured, and 1 is empty, and TFTP is searching for servers, it will not search Alternate Cisco File Servers 2 through 10.
- When phones are configured in a Cisco Unified CallManager other than the cluster where the master TFTP server is configured, and auto-registration is enabled, and the off-cluster Cisco Unified CallManager goes down, if the phones are configured to submit a request from the centralized TFTP server, they may inadvertently get auto-registered on the central Cisco Unified CallManager. Therefore, you should disable auto-registration if it is not already disabled or delete the inadvertently registered phone after making sure that the cluster to which it belongs is up and running.

Customizing and Modifying Configuration Files

You can add customized files (for example, ring tones, callback tones, phone backgrounds). Refer to the *Cisco Unified Communications Operating System Administration Guide, Release 5.0(4)*, for information on how to implement custom files and how to modify their corresponding system configuration files. If two TFTP servers exist in the cluster, ensure that the customized files are placed on both TFTP servers.

TFTP Configuration Checklist

Table 6-3 lists the steps that are needed to configure the Cisco TFTP service.

Table 6-3 TFTP Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Activate and start the Cisco TFTP service on the appropriate server.	<i>Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)</i>
Step 2	Configure the appropriate service parameters, including the Alternate File Location parameters, if appropriate.	Service Parameters Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 3	If you change a non-configuration file such as a load file or RingList.xml, start and stop the Cisco TFTP service. Note You must upload files to the TFTP directory from Cisco Unified Communications Platform Administration. Refer to the <i>Cisco Unified Communications Operating System Administration Guide</i> for more information.	<i>Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)</i> Service Parameters Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>

Where to Find More Information

Related Topic

- SIP Dial Rules, *Cisco Unified CallManager System Guide, Release 5.0(4)*
- Service Parameters Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- DHCP Subnet Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- DHCP Server Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- SIP Dial Rules Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- SIP Profile Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- *Cisco Unified Communications Operating System Administration Guide, Release 5.0(4)*



Understanding Route Plans

The Route Plan drop-down list on the menu bar allows you to configure Cisco Unified CallManager route plans by using route patterns, route filters, route lists, and route groups, as well as hunt pilots, hunt lists, and line groups.

This section describes the following route plan topics:

- [Automated Alternate Routing, page 7-1](#)
- [Route Plan Overview, page 7-4](#)
- [Route Groups and Route Lists, page 7-5](#)
- [Route Patterns, page 7-6](#)
- [Hunt Lists, page 7-10](#)
- [Hunt Pilots, page 7-10](#)
- [Call Coverage, page 7-11](#)
- [Closest Match Routing, page 7-12](#)
- [Static Digit Analysis, page 7-14](#)
- [Special Characters and Settings, page 7-16](#)
- [Calling and Called Party Transformations, page 7-26](#)
- [Caller Identification and Restriction, page 7-29](#)
- [External Route Plan Wizard, page 7-34](#)
- [Route Plan Report, page 7-38](#)
- [Where to Find More Information, page 7-38](#)

Automated Alternate Routing

Automated alternate routing (AAR) provides a mechanism to reroute calls through the PSTN or other network by using an alternate number. As a subset of the AAR feature, Cisco Unified CallManager automatically reroutes calls through the PSTN or other networks 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.

When a call is made from the device of one location to the device of another location, location bandwidth gets deducted from the maximum available bandwidth that is available for the call at either location. If not enough location bandwidth for the call exists at either location, instead of blocking the call,

Cisco Unified CallManager uses the table of AAR groups and the external number of the terminating directory number to supply the alternate number that is used to reroute the call through the PSTN or other network. The Cisco Unified IP Phone displays the message “Network congestion, rerouting.” (Configure this message by using Service Parameters Configuration for the Cisco CallManager service.) Cisco Unified CallManager automatically attempts to reroute the call by using the alternate number. If the reroute is successful, the caller connects to the called party.

AAR supports the following call scenarios for insufficient bandwidth:

- Call originates from a line or directory number (DN) of an IP phone within one location and terminates to a line or DN of another IP phone within another location. This scenario includes calls that terminate at the shared line with terminating IP phone devices that are resident in multiple locations and calls that terminate at the Cisco voice-mail port.
- Incoming call through a gateway device within one location terminates to a line or DN of an IP phone within another location. This scenario includes calls that terminate at the shared line with terminating IP phone devices that are resident in multiple locations and calls that terminate at the Cisco voice-mail port.

Cisco Unified CallManager automatically attempts to reroute calls, due to insufficient bandwidth, through the PSTN or other network only when the AAREnable enterprise parameter is set to true. Cisco Unified CallManager uses the device-based AAR calling search space, which is assigned to Cisco Unified IP Phone station devices and gateway devices, when it attempts to route the call to the gateway device that connects to the PSTN or other network. Cisco Unified CallManager uses the external phone number mask and the directory number of the line or DN and the Cisco voice-mail port to derive the alternate number that is used to reroute the call.

Automated Alternate Routing Example

In the following scenario, line/DN 5000 in the Richardson AAR group calls line 5001 in the San Jose AAR group. If not enough location bandwidth exists, the call attempts to reroute through the PSTN or other network. To route the call from AAR group Richardson to AAR group San Jose, Cisco Unified CallManager needs to know the access digit(s) to dial out to the PSTN or other network, the long-distance dialing requirement, if any, and the alternate number. Cisco Unified CallManager retrieves the information from the AAR dial prefix matrix table, which is indexed by the originating line AAR group value and the terminating line AAR group value. [Table 7-1](#) shows how the AAR group field is data filled in the line/DN table:

Table 7-1 **Line/DN and AAR Group Association**

Line/DN	AAR Group
5000	Richardson
5001	San Jose
5002	Dallas

Cisco Unified CallManager retrieves the prefix digits from the AAR dial prefix matrix table based on the AAR group value of the originating line/DN and gateway device and the AAR group value of the terminating line, and Cisco voice-mail port, to transform the derived alternate number. Table 7-2 shows an example of how the AAR dial prefix matrix table is data filled:

Table 7-2 AAR Dial Prefix Matrix Table Example

From AAR Group	To AAR Group	Prefix Digits
Richardson	San Jose	91
Richardson	Dallas	9
Richardson	Richardson	9
San Jose	Richardson	91
San Jose	Dallas	91
San Jose	San Jose	9
Dallas	Richardson	9
Dallas	San Jose	91
Dallas	Dallas	9

Cisco Unified CallManager prepends the prefix digits that are retrieved from the AAR dial prefix matrix table to the derived alternate number. Digit analysis uses the transformed digits, plus the AAR calling search space, to route the call to the PSTN or other network.

A much greater rate of success for automated alternate routing occurs when a gateway is located in the same location as the originating or terminating device. Therefore, a call that is outgoing to the PSTN or other network from a gateway that is located in the same location as the originating device and that is also incoming from a gateway located in the same location as the terminating device describes the best scenario. In other scenarios, the call remains subject to location bandwidth validation between the originating device and outgoing gateway, and between the terminating device and incoming gateway.

Automated Alternate Routing Enable Service Parameter

Besides configuring AAR groups, ensure that the Automated Alternate Routing Enable clusterwide service parameter is set to *True*. (The default value for this service parameter specifies *False*.)

The Clusterwide Parameters (System - CCMAutomated Alternate Routing) section of the service parameters for the Cisco CallManager service includes the parameter.

Automated Alternate Routing and Hunt Pilots

In previous Cisco Unified CallManager releases, if the voice messaging system is in a central location and the user is in a remote location, when the remote user tries to reach the voice messaging system and bandwidth is not available on the WAN link, Cisco Unified CallManager can reroute the call through the PSTN to the voice messaging system.

In the current Cisco Unified CallManager release, AAR does not automatically work with hunt pilots. Because the fully qualified directory number (DN) of the remote agent is unknown, AAR cannot initiate the reroute.

To enable AAR to work with hunt pilots, two additional fields display in the Hunt Pilot Configuration window: AAR Group and External Number Mask. For each hunt pilot, you must configure these fields in the Hunt Pilot Configuration window for AAR groups to work with hunt pilots. Refer to the “Hunt Pilot Configuration” chapter in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*, for details.

Route Plan Overview

Cisco Unified CallManager uses route plans to route internal calls within a Cisco Unified CallManager cluster, and external calls to a private network or the public switched telephone network (PSTN).

Route patterns, route filters, route lists, route groups, line groups, hunt lists, and hunt pilots provide flexibility in network design. Route patterns work in conjunction with route filters to direct calls to specific devices and to include or exclude specific digit patterns. Use route patterns to include and exclude digit patterns. Use route filters primarily to include digit patterns. Route lists control the selection order of the route groups. Route groups set the selection order of the gateway devices.

You can assign route patterns to gateways, to trunks, or to a route list that contains one or more route groups. Route groups determine the order of preference for gateway and trunk usage. Route groups allow overflows from busy or failed devices to alternate devices.

Route lists determine the order of preference for route group usage. If a route list is configured, you must configure at least one route group. One or more route lists can point to one or more route groups.

Route filters may restrict certain numbers that are otherwise allowed by a route pattern from being routed. Tags, or clauses, provide the core component of route filters. A tag applies a name to a portion of the dialed digits. For example, the North American Numbering Plan (NANP) number 972-555-1234 contains the LOCAL-AREA-CODE (972), OFFICE-CODE (555), and SUBSCRIBER (1234) tags.



Note

The NANP designates the numbering plan for the PSTN in the United States and its territories, Canada, Bermuda, and many Caribbean nations. NANP includes any number that can be dialed and is recognized in North America.

Route patterns represent all valid digit strings. Cisco Analog Access Trunk Gateways, Cisco Digital Access Trunk Gateways, Cisco MGCP gateways, H.323-compliant gateways, and trunks also use route patterns. Cisco gateways can route ranges of numbers with complex restrictions and manipulate directory numbers before the Cisco Unified CallManager passes them on to an adjacent system. The adjacent system can include a central office (CO), a private branch exchange (PBX), or a gateway on another Cisco Unified CallManager system.

Line groups consists of list of DNs. Line groups specify a distribution algorithm (such as Top Down) for the members of the line group. Line groups also specify the hunt options to use in cases where the line group members do not answer, are busy, or are not available. Beginning with Release 4.1 of Cisco Unified CallManager, a directory number may belong to more than one line group.

Hunt lists comprise ordered groupings of line groups. A line group may belong to more than one hunt list. A hunt list must specify at least one line group before the hunt list can accept calls.

Hunt pilots represent route patterns that are used for hunting. A hunt pilot can specify a partition, numbering plan, route filter, and hunt forward settings. A hunt pilot must specify a hunt list.

Route Groups and Route Lists

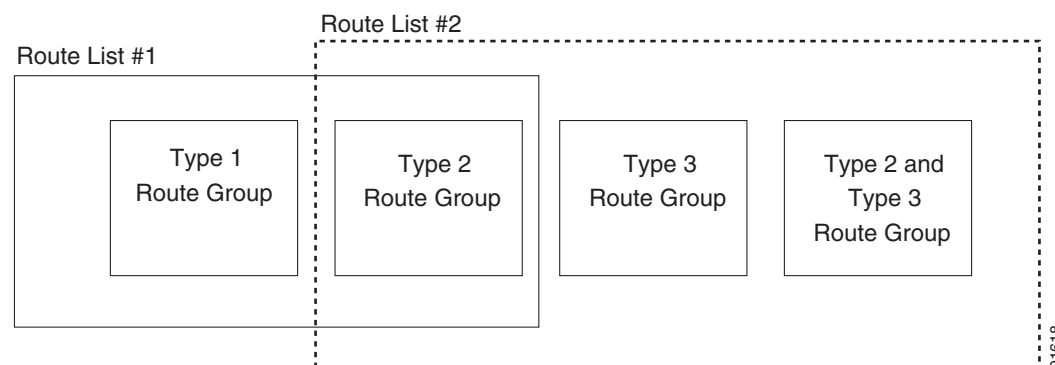
Route groups contain one or more devices, and route lists contain one or more route groups.

Cisco Unified CallManager may restrict the gateways that you can include in the same route group and the route groups that you can include in the same route list. For the purpose of route group and route list restrictions, Cisco Unified CallManager divides gateways into three types:

- Type 1—MGCP QSIG gateways and QSIG-enabled intercluster trunks
- Type 2—MGCP non-QSIG, Skinny, T1-CAS gateways; non-QSIG intercluster trunks
- Type 3—H.225 and H.323 gateways, and all other trunk types

Route lists can contain a mixture of route group types, although you cannot combine an H225 trunk with a Type 1 (QSIG) route group. Cisco Unified CallManager does not allow you to add route groups that contain gateways that use the H.323 or H.225 protocol (Type 3) and route groups that contain MGCP gateways that use a QSIG protocol (Type 1) to the same route list. You can create route lists with any combination of Type 1 route groups and Type 2 route groups as well as with any combination of Type 2 route groups and Type 3 route groups, as illustrated in [Figure 7-1](#).

Figure 7-1 Valid Route Lists Example



For more information on creating route groups, refer to the “Configuring a Route Group” section in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*. For more information on creating route lists, refer to the “Adding a Route List” section in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.



Note

As of Release 4.1 of Cisco Unified CallManager, you cannot combine route groups and line groups, and route lists and hunt lists become separate entities. Thus, route groups make up route lists, and line groups make up hunt lists. In Release 4.0 of Cisco Unified CallManager, possible components of route/hunt lists included both route groups and line groups.



Note

In Release 4.0 of Cisco Unified CallManager, possible members of route/hunt lists included both line groups and route groups. In Release 4.1 of Cisco Unified CallManager, if an existing route/hunt list includes a line group as a member, Cisco Unified CallManager migrates the route/hunt list to a hunt list.

Route Patterns

Cisco Unified CallManager uses route patterns to route or block both internal and external calls.

**Note**

Prior to Release 4.1 of Cisco Unified CallManager, configuration of route patterns and hunt pilots occurred in a single window, since Route Pattern and Hunt Pilot were integrated. Route List and Hunt list were part of the same list. A list could have a Line Group and/or Route Groups.

**Note**

Starting with Release 4.1, Route Group and Route lists are part of Route Pattern configuration. Line groups and Hunt lists are part of Hunt pilot configuration. Route Patterns and Hunt Pilots are configured separately. Route Groups or Route Lists cannot be added to Hunt Pilot and Line Groups. Hunt Lists cannot be added to Route Pattern. If an existing route pattern/hunt pilot associates with a hunt list, Cisco Unified CallManager migrates the route pattern/hunt pilot to a hunt pilot.

The simplest route pattern specifies a set of one or more digits. For example, the number 8912 specifies a route pattern.

Gateways and Cisco Unified IP Phones can also use more complex route patterns that can contain wildcards. A wildcard represents a range of numbers; for example, X represents any digit 0 through 9.

To classify a call as OnNet or OffNet, administrators can set the Call Classification field to OnNet or OffNet, respectively, on the Route Pattern Configuration window. Administrators can override the route pattern setting and use the trunk or gateway setting by checking the Allow Device Override check box on the Route Pattern Configuration window.

**Caution**

If a gateway has no route pattern that is associated with it, or it does not belong to a route group, it cannot route any calls.

You can use route patterns to invoke network-specific services/facilities on a call-by-call basis by configuring the fields in the ISDN Network-Specific Facilities Information Element section on the Route Pattern Configuration window. Cisco Unified CallManager uses the network-specific services/facilities when the user dials the route pattern.

**Note**

Cisco Unified CallManager only uses the network-specific information with PRI protocol gateways. H.323 gateways do not support network-specific facilities, but they support SDN when the dial peers are configured accordingly. Cisco Unified CallManager codes the bearer capability as Speech for the ACCUNET service.

Route Pattern Usage

You can assign a route pattern directly to a Cisco Access Gateway, or you can assign it to a route list for more flexibility. For example, [Figure 7-2](#) shows Cisco Digital Access Gateway 1 designated as the first choice for routing outgoing calls to the PSTN when a matching route pattern is dialed.

**Tip**

If a gateway does not have a route pattern, it cannot place calls to the PSTN or to a PBX. To assign a route pattern to an individual port on a gateway, you must assign a route list and a route group to that port.

Figure 7-2 shows the effects of using route patterns with Cisco Digital Gateways. This example assigns the route pattern to a route list, and that route list associates with a single route group. The route group supports a list of devices that are selected based on availability.

When the system initially presents a call to a member of a route list, Cisco Unified CallManager reroutes for all cause codes other than Out of Bandwidth, User Busy, and Unallocated Number. The value of the associated service parameters for the Cisco CallManager service determines the rerouting decision for those cause codes. The Clusterwide Parameters (Route Plan) grouping includes the Stop Routing on Out of Bandwidth Flag, Stop Routing on User Busy Flag, and Stop Routing on Unallocated Number Flag service parameters. You can set each service parameter to True or False.

After a route list locks onto a trunk, no rerouting occurs. The media connect time of the endpoints and the Stop Routing service parameters determine when a route list stops hunting for the next route group. When media negotiation begins, the route list or hunt list loses the ability to reroute.

The Stop Routing on Q.931 Disconnect Cause Code service parameter for the Cisco CallManager service determines routing behavior when a call that is being routed to a remote site through a route list gets released and a Q.931 cause code gets sent to Cisco Unified CallManager. If the cause code that is encountered in the message matches a cause code that this parameter specifies, a local Cisco Unified CallManager stops routing the call. (The call does not get sent to the next device in the route list).

**Note**

If a route pattern is associated with a gateway, and all the resources of that gateway are used, then the call does not get routed.

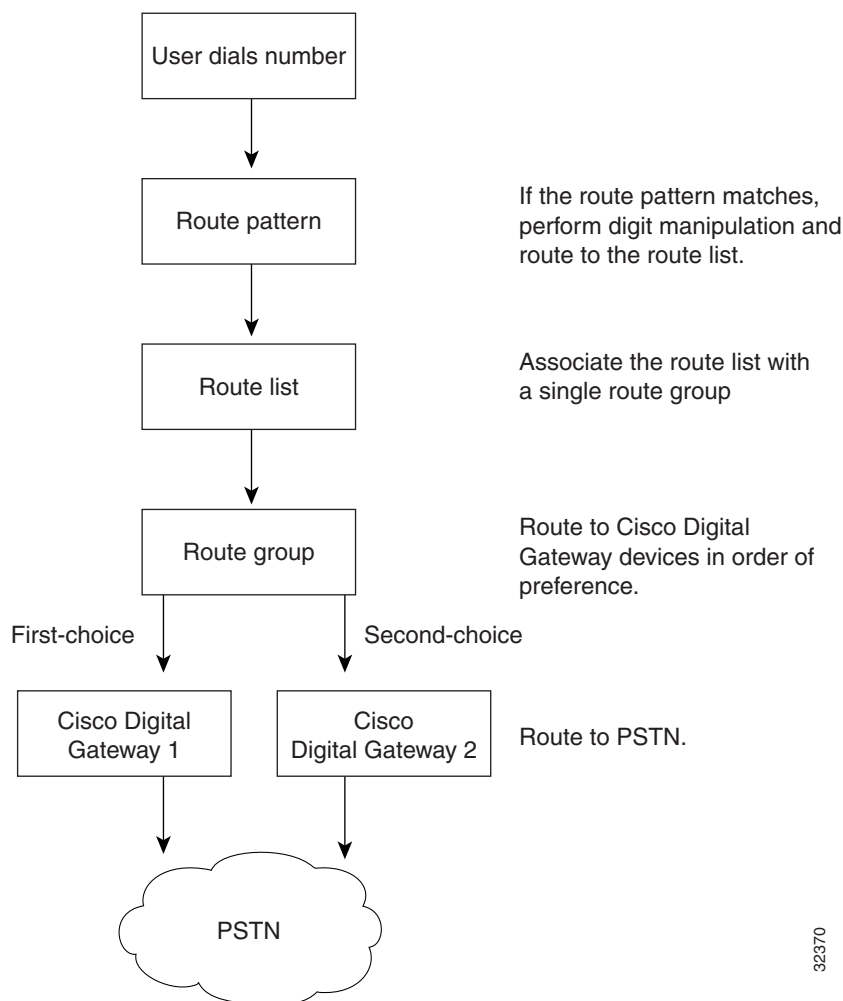
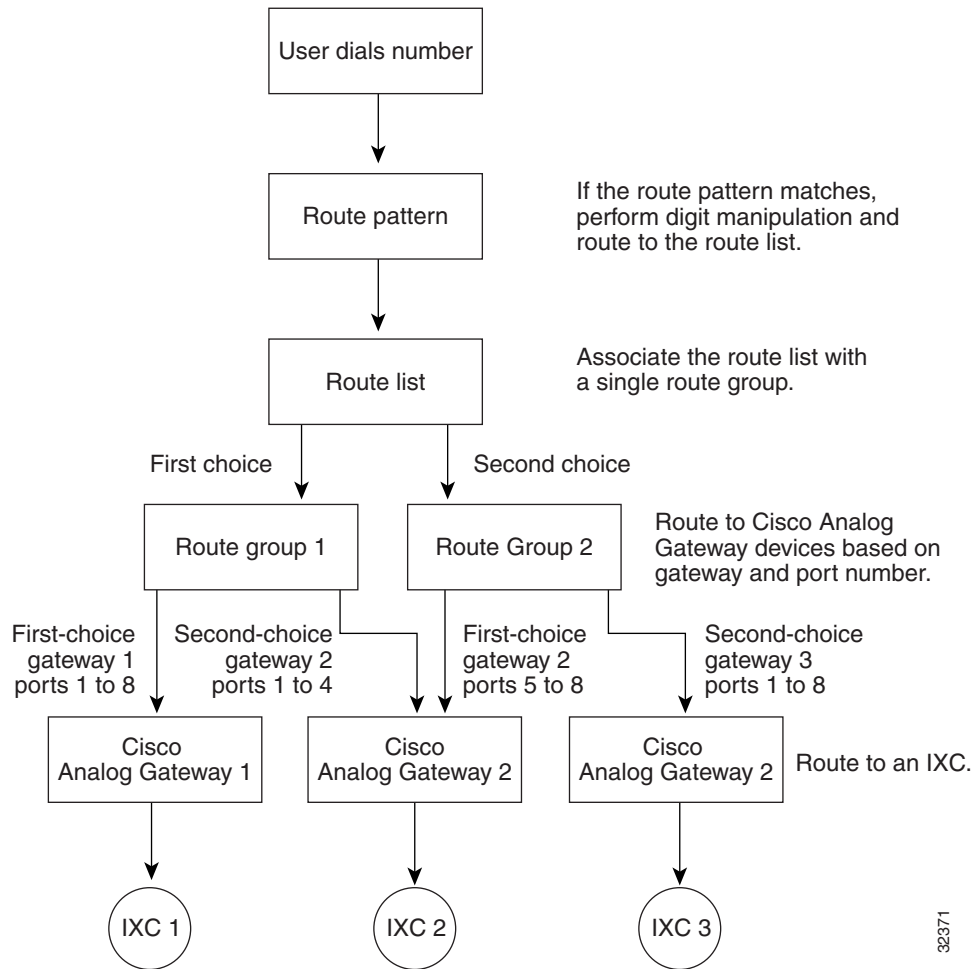
Figure 7-2 *Route Plan Summary Diagram for Cisco Digital Gateways*

Figure 7-3 shows the effects of using route patterns with Cisco Analog Gateways. This example assigns the route pattern to a route list, and that route list associates with two route groups. Route group 1 associates with ports 1 through 8 on gateway 1, which routes all calls to interexchange carrier 1 (IXC 1). Route group 1 also associates with ports 1 through 4 on gateway 2. Route group 2 associates with ports 5 through 8 on gateway 2 and all ports on gateway 3.

Each route group supports a list of devices that are chosen on the basis of availability. For route group 1, if ports 1 through 8 on the first-choice gateway are busy or out of service, calls route to ports 1 through 4 on the second-choice gateway. If all routes in route group 1 are unavailable, calls route to route group 2. For route group 2, if ports 5 through 8 on the first-choice gateway are busy or out of service, calls route to ports 1 through 8 on the second-choice gateway. If no ports on any gateway in either route group are available, the call routes to an all trunks busy tone.

Figure 7-3 Route Plan Summary Diagram for Cisco Analog Access Gateways

Line Groups

Line groups contain one or more directory numbers. A distribution algorithm, such as Top Down, Circular, Longest Idle Time, or Broadcast, associates with a line group. Line groups also have an associated Ring No Answer reversion timeout value.

The following descriptions apply to the members of a line group:

- An *idle* member designates one that is not serving any call.
- An *available* member designates one that is serving an active call but can accept a new call(s).
- A *busy* member cannot accept any calls.

For information on configuring line groups, refer to the “Line Group Configuration” section in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

**Note**

Prior to Release 4.1 of Cisco Unified CallManager, line groups could belong to route/hunt lists. Beginning with Release 4.1 of Cisco Unified CallManager, line groups belong to hunt lists, whereas route groups belong to route lists.

Beginning with Release 4.1 of Cisco Unified CallManager, a directory number may belong to more than one line group.

Hunt Lists

Hunt lists comprise ordered groupings of line groups. A line group may belong to more than one hunt list. Hunt pilots associate with hunt lists. A hunt list may associate with more than one hunt pilot.

For information on configuring hunt lists, refer to the “Hunt List Configuration” section in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

**Note**

Prior to Release 4.1 of Cisco Unified CallManager, configuration of hunt lists and route lists occurred in a single window. Starting with Release 4.1, configuration of hunt lists and route lists occurs separately.

**Note**

In Release 4.0 of Cisco Unified CallManager, both line groups and route groups represent possible members of route/hunt lists. In Release 4.1 of Cisco Unified CallManager, if an existing route/hunt list has a line group as a member, Cisco Unified CallManager migrates the route/hunt list to a hunt list.

**Note**

TOD settings comes into effect when the lines are included in a Hunt List. The settings only apply to the Hunt Pilot and not to the lines within that Hunt List.

Hunt Pilots

Hunt pilots are sets of digits. They comprise lists of route patterns that are used for hunting. A hunt pilot can specify a partition, numbering plan, route filter, and hunt forward settings. A hunt pilot must specify a hunt list.

For information on configuring hunt pilots, refer to the “Hunt Pilot Configuration” section in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

**Note**

Prior to Release 4.1 of Cisco Unified CallManager, configuration of hunt pilots and route patterns occurred in a single window. Starting with Release 4.1, configuration of hunt pilots and route patterns occurs separately.

**Note**

In Release 4.0 of Cisco Unified CallManager, both route lists and hunt lists associated with route patterns/hunt pilots. In Release 4.1 of Cisco Unified CallManager, if an existing route pattern/hunt pilot associates with a hunt list, Cisco Unified CallManager migrates the route pattern/hunt pilot to a hunt pilot.

**Note**

TOD settings comes into effect when the lines are included in a Hunt List. The settings only apply to the Hunt Pilot and not to the lines within that Hunt List.

Call Coverage

The Call Coverage feature, implemented first in Release 4.1 of Cisco Unified CallManager, comprises the following Cisco Unified CallManager capabilities:

- Forwarding provides separate configuration based on whether the call originator is an internal user or an external user. Refer to the [“Internal and External Calls” section on page 7-12](#).
- Hunting supports personal forwarding. Refer to the [“Personal Preferences” section on page 7-12](#).
- In Cisco Unified CallManager 4.0, route patterns and hunt pilots are in one feature. In Cisco Unified CallManager 4.1 and subsequent releases, they are separated in two different features.

Hunting and Call Forwarding

The concept of hunting differs from that of call forwarding. Hunting allows Cisco Unified CallManager to extend a call to one or more lists of numbers, where each such list can specify a hunting order that is chosen from a fixed set of algorithms. When a call extends to a hunt party from these lists and the party fails to answer or is busy, hunting resumes with the next hunt party. (The next hunt party varies depending on the current hunt algorithm.) Hunting thus ignores the Call Forward No Answer (CFNA), Call Forward Busy (CFB), or Call Forward All (CFA) settings for the attempted party.

Call forwarding allows detailed control as to how to extend (*divert* and *redirect* represent equivalent terms for *extend*) a call when a called party fails to answer or is busy and hunting is not taking place. For example, if the CFNA setting for a line is set to a hunt-pilot number, a call to that line that is not answered diverts to the hunt-pilot number and thus begins hunting.

Starting with Release 4.1 of Cisco Unified CallManager, Cisco Unified CallManager offers the ability to redirect a call when hunting fails (that is, when hunting terminates without any hunt party answering, due either to exhausting the list of hunt numbers or to timing out). If used, this final redirection comprises a Call Forwarding action. Therefore, the Hunt Pilot Configuration window includes Call Forwarding configuration concepts that are similar to those found on the Directory Number Configuration window.

Example of Call Hunting

Although hunting differs from forwarding, hunting often originates as a call that gets forwarded to a hunt-pilot number. The call coverage feature extends hunting to allow final forwarding after hunting either exhausts or times out.

A typical call that invokes hunting can include the following phases:

1. A call extends to the original called party.
2. The call forwards to hunting (for example, due to the Call Forward All [CFA], CFNA, or CFB setting for the original called line).

3. The call hunts through provisioned hunt groups according to provisioned algorithms for each group. Hunting either succeeds (if a hunt party answers), exhausts (if all hunt parties are attempted, but none answer), or times out (if the time specified in the Maximum Hunt Timer runs out before all parties are attempted, and none of the parties that were attempted answer).

For the purpose of this example, we assume that hunting does not succeed.

4. If some form of final forwarding is configured, the call forwards to a next destination; otherwise, the call gets released.

Maximum Hunt Timer

The Maximum Hunt Timer field on the Hunt Pilot Configuration window allows the administrator to enter a value (in seconds) to limit the time for hunting through a hunt list. After the specified time lapses, if hunting has not succeeded, the call gets forwarded to a voice-messaging system, a specific dialed number, or some personal treatment (if configured), or the call gets released.

For more details about the Maximum Hunt Timer, refer to the field description in the “Hunt Pilot Configuration” section of the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

Internal and External Calls

Forwarding provides separate configuration based on whether the originator of a call is an internal user or an external user. This distinction applies to Call Forward Busy (CFB), Call Forward No Answer (CFNA), and Call Forward No Coverage (CFNC) cases.

Personal Preferences

Hunting supports the capability to provide a final forwarding treatment to voice-messaging system, a specific dialed number, or some personal treatment (based on the original called party) when hunting either exhausts or times out. The capability to provide separate final forwarding treatment based on whether the call was internal or external also exists. Hunting supports a separate, configurable maximum hunt timer for each hunt-pilot number.

In the Hunt Pilot configuration settings, Use Personal Preferences Destination fields are available to enable the Call Forward No Coverage (CFNC) settings for the original called number that forwarded the call to the hunt pilot. Refer to the “Hunt Pilot Configuration Settings” section in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

Closest Match Routing

Closest match routing process routes a call by using the route pattern that most closely matches the dialed number. When the Cisco Unified CallManager encounters a dialed number that matches multiple route patterns, it uses closest match routing to determine which route pattern most closely matches the number and directs the call by using that route pattern.

When two configured route patterns exactly match the same number of addresses in different partitions, Cisco Unified CallManager chooses the route pattern on the basis of the order in which the partitions are listed in the calling search space. (Cisco Unified CallManager chooses the route pattern from the partition that appears first in the calling search space.)

If two configured route patterns exactly match the same number of addresses in a partition, the Cisco Unified CallManager arbitrarily chooses one. The following paragraphs explain why such exact matches signify an unusual occurrence.

Several route patterns can match a single number. For instance, the number 8912 matches all the following route patterns: 8912, 89XX, and 8XXX.

In this example, the route pattern 8912 matches exactly one address. The route pattern 89XX matches 8912 plus 99 other addresses, and the route pattern 8XXX matches 8912 plus 999 other addresses.

If the user dials 8913, the call routes differently. Using the preceding example, this address matches only the routing patterns 89XX and 8XXX. Because 89XX matches a narrower range of addresses than 8XXX, the Cisco Unified CallManager delivers the call to the device that is assigned the routing pattern 89XX.

Using the @ Wildcard Character in Route Patterns

Using the @ wildcard character in a route pattern provides a single route pattern to match all NANP numbers, and requires additional consideration.

The number 92578912 matches both of the following route patterns: 9.@ and 9.XXXXXXXX. Even though both these route patterns seem to equally match the address, the 9.@ route pattern actually provides the closest match. The @ wildcard character encompasses many different route patterns, and one of those route patterns is [2-9][02-9]XXXXXX. Because the number 2578912 more closely matches [2-9][02-9]XXXXXX than it does XXXXXXXX, the 9.@ route pattern provides the closest match for routing.

When configuring route patterns, take the following considerations into account:

- When @ is used in a routing pattern, the system recognizes octothorpe (#) automatically as an end-of-dialing character for international calls. For routing patterns that do not use @, you must include the # in the routing pattern to be able to use the # character to signal the end of dialing.
- If the route pattern contains an at symbol (@), the Discard Digits field can specify any discard digits instructions (DDIs).

The [“Special Characters and Settings” section on page 7-16](#) lists DDIs and describes the effects of applying each DDI to a dialed number.

Discard Digits Instructions

A discard digits instruction (DDI) removes a portion of the dialed digit string before passing the number on to the adjacent system. Portions of the digit string must be removed, for example, when an external access code is needed to route the call to the PSTN, but the PSTN switch does not expect that access code.



Note

With non-@ patterns, you can use only Discard Digits instructions <None>, NoDigits, and PreDot.

Static Digit Analysis

Prior to Release 4.0 of Cisco Unified CallManager, unregistered devices without configured forwarding got removed from the digit analysis (DA) table and required dynamic digit analysis. Prior to Release 4.0, when a phone unregistered, call processing allowed a call to pass to the next closest match in the Calling Search Space (CSS) list. With the introduction of static DA in Release 4.0, whether a phone is registered or not, the device remains in the DA table, and the directory number intercepts the call.

Configuration Tip

- Administrators should note that Cisco Unified CallManager Assistant does not use translation patterns for failover. Instead, administrators must set up Call Forward No Answer (CFNA) with the data that was in the translation pattern for all Unified CM Assistant failed route points, and these route points must be removed.

Beginning with Release 4.0 of Cisco Unified CallManager, the digit analysis process builds a static digit analysis engine with the patterns that are configured in the database during system initialization. This digit analysis engine reduces the propagation of patterns within a cluster of Cisco Unified CallManagers and makes Cisco Unified CallManager more scalable.

In previous releases, the individual device control process read pattern information from the database and dynamically registered the patterns to the digit analysis process to build its digit analysis engine. Each pattern had a mapping to its control process ID in the digit analysis engine. The control process ID of a pattern got changed dynamically if its associated device was reset or if a Cisco Unified CallManager server restarted. If a change to the control process ID took place, the digit analysis engine had to be changed dynamically, and its contents required propagation to other Cisco Unified CallManager servers. During call processing, the digit analysis engine returned the control process ID of a matched pattern.

Beginning with Release 4.0 of Cisco Unified CallManager, the digit analysis process reads the pattern information directly from the database to build the static digit analysis engine during Cisco Unified CallManager initialization. With the static digit analysis engine, each pattern has a mapping to its callable endpoint name, which is a NumPlanPkID of the pattern in the database, a unique identifier to a configured pattern in Cisco Unified CallManager. The static digit analysis engine no longer holds the control process ID of a pattern.

Static digit analysis integrates with the changes to the device manager to support all existing functions and features. The device manager includes a table where a NumPlanPkID shows a one-to-one mapping to the control process ID of a pattern. When processing a call, digit analysis asks the device manager to get the control process ID for a matched pattern.

Feature Description

Cisco Unified CallManager includes these pattern types: Call Park, Call Forward, Meet-Me Conference, Device, Translation, Call Pickup Group, Route, and Message Waiting. The Device, Translation, and Route pattern types represent static patterns. The digit analysis process reads these patterns directly and inserts them into the static digit analysis engine during the initialization of a Cisco Unified CallManager. Other pattern types (Call Park, Call Forward, Meet-Me Conference, Call Pickup Group, and Message Waiting), which are intercept patterns, remain dynamic patterns. Their individual control process reads the pattern information from the database and then asks the digit analysis process to insert the pattern into the static digit analysis engine via registration messages.

All static patterns remain unchanged until their records are changed in the database. Static patterns do not require propagation because the database change notification is broadcast to the servers within a cluster. Dynamic patterns still use the existing propagating and updating mechanism to update the static digit analysis engines.

Regardless of its pattern type, each static pattern in the static digit analysis engine has a mapping to its PkID in the NumPlan table in the database. When a device registers its patterns to the device manager, the same PkID gets saved and mapped to its control process ID in the device manager. A new interface between the digit analysis and device manager retrieves the control process ID when a matched pattern is found in the static digit analysis engine during call processing.

Caveat 1

A potential loss of change notification exists in the current Cisco Unified CallManager release. This loss could cause a device that is registered with Cisco Unified CallManager to become unreachable by other devices. The following paragraphs provide troubleshooting for this potential problem.

The most common cause for this problem occurs when the DN that is assigned to the device belongs to a partition that is not contained in the calling search space of other devices. If the calling search space of other devices does contain the partition for that DN, other reasons may apply. For example, the DN changed only for that device, and the change notification from the database to Cisco Unified CallManager was lost. Beginning with Release 4.0 of Cisco Unified CallManager, resetting the device may not resolve the problem.

To resolve this problem, remove the DN and add the DN to the system again. Remove the DN from its device on the Directory Number Configuration window and on the Route Plan Report window. After you remove the DN, add it back in with the same partition, pattern, and other configuration information. The process should resolve the problem after you add the new DN to Cisco Unified CallManager again.

The same workaround applies to route patterns and translation patterns if similar problems exist.



Tip

Be sure to document all configurations before removing the patterns.

Caveat 2

Static digit analysis disables the configuration of several applications. These applications rely on the provision of duplicate patterns in the same calling search space. For example, the CTI application may be pattern 5000 in partition A, and a particular phone may be pattern 5000 in partition B. In previous releases, if the CTI route point is down, the phone will ring. With static digit analysis, however, the caller receives a busy tone. This limitation implies that the application failure does not get handled.

Administrators would normally use Call Forward No Answer and Call Forward on failure to handle application failure, but when the pattern on the CTI route point is 5XXX, you cannot configure a forward destination of 5XXX. To resolve this limitation, you can now perform configuration of X characters in Call Forward destinations.

The following example demonstrates the functionality of digit analysis prior to Release 4.0 (with dynamic digit analysis) and in Release 4.0 and subsequent releases (with static digit analysis) for the Cisco Unified CallManager Assistant application.

IPMA Example with Digit Analysis Prior to Release 4.0

Given the following configuration

```
Partitions: IPMA, Managers, Everyone
CSS-I-E: IPMA:Everyone
CSS-M-E: Managers:Everyone
Line-1/CSS-I-E: Everyone/1000
Line-2/CSS-M-E: Manager/1001
CTI RP: IPMA/1XXX
Translation Pattern/CSS-M-E: Everyone/1XXX
```

If the CTI route point (RP) is up, 1000/IPMA:Everyone calls 1001. The call routes by using the CTI route point *IPMA/1XXX*.

If the CTI route point is down, 1000/IPMA:Everyone calls 1001. The call goes through the translation pattern *Everyone/1xxx*, and the call reaches Manager/1001 after the translation and achieves the goal of the IPMA application.

Cisco Unified CallManager Assistant Example with Static Digit Analysis in Release 4.0 and Subsequent Releases

Given an identical configuration, in Release 4.0 and in subsequent releases, you must make the following modification: configure *1xxx* as a CFNA mask and CSS-E as a CFNA calling search space for the CTI route point to handle the CTI route point failure case.

When static digit analysis gets used, the following processing takes place:

- If the CTI route point (RP) is up, 1000/IPMA:Everyone calls 1001. The call routes through CTI route point *IPMA/1XXX*. (Routing does not change from previous releases.)
- If the CTI route point is down, 1000/IPMA:Everyone calls 1001. The call goes to the CTI route point, and its CFNA is triggered. The forwarding feature routes the call through the translation pattern *Everyone/1xxx*, and the call reaches Manager/1001 after translation.

Without configuring the CFNA in the CTI route point, the translation pattern never gets matched, and the Cisco Unified CallManager Assistant application fails.

Special Characters and Settings

Cisco Unified CallManager Administration allows you to use special characters and settings to perform the following tasks:

- Allowing a single route pattern or hunt pilot to match a range of numbers
- Removing a portion of the dialed digit string
- Manipulating the appearance of the calling party number for outgoing calls
- Manipulating the dialed digits, or called party number, for outgoing calls

For more information on how to use special characters and settings, see the following topics:

- [Wildcards and Special Characters in Route Patterns and Hunt Pilots, page 7-16](#)
- [Discard Digits Instructions, page 7-19](#)

Wildcards and Special Characters in Route Patterns and Hunt Pilots

Wildcards and special characters in route patterns and hunt pilots allow a single route pattern or hunt pilot to match a range of numbers (addresses). Use these wildcards and special characters also to build instructions that enable the Cisco Unified CallManager to manipulate a number before sending it to an adjacent system.

[Table 7-3](#) describes the wildcards and special characters that Cisco Unified CallManager supports.

Table 7-3 Wildcards and Special Characters

[illegible]

Table 7-3 Wildcards and Special Characters (continued)

Character	Description	Examples
.	The dot (.) character, used as a delimiter, separates the Cisco Unified CallManager access code from the directory number. Use this special character, with the discard digits instructions, to strip off the Cisco Unified CallManager access code before sending the number to an adjacent system. Each route pattern can have only one dot (.) character.	The route pattern 9.@ identifies the initial 9 as the Cisco Unified CallManager access code in an NANP call.
*	The asterisk (*) character can provide an extra digit for special dialed numbers.	You can configure the route pattern *411 to provide access to the internal operator for directory assistance.
#	The octothorpe (#) character generally identifies the end of the dialing sequence. Ensure the # character is the last character in the pattern.	The route pattern 901181910555# routes or blocks an international number that is dialed from within the NANP. The # character after the last 5 identifies this digit as the last digit in the sequence.

Table 7-4 lists Cisco Unified CallManager Administration fields that require route patterns or hunt pilots and shows the valid entries for each field.

Table 7-4 Field Entries

Field	Valid entries
Call Park Number/Range	[^ 0 1 2 3 4 5 6 7 8 9 -] X * #
Calling Party Transform Mask	0 1 2 3 4 5 6 7 8 9 X A B C D * #
Called Party Transform Mask	0 1 2 3 4 5 6 7 8 9 X A B C D * #
Caller ID DN (Gateways)	0 1 2 3 4 5 6 7 8 9 X * #
Directory Number	[^ 0 1 2 3 4 5 6 7 8 9 -] + ? ! X * # +
Directory Number (Call Pickup Group)	0 1 2 3 4 5 6 7 8 9
External Phone Number Mask	0 1 2 3 4 5 6 7 8 9 X * #
Forward All	0 1 2 3 4 5 6 7 8 9 * #
Forward Busy	0 1 2 3 4 5 6 7 8 9 * #
Forward No Answer	0 1 2 3 4 5 6 7 8 9 * #
Meet-Me Conference Number	[^ 0 1 2 3 4 5 6 7 8 9 -] X * #
Prefix Digits	0 1 2 3 4 5 6 7 8 9 A B C D * #
Prefix DN (Gateways)	0 1 2 3 4 5 6 7 8 9 * #
Route Filter Tag Values	[^ 0 1 2 3 4 5 6 7 8 9 -] X * #
Route Pattern	[^ 0 1 2 3 4 5 6 7 8 9 A B C D -] + ? ! X * # + . @

Table 7-4 *Field Entries (continued)*

Field	Valid entries
Translation Pattern	[^ 0 1 2 3 4 5 6 7 8 9 A B C D -] + ? ! X * # + . @
Hunt Pilot	[^ 0 1 2 3 4 5 6 7 8 9 A B C D -] + ? ! X * # + . @

Discard Digits Instructions

A discard digits instruction (DDI) removes a portion of the dialed digit string before passing the number on to the adjacent system. A DDI must remove portions of the digit string, for example, when an external access code is needed to route the call to the PSTN, but the PSTN switch does not expect that access code.

[Table 7-5](#) lists DDIs and describes the effects of applying each DDI to a dialed number.

Table 7-5 *Discard Digits Instructions*

DDI	Effect	Example
10-10-Dialing	This DDI removes IXC access code	Route pattern: 9.@ Dialed digit string: 910102889728135000 After applying DDI: 99728135000
10-10-Dialing Trailing-#	This DDI removes - IXC access code - End-of-dialing character for international calls	Route pattern: 9.@ Dialed digit string: 9101028801181910555# After applying DDI: 901181910555
11/10D->7D	This DDI removes - Long-distance direct-dialing code - Long-distance operator-assisted dialing code - IXC access code - Area code - Local area code This DDI creates a 7-digit local number from an 11- or 10-digit dialed number.	Route pattern: 9.@ Dialed digit string: 919728135000 or 99728135000 After applying DDI: 98135000

Table 7-5 Discard Digits Instructions (continued)

DDI	Effect	Example
11/10D->7D Trailing-#	This DDI removes • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • IXC access code • Area code • Local area code • End-of-dialing character for international calls This DDI creates a 7-digit local number from an 11- or 10-digit dialed number.	Route pattern: 9.@ Dialed digit string: 919728135000 or 99728135000 After applying DDI: 98135000
11D->10D	This DDI removes • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • IXC access code	Route pattern: 9.@ Dialed digit string: 919728135000 After applying DDI: 99728135000
11D->10D Trailing-#	This DDI removes • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • End-of-dialing character for international calls • IXC access code	Route pattern: 9.@ Dialed digit string: 919728135000 After applying DDI: 99728135000
Intl TollBypass	This DDI removes • International access code • International direct-dialing code • Country code • IXC access code • International operator-assisted dialing code	Route pattern: 9.@ Dialed digit string: 901181910555 After applying DDI: 9910555
Intl TollBypass Trailing-#	This DDI removes • International access code • International direct-dialing code • Country code • IXC access code • International operator-assisted dialing code • End-of-dialing character	Route pattern: 9.@ Dialed digit string: 901181910555# After applying DDI: 9910555

Table 7-5 *Discard Digits Instructions (continued)*

DDI	Effect	Example
NoDigits	This DDI removes no digits.	Route pattern: 9.@ Dialed digit string: 919728135000 After applying DDI: 919728135000
Trailing-#	This DDI removes End-of-dialing character for international calls	Route pattern: 9.@ Dialed digit string: 901181910555# After applying DDI: 901181910555
PreAt	This DDI removes all digits prior to the NANP portion of the route pattern, including - Cisco Unified CallManager external access code - PBX external access code	Route pattern: 8.9@ Dialed digit string: 899728135000 After applying DDI: 9728135000
PreAt Trailing-#	This DDI removes all digits prior to the NANP portion of the route pattern, including - Cisco Unified CallManager external access code - PBX external access code - End-of-dialing character for international calls	Route pattern: 8.9@ Dialed digit string: 8901181910555# After applying DDI: 01181910555
PreAt 10-10-Dialing	This DDI removes all digits prior to the NANP portion of the route pattern, including - Cisco Unified CallManager external access code - PBX external access code - IXC access code	Route pattern: 8.9@ Dialed digit string: 8910102889728135000 After applying DDI: 9728135000
PreAt 10-10-Dialing Trailing-#	This DDI removes all digits prior to the NANP portion of the route pattern, including - Cisco Unified CallManager external access code - PBX external access code - IXC access code - End-of-dialing character for international calls	Route pattern: 8.9@ Dialed digit string: 89101028801181910555# After applying DDI: 01181910555

Table 7-5 Discard Digits Instructions (continued)

DDI	Effect	Example
PreAt 11/10D->7D	This DDI removes all digits prior to the NANP portion of the route pattern, including • Cisco Unified CallManager external access code • PBX external access code • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • IXC access code • Area code • Local area code This DDI creates a 7-digit local number from an 11- or 10-digit dialed number.	Route pattern: 8.9@ Dialed digit string: 8919728135000 or 899728135000 After applying DDI: 8135000
PreAt 11/10D->7D Trailing-#	This DDI removes all digits prior to the NANP portion of the route pattern, including • Cisco Unified CallManager external access code • PBX external access code • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • IXC access code • Area code • Local area code • End-of-dialing character for international calls This DDI creates a 7-digit local number from an 11- or 10-digit dialed number.	Route pattern: 8.9@ Dialed digit string: 8919728135000 or 899728135000 After applying DDI: 8135000
PreAt 11D->10D	This DDI removes all digits prior to the NANP portion of the route pattern, including • Cisco Unified CallManager external access code • PBX external access code • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • IXC access code	Route pattern: 8.9@ Dialed digit string: 8919728135000 After applying DDI: 9728135000

Table 7-5 Discard Digits Instructions (continued)

DDI	Effect	Example
PreAt 11D->10D Trailing-#	This DDI removes all digits prior to the NANP portion of the route pattern, including • Cisco Unified CallManager external access code • PBX external access code • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • IXC access code • End-of-dialing character for international calls	Route pattern: 8.9@ Dialed digit string: 8919728135000 After applying DDI: 9728135000
PreAt Intl TollBypass	This DDI removes all digits prior to the NANP portion of the route pattern, including • Cisco Unified CallManager external access code • PBX external access code • International access code • International direct-dialing code • Country code • IXC access code • International operator-assisted dialing code	Route pattern: 8.9@ Dialed digit string: 8901181910555 After applying DDI: 910555
PreAt Intl TollBypass Trailing-#	This DDI removes all digits prior to the NANP portion of the route pattern, including • Cisco Unified CallManager external access code • PBX external access code • International access code • International direct-dialing code • Country code • IXC access code • International operator-assisted dialing code • End-of-dialing character	Route pattern: 8.9@ Dialed digit string: 8901181910555# After applying DDI: 910555

Table 7-5 *Discard Digits Instructions (continued)*

DDI	Effect	Example
PreDot	This DDI removes • Cisco Unified CallManager external access code	Route pattern: 8.9@ Dialed digit string: 899728135000 After applying DDI: 99728135000
PreDot Trailing-#	This DDI removes • Cisco Unified CallManager external access code • End-of-dialing character for international calls	Route pattern: 8.9@ Dialed digit string: 8901181910555# After applying DDI: 901181910555
PreDot 10-10-Dialing	This DDI removes • Cisco Unified CallManager external access code • IXC access code	Route pattern: 8.9@ Dialed digit string: 8910102889728135000 After applying DDI: 99728135000
PreDot 10-10-Dialing Trailing-#	This DDI removes • Cisco Unified CallManager external access code • IXC access code • End-of-dialing character for international calls	Route pattern: 8.9@ Dialed digit string: 89101028801181910555# After applying DDI: 901181910555
PreDot 11/10D->7D	This DDI removes • Cisco Unified CallManager external access code • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • IXC access code • Area code • Local area code This DDI creates a 7-digit local number from an 11- or 10-digit dialed number.	Route pattern: 8.9@ Dialed digit string: 8919728135000 or 899728135000 After applying DDI: 98135000

Table 7-5 *Discard Digits Instructions (continued)*

DDI	Effect	Example
PreDot 11/10D->7D Trailing-#	This DDI removes • Cisco Unified CallManager external access code • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • IXC access code • Area code • Local area code • End-of-dialing character for international calls This DDI creates a 7-digit local number from an 11- or 10-digit dialed number.	Route pattern: 8.9@ Dialed digit string: 8919728135000 or 899728135000 After applying DDI: 98135000
PreDot 11D->10D	This DDI removes • Cisco Unified CallManager external access code • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • IXC access code	Route pattern: 8.9@ Dialed digit string: 8919728135000 After applying DDI: 99728135000
PreDot 11D->10D Trailing-#	This DDI removes • Cisco Unified CallManager external access code • Long-distance direct-dialing code • Long-distance operator-assisted dialing code • IXC access code • End-of-dialing character for international calls	Route pattern: 8.9@ Dialed digit string: 8919728135000 After applying DDI: 99728135000

Table 7-5 *Discard Digits Instructions (continued)*

DDI	Effect	Example
PreDot Intl TollBypass	This DDI removes • Cisco Unified CallManager external access code • International access code • International direct-dialing code • Country code • IXC access code • International operator-assisted dialing code	Route pattern: 8.9@ Dialed digit string: 8901181910555 After applying DDI: 9910555
PreDot Intl TollBypass Trailing-#	This DDI removes • Cisco Unified CallManager external access code • International access code • International direct-dialing code • Country code • IXC access code • International operator-assisted dialing code • End-of-dialing character	Route pattern: 8.9@ Dialed digit string: 8901181910555# After applying DDI: 9910555

Calling and Called Party Transformations

Cisco Unified CallManager Administration allows you to manipulate the calling party number and the called party number that Cisco Unified CallManager sends with each call setup message.

The following topics provide information on these settings:

- [Calling Party Number Transformations Settings, page 7-26](#)
- [Called Party Number Transformations Settings, page 7-28](#)

Calling Party Number Transformations Settings

Calling party transformations settings allow you to manipulate the appearance of the calling party number for outgoing calls. Cisco Unified CallManager uses the calling party number for calling line identification (CLID). During an outgoing call, the CLID passes to each private branch exchange (PBX), central office (CO), and interexchange carrier (IXC) as the call progresses. The called party receives the calling line identification (CLID) when the call is offered to the called party.

Configuration for calling party transformations settings that are used in route lists occurs in the individual route groups that comprise the list. The calling party transformations settings that are assigned to the route groups in a route list override any calling party transformations settings that are assigned to a route pattern that is associated with that route list.

You can set the following calling party transformation settings in the route group configuration:

- Use Calling Party's External Phone Number Mask
- Calling Party Transform Mask
- Prefix Digits (Outgoing Calls)

Table 7-6 describes the fields, options, and values that are used to specify calling party number transformations.

Table 7-6 *Calling Party Number Transformations Settings*

Field Name	Description
Use Calling Party's External Phone Number Mask	This field determines whether the full, external phone number is used for calling line identification (CLID) on outgoing calls. (Configure the external number by using the Directory Number Configuration window.) You can set the following Calling Party Transformations settings for the route group by clicking the members in the Route List Details panel of the Route List Configuration window: • Default: This setting indicates that the route group does not govern the calling party external phone number and calling party transform masks. If a calling party external phone number mask or transform mask is chosen for the route pattern, calls that are routed through this route group use those masks. • Off: This setting indicates that the calling party external phone number is not used for CLID. If no transform mask is entered for this route group, calls that are routed through this group do not get associated with a CLID. • On: This setting indicates that the calling party full, external number is used for CLID. The external phone number mask can contain up to 24 digits.
Calling Party Transform Mask	This field specifies the calling party transform mask for all calls that are routed through this route group. Valid values for this field range from 0 through 9, the wildcard character X, and the characters * and #. You can also leave this field blank. If it is blank and the preceding field is set to Off, this means that no calling party number is available for CLID. The calling party transform mask can contain up to 50 digits.
Prefix Digits (Outgoing Calls)	This field contains a prefix digit or a set of Prefix Digits (Outgoing Calls) that are appended to the calling party number on all calls that are routed through this route group. Valid values for this field range from 0 through 9, the characters * and #, and blank. Prefix Digits (Outgoing Calls) can contain up to 50 digits on route patterns or up to 24 digits on DNs.

Called Party Number Transformations Settings

Called party transformations settings allow you to manipulate the dialed digits, or called party number, for outgoing calls. Examples of manipulating called numbers include appending or removing prefix digits (outgoing calls), appending area codes to calls dialed as seven-digit numbers, appending area codes and office codes to interoffice calls dialed as four- or five-digit extensions, and suppressing carrier access codes for equal access calls.

Configuration of called party transformations settings that are used in route lists occurs in the individual route groups that comprise the list. The called party transformations settings that are assigned to the route groups in a route list override any called party transformations settings that are assigned to a route pattern or translation pattern that is associated with that route list.

You can set the following called party transformation settings in the route group, route pattern, and translation pattern configuration:

- Discard Digits
- Called Party Transform Mask
- Prefix Digits (Outgoing Calls)

[Table 7-7](#) describes the fields, options, and values that are used to specify called party number transformations.

Table 7-7 *Called Party Number Transformations Settings*

Field Name	Description
Route Group Configuration	
Discard Digits	This field contains a list of discard patterns that control the discard digit instructions. For example, in a system where users must dial 9 to make a call to the public switched telephone network (PSTN), the PreDot discard pattern causes the 9 to be stripped from the dialed digit string. See the “Closest Match Routing” section on page 7-12 for more information. Note Any setting other than the default setting of <None> overrides the setting in the route pattern. The <None> setting means “do not discard digits.”
Called Party Transform Mask	This field specifies the called party transform mask for all calls that are routed through this route group. Valid values for this field range from 0 through 9, the wildcard character X, and characters * and #. You can also leave this field blank. If this field is blank, no transformation takes place; Cisco Unified CallManager sends the dialed digits exactly as dialed. The called party transform mask can contain up to 50 digits.
Prefix Digits (Outgoing Calls)	This field contains a prefix digit or a set of Prefix Digits (Outgoing Calls) that are appended to the called party number on all calls that are routed through this route group. Valid values for this field range from 0 through 9, the characters * and #, and blank. Prefix Digits (Outgoing Calls) can contain up to 50 digits on route patterns or up to 24 digits on DNs.

Related Topics

- [Special Characters and Settings, page 7-16](#)
- [Closest Match Routing, page 7-12](#)

- [Caller Identification and Restriction, page 7-29](#)
- [Understanding Route Plans, page 7-1](#)

Caller Identification and Restriction

Cisco Unified CallManager provides the following types of caller identification information:

- Calling Line Identification (CLID)—Provides the called party with the calling party's extension or directory number on a display.
- Calling Name Identification—Provides the called party with the calling party's name on a display.
- Connected Line Identification—Provides the calling party with the connected party's phone number on a display.
- Connected Name Identification—Provides the calling party with the connected party's name on a display

Cisco CallManger provides flexible configuration options to allow and to restrict the display of the line and name information for both calling and connected parties.

For more information on how to use caller identification settings, see the following topics:

- [Calling Party Presentation and Restriction Settings, page 7-29](#)
- [Connected Party Presentation and Restriction Settings, page 7-31](#)

Calling Party Presentation and Restriction Settings

Calling party presentation information controls whether to display the phone number and name information that Cisco Unified CallManager sends with setup messages for an outgoing call.

Cisco Unified CallManager uses the following fields to provide these supplementary services:

- Calling Line ID Presentation field—Calling line identification presentation (CLIP) or calling line identification restriction (CLIR)
- Calling Name Presentation field—Calling name presentation (CNIP) or calling name restriction (CNIR)

You can use the Calling Line ID Presentation field in the Gateway Configuration window to control whether the CLID displays for all outgoing calls on the gateway. To control the CLID display on a call-by-call basis, you use the Calling line ID Presentation field in Route Pattern Configuration or Translation Pattern Configuration windows.



Note

Configure Calling Line ID Presentation and Connected Line ID Presentation, in combination with the Ignore Presentation Indicators (internal calls only) device-level parameter, to set up call display restrictions. Together, these settings allow you to selectively present or block calling and/or connected line display information for each call. For more information about the Ignore Presentation Indicators (internal calls only) field, refer to the Device Profile Configuration chapter and the Cisco Unified IP Phone Configuration chapter in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*. For more information about call display restrictions, refer to the Call Display Restrictions chapter in the *Cisco Unified CallManager Features and Services Guide, Release 5.0(4)*.

The following example describes how calling line ID presentation works. When a user makes a call, Cisco Unified CallManager checks whether the dialed number matches a translation pattern. Cisco Unified CallManager finds a match and sets the presentation indicator to the value in the translation pattern Calling Line ID Presentation field, which specifies “restricted” in this example. Next, Cisco Unified CallManager checks and finds a match on a route pattern that is configured for the dialed number. Cisco Unified CallManager checks the Calling Line ID Presentation field and finds that the value specifies “default.” The presentation indicator remains as “restricted” because the previous setting is unchanged when default is set.

The gateway Calling Line ID Presentation field gets checked last. In this example, the value specifies “allowed” and overrides the previous calling line ID presentation indicator to allow the calling party number to display on the called party phone. Therefore, the calling line ID presentation field indicator changed from “restricted” at the time that the calling party initiated the call to “allowed” by the time that Cisco Unified CallManager sends the call setup message to the endpoint device.

You can configure line and name presentation or restriction on a call-by-call basis for outgoing calls and incoming calls by using the Route Pattern Configuration or Translation Pattern Configuration pages.

For the gateway, you can only configure calling line ID presentation for outgoing calls. For incoming calls, Cisco Unified CallManager uses the Connected Line ID Presentation field for the gateway to specify whether to allow or restrict the connected party number to display on the calling party phone. Gateway settings only apply in these two situations, and these settings override all other settings. For the gateway, you can only configure calling and connected line presentation. No settings exist to control name presentation on the gateway.

The type of device control protocol that handles the call limits caller name and number information. See [Table 7-10](#) for a list of protocols with the supported caller name and number information.



Note

To control the name display for non-QSIG trunks, you must enable the Display IE Delivery field or Send Calling Name in Facility IE field in the Gateway Configuration window.

[Table 7-8](#) describes the fields, options, and values that are used to specify calling party presentations.

Table 7-8 Calling Party Presentation Settings

Field Name	Description
Calling Line ID Presentation (outgoing call)	This field determines whether the calling party phone number displays on the called party phone display screen. The Gateway Configuration, the Route Pattern Configuration, and the Translation Pattern Configuration windows use the Calling Line Presentation field. The following list gives the options for this field: • Default: If default is set, calling line ID presentation does not get modified. • Allowed: Use this setting to permit the calling party phone number to display in the called party phone display. • Restricted: Use this setting to display “Private” in the called party phone display and block the display of the calling party phone number.

Table 7-8 *Calling Party Presentation Settings (continued)*

Field Name	Description
Calling Name Presentation (outgoing call)	This field determines whether the calling party's name displays on the called party phone display. The Route Pattern Configuration and Translation Pattern Configuration windows use the Calling Name Presentation field. The following list gives the options for this field: • Default: If default is set, calling name presentation does not get modified. • Allowed: Use this setting to display the calling party name in the called party phone display. • Restricted: Use this setting in the route patterns or translation patterns configuration displays "Private" in the called party phone display. Note The gateway has no setting for calling name presentation.
Calling Line ID Presentation (incoming call)	If the incoming call goes through a translation pattern or route pattern and the calling line ID presentation setting is allowed or restricted, the calling line presentation gets modified with the translation or route pattern setting. If the call comes into the Cisco Unified CallManager system and then goes out to a PBX or the PSTN, the outgoing call rules apply as stated in the "Calling Party Presentation and Restriction Settings" section on page 7-29. Note The gateway calling line ID presentation setting controls outgoing calls only.
Calling Name Presentation (incoming call)	If the incoming call goes through a translation pattern or route pattern and the calling name presentation setting is allowed or restricted, the calling name presentation gets modified with the translation or route pattern setting. If the call comes into the Cisco Unified CallManager system and then goes out to a PBX or the PSTN, the outgoing call rules apply as stated in the "Calling Party Presentation and Restriction Settings" section on page 7-29. Note The gateway has no settings to control name information.

Connected Party Presentation and Restriction Settings

Connected party presentation information controls whether to display the phone number and name information that Cisco Unified CallManager receives with an incoming call. Cisco Unified CallManager uses the following fields to provide these supplementary services:

- Connected Line ID Presentation field—Connected line identification presentation (COLP) or connected line identification restriction (COLR)
- Connected Name Presentation field—Connected name presentation (CONP) or calling name restriction (CONR)

Connected party settings allow you to display or restrict the display of the phone number and name of the connected party on the calling party's phone. Translation Pattern Configuration and Route Pattern Configuration windows include these two settings. The calling party receives the connected name information after the call connects to Cisco Unified CallManager and the terminating phone.

The following example describes how connected line ID works. When Cisco Unified CallManager receives an incoming call, it checks whether a translation pattern is configured for the incoming number. Cisco Unified CallManager uses the value in the Connected Line ID Presentation field that specifies "restricted" for this example. Next, if a route pattern is configured for the incoming call, the value in the Connected Line ID Presentation field gets checked. In this example, the value specifies "default," so the indicator remains as "restricted," which prevents the connected party number from displaying on the calling party's phone.

For incoming calls only, the gateway Connected Line ID Presentation field value gets checked last and is set for "allowed" in this example. The gateway setting specifies whether the connected party number can display on the calling party phone. In this case, Cisco Unified CallManager sends "allowed" in the CONNECT message, so the connected line can display on the originating caller's phone display.

You can configure connected line and name presentation or restriction on a call-by-call basis for outgoing calls and incoming calls by using the Route Pattern Configuration or Translation Pattern Configuration windows.

For incoming calls on the gateway, you use the Connected Line ID Presentation field to specify whether to allow or restrict the display of the connected party number on the calling party's phone. Gateway settings only apply to line presentation settings and override all other settings.



Note

For the gateway, you can only configure calling and connected line presentation options. No settings exist for name presentation on the gateway.

Table 7-9 describes the fields, options, and values that are used to specify connected party presentations.

Table 7-9 Connected Party Presentation Settings

Field Name	Description
Connected Line ID Presentation (outgoing call)	In the Route Pattern Configuration and the Translation Pattern Configuration windows, this field determines whether the connected party number displays on the calling party phone display. The following list gives the options for this field: • Default: If default is set, connected line ID presentation does not get modified. • Allowed: Use this setting to display the connected line number that Cisco Unified CallManager received in protocol messages on the calling party phone display. • Restricted: Use this setting to block the connected party number from displaying in the calling party phone display, and "Unknown Number" displays instead. Note This setting applies to internal calls and calls on QSIG connections only.

Table 7-9 **Connected Party Presentation Settings (continued)**

Field Name	Description
Connected Name Presentation (CONP/CONR) (outgoing call)	This field determines whether the connected party name displays on the calling party phone display. The Route Pattern Configuration and Translation Pattern Configuration windows use the Connected Name Presentation field. The following list gives the options for this field: • Default: If default is set, calling name presentation does not get modified. • Allowed: Use this setting to display the connected party name that Cisco Unified CallManager received in protocol messages in the calling party phone display. • Restricted: Use this setting to block the connected party name from displaying, and display “Unknown” in the calling party phone display.
Connected Line ID Presentation (incoming call)	If the incoming call goes through a translation or route pattern and the connected line ID presentation field is set to allowed or restricted, the connected line presentation indicator gets modified with the translation or route pattern setting. Note The Connected Line ID Presentation setting on the gateway determines if the connected party number can display on the originating party’s phone. If the call comes into the Cisco Unified CallManager system and then goes out to a PBX or the PSTN, the outgoing call rules apply as stated in the “Connected Party Presentation and Restriction Settings” section on page 7-31.
Connected Name Presentation (incoming call)	If the incoming call goes through a translation or route pattern and the connected name presentation setting is set to allowed or restricted, the connected name presentation gets modified with the translation or route pattern setting. If the call comes into the Cisco Unified CallManager system and then goes out to a PBX or the PSTN, the outgoing call rules apply as stated in the “Connected Party Presentation and Restriction Settings” section on page 7-31. Note The gateway has no settings to control name information.

Caller Identification Support with Device Control Protocols in Cisco Unified CallManager

Cisco Unified CallManager provides support for caller name and number identification presentation based on the device control protocols that handle the call. Not all device protocols provide caller number and name information in the protocol messages. [Table 7-10](#) summarizes which protocols support caller identification services.

Table 7-10 *Caller Identification Information Supported by Device Control Protocols*

Device Control Protocol	Calling Line	Calling Name	Connected Line	Connected Name
IP Phones with SCCP	provides line number	provides name associated with DN	displays number when received	displays name when received
MGCP Stations (FXS)	provides line number	provides name associated with DN	not supported	displays name when received
MGCP Trunk (FXO, T1 CAS)	not supported	not supported	not supported	not supported
H.323 Trunk	calling line sent in H.225 SETUP	supported by using DISPLAY IE in H.225 messages for intercluster trunks only	supported by H.225 NOTIFY for intercluster trunks only	supported by DISPLAY IE in H.225 messages for intercluster trunks only
PRI Trunk	calling line in PRI SETUP	supported by using FACILITY IE in PRI messages	not supported	supported by using FACILITY IE in PRI messages
QSIG Trunk	calling line in QSIG SETUP	supported by using FACILITY IE in QSIG messages	supported by QSIG CONNECT	supported by using FACILITY IE in QSIG messages
SIP Trunk	calling line included in From and Remote-Party-ID headers	calling name included in From and Remote-Party-ID headers	connected line included in Remote-Party-ID header	connected name included in Remote-Party-ID header

Related Topics

- [Calling and Called Party Transformations, page 7-26](#)
- [Special Characters and Settings, page 7-16](#)
- Enhanced Call Identification Services, *Cisco Unified CallManager System Guide, Release 5.0(4)*

External Route Plan Wizard

The external route plan wizard generates a single-tenant, multilocation, partitioned route plan for the North American Numbering Plan (NANP) area by using information that the administrator provides through a series of prompts.

The route plan that the external route plan wizard generates includes the following elements:

- Route filters
- Route groups
- Route lists
- Route patterns
- Partitions
- Calling search spaces
- Calling party and calling party transformations
- Access code manipulation

The following topics describe the basic concepts that are used when you generate route plans with the external route plan wizard:

- [Generated Route Filters, page 7-35](#)
- [Generated Route Groups, page 7-36](#)
- [Generated Route Lists, page 7-36](#)
- [Generated Route Patterns, page 7-37](#)

Generated Route Filters

A generated route filter permits or restricts access through a route list by using route patterns. The external route plan wizard associates each route list with a particular route filter. It names route filters by using the TenantLocationCalltype convention and appends the suffix RF to each route filter for easy identification.

[Table 7-11](#) shows the seven types of route lists that use route filters. The table shows examples that use specific route filter names and actual access and area codes for better readability.

Table 7-11 **Route Lists and Associated Route Filters**

Route List Type	Route Filter Name and Content Examples
911 calls	Name: CiscoDallas911RF Content: 9.@ where (SERVICE == 911)
Local calls with metro (7- and 10-digit) dialing	Name: CiscoDallasLocalRF Content: 9.@ where (INTERNATIONAL-ACCESS DOES-NOT-EXIST) AND (LOCAL-AREA-CODE DOES-NOT-EXIST) AND (AREA-CODE DOES-NOT-EXIST) AND (SERVICE DOES-NOT-EXIST) OR (LOCAL-AREA-CODE == 972) OR (LOCAL-AREA-CODE == 214)
Local calls with 10-digit dialing	Name: CiscoDallasLocal10DCallRF Content: 9.@ where (LOCAL-AREA-CODE == 972) OR (LOCAL-AREA-CODE == 214)
Local calls with 7-digit dialing	Name: CiscoDallasLocal7DCallRF Content: 9.@ where (INTERNATIONAL-ACCESS DOES-NOT-EXIST) AND (AREA-CODE DOES-NOT-EXIST) AND (SERVICE DOES-NOT-EXIST)
Toll bypass calls	Name: CiscoTollByPassToDallasRF Content: 9.@ where (AREA-CODE == 972) OR (AREA-CODE == 214)
Long-distance calls	Name: CiscoDallasLongDistanceRF Content: 9.@ where (AREA-CODE EXISTS)
International calls	Name: CiscoDallasIntlRF Content: 9.@ where (INTERNATIONAL-ACCESS EXISTS)

Generated Route Groups

A generated route group sets the order of preference for gateway and port usage. The external route plan wizard assigns one gateway to each generated route group. The wizard uses all ports on the gateways. It does not support using partial resources for generated external route plans.

The external route plan wizard names route filters by using the TenantLocationGatewayTypeNumber convention for easy identification. The following list shows the gateway type abbreviations:

- AA: analog access
- DA: digital access
- HT: H.323 trunk
- MS: MGCP station
- MT: MGCP trunk

The external route plan wizard identifies route groups that are associated with multiple gateways of the same type by attaching a number suffix to all route groups. For example, if three MGCP trunk gateways exist at the Cisco Dallas location, the external route plan wizard names the associated route groups CiscoDallasMT1, CiscoDallasMT2, and CiscoDallasMT3.

If a route list includes more than one route group and more than one gateway (with one gateway for each route group), an arbitrary order designates how the external route plan wizard lists the route groups. The only order that is imposed ensures that route groups that are associated with the local gateways are listed before the route groups that are associated with remote gateways. If needed, manually change the order after the route plan is generated.

**Note**

Cisco Unified CallManager treats all gateways that belong to a location as shared resources for that location.

Generated Route Lists

A generated route list sets the order of preference for route group usage and defines the route filters that are applied to those route groups. The external route plan wizard creates between five and seven route lists for each location depending on the types of local dialing choices that are available. Therefore, the total number of route lists depends on the local dialing scheme and the number of locations that the route plan serves.

Using the TenantLocationCalltype convention, the external route plan wizard names route lists and appends the suffix RL to each route list for easy identification.

[Table 7-12](#) shows the various types of route lists. The examples shown in this table use specific route list names for better readability.

Table 7-12 **Route List Types**

Route List Type	Example Route List Name and Usage
911 calls	Name: CiscoDallas911RL Use: This route list type applies for 911 emergency calls.
Enterprise calls	Name: CiscoDallasEnterpriseRL Use: This route list type applies for route plans that include Cisco Unified CallManager to adjacent PBX calls. If the route plan does not include routing to an adjacent PBX, the wizard does not generate this route list type.
Local calls with metro dialing	Name: CiscoDallasLocalRL Use: This route list type applies for route plans that encompass both 7- and 10-digit dialing areas. This route list type generates two route lists: one for 7-digit dialing and another for 10-digit dialing. If you chose to generate a route plan that uses metro route lists, you cannot also choose 7- or 10-digit dialing route lists.
Local calls with 10-digit dialing	Name: CiscoDallasLocal10DCallRL Use: This route list type applies for route plans that use 10-digit dialing. This route list type generates one route list for 10-digit dialing. If you chose to generate a route plan that uses a 10-digit dialing route list, you cannot also choose 7-digit or metro dialing route lists.
Local calls with 7-digit dialing	Name: CiscoDallasLocal7DCallRL Use: This route list type applies for route plans that use 7-digit dialing. This route list type generates one route list for 7-digit dialing. If you chose to generate a route plan that uses a 7-digit dialing route list, you cannot also choose 10-digit or metro dialing route lists.
Toll bypass calls	Name: CiscoTollByPassToDallasRL Use: This route list type applies for intracluster calls that originate from a remote location and that get routed out the local gateway as local calls.
Long-distance calls	Name: CiscoDallasLongDistanceRL Use: This route list type applies for long-distance toll calls.
International calls	Name: CiscoDallasIntlRL Use: This route list type applies for international toll calls.

Generated Route Patterns

A generated route pattern directs calls to specific devices and either includes or excludes specific dialed-digit strings. The external route plan wizard only generates route patterns that require an access code prefix. The typical route pattern for routing a call to the PSTN includes the prefix construction 9.@. The typical route pattern for routing a call to the PBX includes the prefix construction 9.9@.

The external route plan wizard associates a route list, a route filter, and a partition with each route pattern. The route pattern provides the appropriate calling party transform mask, called party transform mask, discard digits instructions, and prefix digits for the associated route list.

The wizard bases route patterns for calls to an adjacent PBX on the access code and the range of directory numbers that are served by that PBX. For example, if the access code that is used to direct calls to the adjacent PBX is 9 and the range of directory numbers that is served by that PBX is 1000 through 1999, the external route plan wizard generates the route pattern 9.1XXX for enterprise calls.

Route Plan Report

The route plan report comprises a listing of all unassigned directory numbers (DN), call park numbers, call pickup numbers, conference numbers (Meet-Me numbers), directory numbers, route patterns, translation patterns, voice-mail ports, message-waiting indicators, and attendant console 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 choosing a route pattern, partition, route group, route list, directory number, call park number, call pickup number, conference number (Meet-Me number), or gateway.

Using the route plan report, you can get a list of unassigned directory numbers and delete those numbers from the Cisco Unified CallManager database, if required.

In addition, the route plan report allows you to save report data into a .csv file that you can import into other applications such as the Bulk Administration Tool (BAT). The .csv file contains more detailed information, including directory numbers (DN) for phones, route patterns, and translation patterns. Refer to the “Route Plan Report” section in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*, for more information.

Where to Find More Information

Related Topic

- Partitions and Calling Search Spaces, *Cisco Unified CallManager System Guide, Release 5.0(4)*

Related Cisco Documentation

- Partition Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Calling Search Space Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Route Group Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Route List Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Route Pattern Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Line Group Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Hunt List Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Hunt Pilot Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Presence, *Cisco Unified CallManager Features and Services Guide, Release 5.0(4)*
- *Cisco Unified Communications Solution Reference Network Design (SRND)*



Understanding Directory Numbers

Using the Directory Number Configuration window in Cisco Unified CallManager Administration, you can configure and modify directory numbers (lines) that are assigned to phones. Keep in mind, however, that directory numbers (DNs) do not always associate with devices (see the [“Managing Directory Numbers”](#) section on page 8-5).

This section covers the following topics:

- [Characteristics of Directory Numbers, page 8-1](#)
- [Shared Line Appearance, page 8-2](#)
- [Managing Directory Numbers, page 8-5](#)
- [Directory Number Features, page 8-5](#)
- [Making and Receiving Multiple Calls Per Directory Number, page 8-7](#)
- [Directory Number Search, page 8-8](#)
- [Dependency Records, page 8-9](#)
- [Directory Number Configuration Checklist, page 8-10](#)
- [Where to Find More Information, page 8-11](#)

Characteristics of Directory Numbers

You can configure up to 200 calls for a line on a device in a cluster, with the limiting factor being the device. As you configure the number of calls for one line, the calls that are available for another line decrease. Cisco Unified IP Phones that support the multicall display (such as a Cisco Unified IP Phone model 7960) support up to 200 calls per DN and 2 calls per DN for non-multicall display devices (such as Cisco Unified IP Phone model 7905).

The Cisco Unified IP Phone displays the following information about each line:

- Unique call identifier (from 1 to 200). This identifier remains consistent across all multicall display devices that have a shared-line appearance.
- Call select status, an icon that shows the state of the currently selected call
- Call information such as calling party or called party
- Call state icon such as connected or hold
- Duration of a call

For configuration information, refer to the “Configuring a Directory Number” section in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

User/Phone Add and Directory Numbers

The End User, Phone, DN, and LA Configuration window allows all-at-once addition of a new end user and a new phone that is associated with the new end user. You can associate a directory number (existing or new) and line appearance for the new end user by using the same window. To access the End User, Phone, DN, and LA Configuration window, choose the **User Management > User/Phone Add** menu option. See “User/Phone Add Configuration” in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)* for configuration details.



Note

The End User, Phone, DN, and LA Configuration window only allows addition of a new end user and a new phone. The window does not allow entry of existing end users or existing phones.

Shared Line Appearance

You can set up one or more lines with a shared-line appearance. A Cisco Unified CallManager system considers a directory number to be a shared line if it appears on more than one device in the same partition. For example, if directory number 9600 on phone A is in the partition called Dallas and on phone B in the partition called Texas, that directory number does not represent a shared-line appearance. (Ensure the directory number 9600 for phone A and phone B are in the same partition; for example, Dallas.)

In a shared-line appearance, for example, you can set up a shared line, so a directory number appears on line 1 of a manager phone and also on line 2 of an assistant phone. Another example of a shared line involves a single incoming 800 number that is set up to appear as line 2 on every sales representative phone in an office. You can also choose to update a directory number and have the updates apply to all devices that share the directory number.

The following information provides tips about and lists the restrictions for using shared-line appearances with Cisco Unified CallManager.

Shared Line Tips

Use the following tips when configuring shared lines:

- You create a shared-line appearance by assigning the same directory number and route partition to different devices.
- If multiple devices share a line, each device name displays in the Associated Devices pane of the directory number in the Directory Number Configuration window in Cisco Unified CallManager Administration.
- If you change the Calling Search Space or Call Forward and Pickup settings on any device that uses the shared line, the changes apply to all devices that use that shared line.
- To stop sharing a line appearance on a device, change the directory number or partition name for the line and update the directory number in the Directory Number Configuration window in Cisco Unified CallManager Administration.
- In the case of a shared-line appearance, Remove From Device removes the directory number on the current device only and does not affect other devices.

- Most devices with a shared-line appearance can make or receive new calls or resume held calls at the same time. Incoming calls display on all devices that share a line, and anyone can answer the call. Only one call remains active at a time on a device. For limitations, see the [“Shared Line Appearance” section on page 8-2](#).



Note Cisco Unified SIP IP Phones models 7905, 7912, 7940, and 7960 will not display remote-in-use calls and cannot do remote resume (cannot pick up a held line that is shared). These Cisco SIP phones do not support shared-line features such as Barge, cBarge, and Privacy.

- Call information (such as calling party or called party) displays on all devices that are sharing a line. If one of the devices turns on the Privacy feature, other devices that share the line will not see outbound calls that are made from the device that turned on privacy. All devices will still see inbound calls to the shared line.
- Devices with shared-line appearances can initiate independent transfer transactions.
- Devices with shared-line appearances can initiate independent conference transactions.
- Devices with shared-line appearance support the Call Forward Busy Trigger and the Maximum Number of Calls settings. You can configure Call Forward Busy Trigger per line appearance, but the configuration cannot exceed the maximum number call setting for that directory number.

The following example demonstrates how three Cisco Unified IP Phones with the same shared-line appearance, directory number 2000, use Call Forward Busy Trigger and Maximum Number of Calls settings. This example assumes that two calls occur. The following values configuration applies for the devices:

- Cisco Unified IP Phone 1—Configured for a maximum call value of 1 and busy trigger value of 1
- Cisco Unified IP Phone 2—Configured for a maximum call value of 1 and busy trigger value of 1
- Cisco Unified IP Phone 3—Configured a for maximum call value of 2 and busy trigger value of 2

When Cisco Unified IP Phone User 1 dials directory number 2000 for the first call, all three devices ring. The user for the Cisco Unified IP Phone 3 picks up the call, and the Cisco Unified IP Phones 1 and 2 go to remote in use. When the user for Cisco Unified IP Phone 3 puts the call on hold, user can retrieve the call from the Cisco Unified IP Phone 1 or Cisco Unified IP Phone 2. When User 2 dials directory number 2000 for the second call, only Cisco Unified IP Phone 2 and Cisco Unified IP Phone 3 ring.

The following example demonstrates how an H.323 client, MGCP POTS phone, and Cisco Unified IP Phone with the same shared line appearance, directory number 2000, can use the Call Forward Busy Trigger and the Maximum Number of Calls settings. This example assumes that two calls occur. The following values configuration applies for the devices:

- H.323 client—Configured for a maximum call value of 1 and busy trigger value of 1
- MGCP POTS Phone—Configured for a maximum call value of 1 and busy trigger value of 1
- Cisco Unified IP Phone—Configured for a maximum call value of 2 and busy trigger value of 2

When User 1 dials directory number 2000 for the first call, all three devices ring. The user for the Cisco Unified IP Phone picks up the call; when the user for Cisco Unified IP Phone puts the call on hold, the user(s) for H323 client and MGCP POTS phone cannot retrieve the call. If User 2 dials directory number 2000 for the second call, all three devices (IP phone, MCGP POTS phone, H.323 client) ring, and all three users can answer the call.

For information on the Maximum Number of Calls setting, refer to the “Directory Number Configuration Settings” section in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

The check box, Update Directory Number of All Devices Sharing this Line, in the Directory Number Configuration window, determines whether a shared directory number gets updated to all devices that share the number. See the [“Update Directory Number of All Devices That Share This Line” section on page 8-5](#) for more information.

A shared-line phone should not be able to interact with the call that it rejects, due to the limitation of the maximum number of calls per DN or for other reasons. For example, A and A¹ share the same DN. A¹ and A have the maximum number of calls set to 1 and 2, respectively. When C and D call the share line DN, A¹ answers these two calls. A can only interact with the first call, as it rejects the second call due to its own maximum number of calls per DN limitation. For this reason, Cisco recommends that the same value be configured for the maximum number of calls for all shared-line MCID devices. For N number of devices that share the same line, ensure both Maximum Calls setting and Busy Trigger setting are set to N. This allows each shared-line user to receive at least one call.

The shared-line phone should not interact with the call that it does not receive (because the Line Control does not maintain call information). So, a newly registered device will not recognize any existing calls on that line. The newly registered device cannot resume any held call if the call started before this device was registered with the Line Control. For example, A and A¹ share the same line, A is powered down (or logged out for the extension mobility user), and A receives an active call. After phone A is on and it registers with Cisco Unified CallManager, A should not see the existing active call in this line.

If shared-line phone calls should interact with each other, Cisco recommends that you set the maximum number of calls for all shared-lines MCID devices to 2*N, where N specifies the number of shared-line devices.

Shared Line Restrictions

The following restrictions apply to shared lines:

- Do not use shared lines for Cisco Unified CallManager Attendant Console pilot points or hunt group members. The phone that acts as the attendant console supports shared lines.
- Do not use shared-line appearances on any Cisco Unified IP Phone that requires autoanswer capability and do not turn on auto answer for a shared-line appearance.
- Do not configure shared-line appearances on the primary lines of the phones; for example, if two phones have a shared-line appearance, only one of the phones should have the primary line configured as shared (the other phone should have the secondary line configured as shared).
- Barge and Privacy work with shared lines only.
- Cisco recommends that you do not configure shared lines for Cisco Unified IP Phones, H.323 clients, and MGCP POTS phones; likewise, Cisco recommends that you do not configure shared lines for H.323 clients and MGCP POTS phones. If you configure the same shared-line appearance for a H.323 client, a MGCP POTS phone, for example, NetMeeting, and a Cisco Unified IP Phone, you cannot use the hold/resume feature on the H.323 client or MGCP POTS phone.
- Cisco recommends that you do not configure shared lines for Cisco SIP IP Phone models 7905, 7912, 7940, and 7960 because these phones cannot pick up held calls on shared lines nor can they use the shared-line features Barge, cBarge, and Privacy.

Managing Directory Numbers

Directory numbers associate with devices such as phones, route points, CTI ports, and H.323 clients. Administrators manage directory numbers from the Directory Number Configuration and Route Plan Report windows in Cisco Unified CallManager Administration. Use the Directory Number Configuration window or the Phone Configuration window to add, update, and remove directory numbers from a device, route point, or port. Use the Route Plan Report window to delete or update unassigned directory numbers from Cisco Unified CallManager database.

**Note**

Do not associate a directory number with a CTI route point or CTI port if the directory number is a member of a line group.

The Directory Number Configuration window contains two check boxes: Active and Update Directory Number of All Device Sharing this Line.

Active Check Box

The Active check box, which only displays for unassigned directory numbers, determines whether the directory number gets loaded and used by Cisco Unified CallManager. By checking the check box, the directory number gets loaded and used by Cisco Unified CallManager. For example, the directory number belonged to an employee who left the company. The directory number had certain settings that were configured, such as call forwarding to voice-messaging system. By leaving the directory number active, a call that is intended for the directory number will get forwarded. This eliminates the need to reconfigure another employee to have the same call-forwarding options. If the check box is not checked, the directory number will not get loaded by Cisco Unified CallManager, which results in settings that are configured for that DN to not be used (for example, call forward destinations), and callers will not get their call forwarded properly.

Update Directory Number of All Devices That Share This Line

This check box determines whether a shared directory number gets updated to all devices that share the number. When the check box is checked, all devices that share the directory number will receive the directory number change. If the check box remains unchecked, only the current device that displays in the window gets the directory number changed, and all other devices that share the directory number remain unchanged.

**Note**

This check box only applies to the actual directory number and partition. It does not apply to the other device settings such as voice-messaging profile, call-forwarding options, or MLPP. If any of these settings are changed for a shared line, all devices get changed.

For directory number configuration and update information, refer to the “Directory Number Configuration Overview” section in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*. For information about deleting and updating unassigned directory numbers, refer to “Deleting Unassigned Directory Numbers” and “Updating Unassigned Directory Numbers” in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

Directory Number Features

Cisco Unified CallManager enables you to configure the following features for directory numbers: call waiting and call forward.

For information about features that relate to phones, see the [“Phone Features” section on page 11-21](#). The following features get configured for phones: barge, privacy release, call back, call park, call pickup, immediate divert, malicious call identification, quality report tool, service URL, and speed dial and abbreviated dial

Call Forward

Call forward allows a user to configure a Cisco Unified IP Phone, so all calls that are destined for it ring another phone. The following types of call forward exist:

- Call forward all—Forwards all calls.
- Call forward busy—Forwards calls only when the line is in use and busy trigger setting is reached.
- Call forward no answer—Forwards calls when the phone is not answered after the configured no answer ring duration, or if the destination is unregistered.
- Call forward no coverage—Forwards calls when call either exhausts or times out, and the associated hunt-pilot for coverage specifies Use Personal Preferences for its final forwarding.

You can configure each call forward type for internal and external calls that can be forwarded to voice-messaging system, dialed destination number, or calling search space.

Cisco Unified CallManager, release 5.0, supports a secondary Calling Search Space (CSS) for Call Forward All (CFA) field. The secondary CSS for CFA combines with the existing CSS for CFA to allow the support of the alternate CSS system configuration. When CFA is activated, only the primary and secondary CSS for CFA get used to validate the CFA destination and redirect the call to the CFA destination. If these fields are empty, the null CSS gets used. The combination of the line CSS and device CSS no longer gets used when the CSS for CFA is None. Only the CSS fields that are configured in the primary CSS for CFA and secondary CSS for CFA fields get used. If CFA is activated from the phone, the CFA destination gets validated by using the CSS for CFA and the secondary CSS for CFA, and the CFA destination gets written to the database. When the CFA is activated, the CFA destination always gets validated against the CSS for CFA and the secondary CSS for CFA.

The administrator can configure call-forward information display options to the original dialed number or the redirected dialed number or both. The administrator can enable or disable the calling line ID (CLID) and calling name ID (CNID). The display option gets configured for each line appearance.

The call forward busy trigger gets configured for each line appearance in a cluster and cannot exceed the maximum number of calls that are configured for a line appearance. The call forward busy trigger determines how many active calls exist on a line before the call forward busy setting gets activated (for example, 10 calls).

The call forward no answer ring duration gets configured for each line appearance in a cluster, and the default specifies 12 seconds. The call forward no answer ring duration determines how long a phone rings before the call forward no answer setting gets activated.



Tip

Keep the busy trigger slightly lower than the maximum number of calls, so users can make outgoing calls and perform transfers.

Configure call forward in the Directory Number Configuration window in Cisco Unified CallManager Administration.

Cisco Unified CallManager provides a service parameter (CFA Destination Override) that allows the administrator to override Call Forward All (CFA) when the target of the CFA calls the initiator of the CFA, so the CFA target can reach the initiator for important calls. In other words, when the user to whom

calls are being forwarded (the target) calls the user whose calls are being forwarded (the initiator), the phone of the initiator rings instead of call forwarding back to the target. The override works whether the CFA target phone number is internal or external.

When the CFA Destination Override service parameter is set to False (the default value), no override occurs. Ensure the service parameter is set to True for CFA override to work. See Service Parameters Configuration in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*, for information about configuring service parameters.

**Note**

CFA override only takes place if the CFA destination matches the calling party and the CFA Destination Override service parameter is set to True. If the service parameter is set to True and the calling party does not match the CFA destination, CFA override does not take place, and the CFA remains in effect.

Call Waiting

Call waiting lets users receive a second incoming call on the same line without disconnecting the first call. When the second call arrives, the user receives a brief call-waiting indicator tone, which is configured with the Ring Setting (Phone Active) in the Directory Number Configuration window.

Configure call waiting in the Directory Number Configuration window in Cisco Unified CallManager Administration by setting the busy trigger (greater than 2) and maximum number of calls.

**Tip**

To configure call waiting for phones with no display (such as the Cisco IP Phone model 30 VIP), set the busy trigger to 2 and the maximum number of calls to 2.

Making and Receiving Multiple Calls Per Directory Number

Cisco Unified CallManager supports various behaviors when users make and receive multiple calls per DN: Transfer/Direct Transfer and Conference/Join.

Transfer allows different line appearances in one device to initiate independent transfer transactions and allows multiple transfer transactions per line appearance per device.

Conference allows different line appearances in one device to initiate independent conference transactions and allows multiple conference transactions per line appearance per device.

**Note**

Devices that do not support multicall display, such as Cisco Unified IP Phone model 7910, cannot transfer or conference two existing calls together.

Transfer and Conference Behavior

If only one active call exists on the directory number, the first invocation of a feature results in putting the active call on hold and initiating a new call by using the same directory number. When the new call gets set up, the second invocation of the same feature starts the feature operation. The first invocation of Transfer/Conference will always initiate a new call by using the same directory number, after putting the active call on hold.

Direct Transfer and Join Behavior

The following information describes Direct Transfer and Join behavior:

- Direct Transfer joins two established calls (call is in hold or in connected state) into one call and drops the feature initiator from the call. Direct Transfer does not initiate a consultation call and does not put the active call on hold.
- Join does not create a consultation call and does not put the active call on hold. To implement Join, choose at least two calls and then press the Join softkey on one of the calls. Join can include more than two calls, which results in a call with three or more parties. Join supports up to 16 participants in a call. To choose an active or held call, highlight the call and press the Select softkey. A checked indicator displays next to a selected call on the phone.

The call that initiates the Join automatically gets included, even if it is not selected. The active call gets included even if not selected. If all the calls in the join represent a basic call, the call that initiated the join represents the primary call. If any call in the join is a conference call (that is, it was in a conference before being joined), that call represents the primary call.

The selected status of the final call after the join depends on the selected status of the primary call before the join. If the primary call was selected, the final call remains selected after the join. This means that if that call is put on hold, shared lines would not be able to retrieve the call because the call is still selected. If the primary call was not selected, the final call remains unselected after the call.

**Note**

If more than one call in the join is a conference call, the join will fail (join supports only one conference call).

Directory Number Search

The following sections describe how to modify your search to locate a directory number. If you have thousands of directory numbers in your network, you may need to limit your search to find the directory number that you want. If you cannot locate a directory number, you may need to expand your search to include more directory numbers.

**Note**

Be aware that the directory number search is not case sensitive.

Searching by Directory Number

To search for a phone by its directory number (DN), choose Directory Number and either enter a search criteria (such as begins with or ends with) or click the **Find** button.

**Note**

Some directory numbers do not associate with phones. To search for those directory numbers, which are called unassigned DN, use the Route Plan Report window.

Searching by Route Partition

To search for a phone by its route partition, choose Route Partition and either enter a search criteria (such as begins with or ends with) or click the **Find** button.

Searching by Description

To search for a phone by its description, choose Description and either enter a search criteria (such as begins with or ends with) or click the **Find** button.

Search Within Results

To refine your search results, you can search for additional information. For example, if you search for directory numbers by directory number, you may want to search within the directory number results for DNs that share the same route partition. After you perform an initial search, check the Search Within Results check box. You can enter additional, or different, search criteria in the drop-down list boxes. Click **Find** again to search within the previous results.

Finding All Directory Numbers in the Database

To find all directory numbers that are registered in the database, choose Directory Number from the list of fields; choose “is not empty” from the list of patterns; then, click the **Find** button.

Dependency Records

If you need to find the directory numbers that a specific phone is using or the phones to which a directory number is assigned, choose Dependency Records from the Related Links drop-down list box on the Cisco Unified CallManager Administration Phone Configuration or Directory Number Configuration window. The Dependency Records Summary window displays information about directory numbers that are using the phone. To find more information about the directory number, click the directory number, and the Dependency Records Details window displays. 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 and the “Removing a Directory Number from a Phone” section in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

Directory Number Configuration Checklist

Table 8-1 provides steps to manually configure a directory number in Cisco Unified CallManager Administration. If you are using autoregistration, Cisco Unified CallManager adds the phone and automatically assigns the directory number.

Table 8-1 **Directory Number Configuration Checklist**

Configuration Steps		Procedures and Related Topics
Step 1	If you want to configure a DN for a phone, add and configure the phone. You may need the following information about the phone: • Model • 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	Configuring Cisco Unified IP Phones, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 2	Add and configure lines (DNs). Configure DNs either from the Directory Number Configuration window or, if you want to configure a DN for a phone, from the Phone Configuration window. You can also configure phone features such as call park, call forward, and call pickup.	Configuring a Directory Number, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> Configuring Cisco Unified IP Phones, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 3	Configure speed-dial buttons. You can 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 can change the speed-dial settings on their phones by using Cisco IP Phone User Options.	Configuring Speed-Dial Buttons, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 4	Configure Cisco Unified IP Phone services. You can configure services for Cisco Unified IP Phone models 7970, 7960, 7940, 7912, and 7905 and Cisco IP Communicator if you want to provide services for users or if you are configuring phones that do not have a specific user who is assigned to them. Users can change the services on their phones by using the Cisco IP Phone User Options.	Configuring Cisco Unified IP Phones, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>

Table 8-1 Directory Number Configuration Checklist (continued)

Configuration Steps	Procedures and Related Topics
Step 5 Customize phone button templates and softkey templates, if required. Configure templates for each phone.	Configuring Phone Button Templates, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> Configuring Cisco Unified IP Phones, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> Adding Nonstandard Softkey Templates, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 6 Assign services to phone buttons, if required.	Adding a Cisco Unified IP Phone Service to a Phone Button, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 7 Provide power, install, verify network connectivity, and configure network settings for the Cisco Unified IP Phone.	<i>Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager, Release 5.0</i>
Step 8 Associate a user with the phone (if required).	Associating Devices to an End User, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>

Where to Find More Information

Related Topics

- [Cisco Unified IP Phones, page 11-1](#)
- Voice Mail Connectivity to Cisco Unified CallManager, *Cisco Unified CallManager System Guide, Release 5.0(4)*
- Call Pickup Group, *Cisco Unified CallManager System Guide, Release 5.0(4)*
- Directory Number Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Enabling Autoregistration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Configuring Cisco Unified IP Phones, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Associating Devices to an End User, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- User/Phone Add Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Phone Button Template Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Service Parameters Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Barge and Privacy, *Cisco Unified CallManager Features and Services Guide, Release 5.0(4)*
- Call Park, *Cisco Unified CallManager Features and Services Guide, Release 5.0(4)*

- Immediate Divert, *Cisco Unified CallManager Features and Services Guide, Release 5.0(4)*
- Quality Report Tool, *Cisco Unified CallManager Features and Services Guide, Release 5.0(4)*

Additional Cisco Unified CallManager Documentation

- Phone administration documentation that supports your phone model and this version of Cisco Unified CallManager
- Cisco Unified IP Phone user documentation, including Getting Started documents
- Firmware release notes for your phone model
- *Cisco Unified CallManager Bulk Administration Guide*
- *Cisco Unified CallManager Security Guide*
- *Cisco Unified CallManager Assistant User Guide*
- *Cisco IP Communicator Administration Guide*



Understanding the Directory

Directories comprise specialized databases that are optimized for a high number of reads and searches and occasional writes and updates. Directories typically store data that does not change often, such as employee information, user privileges on the corporate network, and so on.

Because directories are extensible, you can modify and extend the type of information that is stored in them. The term directory schema refers to the type of stored information and the rules that it obeys. Many directories provide methods for extending the directory schema to accommodate information types that different applications define. This capability enables enterprises to use the directory as a central repository for user information.

The Lightweight Directory Access Protocol (LDAP) provides applications with a standard method for accessing and potentially modifying the information that is stored in the directory. This capability enables companies to centralize all user information in a single repository that is available to several applications with a reduction in maintenance costs through the ease of adds, moves, and changes.

This chapter covers the main principles for synchronizing Cisco Unified CallManager with a corporate LDAP directory. The chapter also discusses the administrator choice not to synchronize with a corporate LDAP directory and the consequences of that choice of configuration. The chapter also summarizes considerations for providing Cisco Unified Communications endpoints, such as Cisco Unified IP Phones and Cisco IP SoftPhone, with access to a corporate LDAP directory.

The following list summarizes the changes in directory functionality from previous releases of Cisco Unified CallManager:

- Decoupling the directory component from Cisco Unified CallManager ensures high Cisco Unified CallManager availability independent of the corporate directory.
- Cisco Unified CallManager and related applications store all application data in the local database instead of in an embedded directory. The embedded directory gets removed, and Cisco Unified CallManager supports synchronization with the customer directory.

This chapter includes the following topics:

- [Cisco Unified CallManager and the Corporate LDAP Directory, page 9-2](#)
- [Directory Access, page 9-3](#)
- [DirSync Service, page 9-3](#)
- [Data Migration Assistant, page 9-4](#)
- [Authentication, page 9-4](#)
- [Using the Cisco Unified CallManager Database Versus the Corporate LDAP Directory, page 9-5](#)
- [Directory Access for Cisco Unified Communications Endpoints, page 9-5](#)

- [LDAP Directory Configuration Checklist, page 9-6](#)
- [Where to Find More Information, page 9-7](#)

The considerations that this chapter presents apply to Cisco Unified CallManager as well as the following applications that are bundled with it: Cisco Extension Mobility, Cisco WebDialer, Bulk Administration Tool, and Real-Time Monitoring Tool.

For all other Cisco voice applications, refer to the respective product documentation that is available at <http://www.cisco.com>

In particular, for Cisco Unity, refer to the *Cisco Unity Design Guide* and to the following white papers: *Cisco Unity Data and the Directory*, *Active Directory Capacity Planning*, and *Cisco Unity Data Architecture and How Cisco Unity Works*.

Cisco Unified CallManager and the Corporate LDAP Directory

Administrators access directory information about end users from the Cisco Unified CallManager Administration End User Configuration window (**User Management > End User**). Administrators use this window to add, update, and delete user information such as user ID, password, and device association, but only if synchronization from the LDAP Server is not enabled (that is, if the Enable Synchronizing from LDAP Server check box is not checked in the Cisco Unified CallManager Administration LDAP System window).

Applications and Services That Use the Database

The following Cisco Unified CallManager applications and services use the database for user and other types of information:

- Bulk Administration Tool (BAT)
- Tool for Auto-Registered Phone Support (TAPS)
- AXL
- Cisco Extension Mobility
- Cisco Unified CallManager User Options
- Cisco Conference Connection
- CTIManager
- CDR Analysis and Reporting (CAR)
- Cisco Unified CallManager Assistant
- Cisco Customer Response Solutions (CRS)
- Cisco Emergency Responder (CER)
- Cisco Unified IP Phone Services
- Personal Address Book (PAB)
- FastDials
- Cisco WebDialer
- Cisco IP Communicator
- Cisco Unified CallManager Attendant Console

Directory Access

The following definition applies throughout this chapter:

- Directory access refers to the ability of Cisco IP Telephony endpoints, such as Cisco Unified IP Phones and Cisco Unified IP SoftPhone, to access a corporate LDAP directory.

Figure 9-1 **Directory Access for Cisco Unified Communications Endpoints**

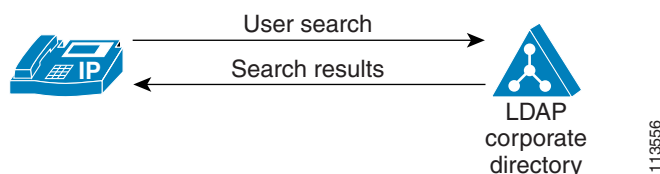


Figure 9-1 illustrates directory access as it is defined in this chapter. In this example, a Cisco Unified IP Phone gets access. The client application performs a user search against an LDAP directory, such as the corporate directory of an enterprise, and receives several matching entries. The Cisco Unified IP Phone user can then select one entry and use it to dial the corresponding person from the Cisco Unified IP Phone.



Note

Directory access, as defined here, involves only read operations on the directory and does not require that the administrator make any directory schema extensions or other configuration changes.

DirSync Service

The DirSync application performs the synchronization of data in the Cisco Unified CallManager database with the customer LDAP directory information. Cisco Unified CallManager administrators set up the DirSync service by first configuring the LDAP-directory-related Cisco Unified CallManager windows. The following windows apply:

- LDAP System (**System > LDAP System**)
- LDAP Directory (**System > LDAP Directory**)

DirSync allows Cisco Unified CallManager to synchronize the data from corporate directories to Cisco Unified CallManager. DirSync allows synchronization from Microsoft Windows Server 2000 and Windows Server 2003 Active Directory (AD), Netscape/iPlanet Directory, Sun ONE Directory Server 5.1, and Sun Java System Directory Server 5.2 to the Cisco Unified CallManager database.



Note

A DirSync that is invoked for Microsoft Active Directory performs a complete (total) synchronization of data. A DirSync that is invoked for Netscape Directory performs an incremental synchronization.

DirSync allows the following options:

- Automatic synchronization, which synchronizes the data at regular intervals
- Manual synchronization, which allows forcing the synchronization
- Stop synchronization, which stops the current synchronization. If synchronization is in progress, check for agreement.

**Note**

When directory synchronization is enabled, Cisco Unified CallManager Administration cannot update any user information that is synchronized from the customer Corporate Directory.

DirSync Service Parameters

You can configure service parameters for the DirSync service. Use the **System > Service Parameters** menu option in Cisco Unified CallManager Administration. On the window that displays, choose a server in the Server drop-down list box. Choose the Cisco DirSync service in the Service drop-down list box. The Service Parameter Configuration window allows configuration of the DirSync service parameters.

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

Data Migration Assistant

The Cisco Unified CallManager Data Migration Assistant (DMA) provides conversion of Cisco Unified CallManager 4.x data to a format that is compatible with Cisco Unified CallManager 5.0.

For details on obtaining, installing, and using DMA, refer to the *Cisco Unified CallManager Data Migration Assistant 1.0 User Guide*.

Authentication

The authentication process verifies the identity of the user by validating the user ID and password before granting access to the system. Verification takes place against the existing database or the LDAP corporate directory.

The system makes authentication, which the Cisco Unified CallManager administrator makes available in the LDAP Authentication window, available only if LDAP synchronization is enabled in the LDAP System window. If synchronization and authentication are both enabled, the following actions take place:

- The system always authenticates application users against the Cisco Unified CallManager database. When both synchronization and authentication are enabled, the user gets authenticated against the corporate directory. Thus, users need to use their corporate directory password.
- If only synchronization is enabled (and authentication is not enabled), users get authenticated against the Cisco Unified CallManager database. In this case, the administrator can configure a password by using the Cisco Unified CallManager Administration End User Configuration window. The default password specifies *ciscocisco*.

Using the Cisco Unified CallManager Database Versus the Corporate LDAP Directory

Two options exist for using directory information:

- To use only the Cisco Unified CallManager database for users, which is the default functionality when you install Cisco Unified CallManager, Release 5.0, create users with End User Configuration to add to the database (password, names, device association, and so forth). Authentication takes place against the information that is configured in Cisco Unified CallManager Administration. End users and administrators can make password changes if this method is used. This method does not entail LDAP synchronization.
- To use the Corporate LDAP directory (either Microsoft Active Directory or Netscape Directory) with Cisco Unified CallManager, the following steps must take place:
 - For users to use their LDAP corporate directory passwords, the Cisco Unified CallManager administrator must configure LDAP authentication (System > LDAP > LDAP Authentication).
 - Administrators cannot configure LDAP authentication unless they first configure LDAP synchronization. Doing so blocks further End User configuration.

**Note**

Keep in mind that configuring authentication is optional. If authentication is not enabled, administrators and end users have two passwords, an Active Directory or Netscape Directory password and a Cisco Unified CallManager password, which is *ciscocisco* by default.

Directory Access for Cisco Unified Communications Endpoints

The guidelines in this section apply regardless of whether Cisco Unified CallManager or other Cisco Unified Communications applications have been synchronized with a corporate directory. The end-user perception in both cases remains the same because the differences affect only how applications store their user information and how such information is kept consistent across the network.

The following sections summarize how to configure corporate directory access to any LDAPv3-compliant directory server for XML-capable phones such as Cisco Unified IP Phone models 7940, 7960, and so on.

**Note**

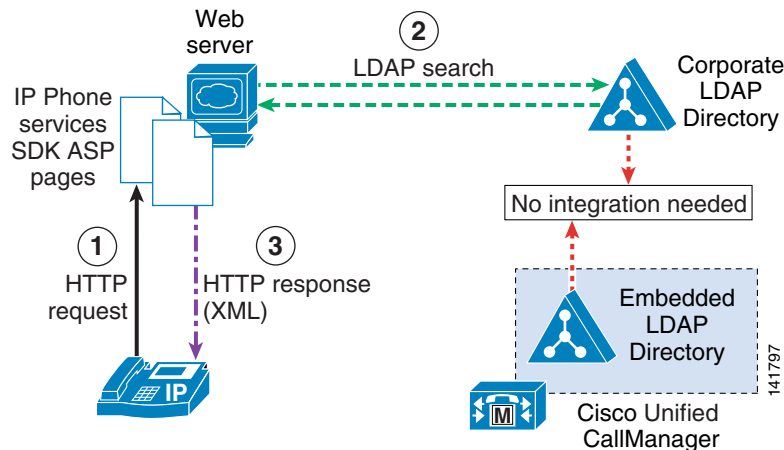
Cisco Unified IP SoftPhone, Release 1.2 and later, includes a built-in mechanism to access and search LDAP directories, as does the Cisco IP Communicator. Refer to the product documentation for details on how to configure this feature.

Directory Access for Cisco Unified IP Phones

XML-capable Cisco Unified IP Phones (such as models 7940, 7960, and so on) can search a corporate LDAP directory when a user presses the Directories button on the phone. The IP phones use HyperText Transfer Protocol (HTTP) to send requests to a web server. The responses from the web server must contain some specific Extensible Markup Language (XML) objects that the phone can interpret and display. In the case of a corporate directory search, the web server operates as a proxy by receiving the request from the phone and translating it into an LDAP request, which is in turn sent to the corporate directory server. After the response is encapsulated in the appropriate XML objects, the response gets interpreted and sent back to the phone.

Figure 9-2 illustrates this mechanism in a deployment where Cisco Unified CallManager has not been synchronized with the corporate directory. In this scenario, the message exchange does not involve Cisco Unified CallManager.

Figure 9-2 Message Exchange for Cisco Unified IP Phone Corporate Directory Access Without Directory Synchronization



You can configure the proxy function that the web server provided by using the Cisco Unified IP Phone Services Software Development Kit (SDK) version 2.0 or later, which includes the Cisco LDAP Search Component Object Model (COM) server.

In addition, directory access for Cisco Unified IP Phones includes the following characteristics:

- The system supports all LDAPv3-compliant directories.
- Cisco Unified CallManager user preferences (speed dials, call forward all, personal address book) do not get synchronized with the corporate LDAP directory. Therefore, users have a separate login and password to access the Cisco Unified CallManager User Options window.

LDAP Directory Configuration Checklist

Table 9-1 lists the general steps and guidelines for configuring LDAP directory information.

Table 9-1 User Directory Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	Use the LDAP System windows to configure LDAP system settings.	LDAP System Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 2	Use the LDAP Directory windows to configure LDAP directory settings.	LDAP Directory Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 3	Use the LDAP Authentication windows to configure LDAP authentication settings.	LDAP Authentication Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>

Table 9-1 User Directory Configuration Checklist (continued)

Configuration Steps		Related procedures and topics
Step 4	If directory synchronization is enabled, use the DirSync service to synchronize with the customer corporate LDAP directory.	<i>Cisco Unified CallManager Serviceability System Guide</i> <i>Cisco Unified CallManager Serviceability Administration Guide</i>
Step 5	To convert Cisco Unified CallManager 4.x data to a format that is compatible with Cisco Unified CallManager 5.0, use the Cisco Unified CallManager Data Migration Assistant (DMA).	<i>Cisco Unified CallManager Data Migration Assistant 1.0 User Guide</i>

Where to Find More Information

Related Topics

- LDAP System Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- LDAP Directory Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- LDAP Authentication Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- *Cisco Unified CallManager Data Migration Assistant 1.0 User Guide*
- *Cisco Unified CallManager Serviceability System Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*
- Cisco Unified CallManager Groups, *Cisco Unified CallManager System Guide, Release 5.0(4)*
- System Configuration Checklist, *Cisco Unified CallManager System Guide, Release 5.0(4)*
- Application Users and End Users, *Cisco Unified CallManager System Guide, Release 5.0(4)*
- Application User Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- End User Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*

Additional Cisco Documentation

- *Installing Cisco Unified CallManager Release 5.0(4)*
- *Cisco Unified Communications Solution Reference Network Design for Cisco Unified CallManager*



Understanding Cisco Unified CallManager Voice Gateways

Cisco Unified Communications gateways enable Cisco Unified CallManager to communicate with non-IP telecommunications devices. Cisco Unified CallManager supports several types of voice gateways.

This section covers the following topics:

- [Cisco Voice Gateways, page 10-1](#)
- [Gateways, Dial Plans, and Route Groups, page 10-16](#)
- [Gateway Failover and Fallback, page 10-17](#)
- [Gateway Configuration Checklist, page 10-20](#)
- [Where to Find More Information, page 10-22](#)

Cisco Voice Gateways

Cisco Unified CallManager supports several types of Cisco Unified Communications gateways. Gateways use call control protocols to communicate with the PSTN and other non-IP telecommunications devices, such as private branch exchanges (PBXs).

Trunk interfaces specify how the gateway communicates with the PSTN or other external devices by using time-division multiplexing (TDM) signaling. Cisco Unified CallManager and Cisco gateways use a variety of TDM interfaces, but supported TDM interfaces vary by gateway model. Refer to the *Cisco Unified Communications Solution Reference Network Design (SRND)* document for more information about selecting and configuring gateways. The following list gives available interfaces that Cisco Unified CallManager supports:

- Foreign Exchange Office (FXO)
- Foreign Exchange Station (FXS)
- T1 Channel Associated Signaling (CAS)
- Basic Rate Interface (BRI)
- T1 PRI—North American ISDN Primary Rate Interface (PRI)
- E1 PRI—European ISDN Primary Rate Interface (PRI)
- QSIG—Q signaling protocol that is based on ISDN standards
- Session Initiation Protocol (SIP)

Cisco Unified CallManager can use H.323 gateways that support E1 CAS, but you must configure the E1 CAS interface on the gateway.

For information about IP telephony protocols, see Understanding IP Telephony Protocols in the *Cisco Unified CallManager System Guide, Release 5.0(4)*.

These sections provide an overview of the following gateways that Cisco Unified CallManager supports:

- [Standalone Voice Gateways, page 10-2](#)
- [Cisco Catalyst 4000 and 6000 Voice Gateway Modules, page 10-5](#)
- [H.323 Gateways, page 10-7](#)

Standalone Voice Gateways

This section describes these standalone, application-specific gateway models that are supported for use with Cisco Unified CallManager.

Cisco Voice Gateway 200

The Cisco Unified Communications Voice Gateway (VG200) provides a 10/100BaseT Ethernet port for connection to the data network. The following list gives available telephony connections:

- 1 to 4 FXO ports for connecting to a central office or PBX
- 1 to 4 FXS ports for connecting to POTS telephony devices
- 1 or 2 Digital Access T1 ports for connecting to the PSTN
- 1 or 2 Digital Access PRI ports for connecting to the PSTN
- MGCP or H.323 interface to Cisco Unified CallManager
 - MGCP mode supports T1/E1 PRI, T1 CAS, FXS, FXO. (Only the user side supports BRI.)
 - H.323 mode supports E1/T1 PRI, E1/T1 CAS, FXS, and FXO. H.323 mode supports E&M, fax relay, and G.711 modem.

The MGCP VG200 integration with legacy voice-messaging systems allows the Cisco Unified CallManager to associate a port with a voice mailbox and connection.

Cisco Access Digital Trunk Gateways DT-24+/DE-30+

The Cisco Access Digital Trunk Gateways DT-24+/DE-30+ provide the following features:

- Digital Access PRI (network or user side)
- T1 CAS connections (DT-24+) that support E&M signaling with wink or delay dial supervision
- FXO with loop-start or ground-start circuit emulation
- MGCP interface to Cisco Unified CallManager

Cisco VG248 Analog Phone Gateway

The Cisco VG248 Analog Phone Gateway has a standalone, 19-inch rack-mounted chassis with 48-FXS ports. This product allows on-premise analog telephones, fax machines, modems, voice-messaging systems, and speakerphones to register with a single Cisco Unified CallManager cluster.

Cisco VG248 Analog Phone Connectivity

The Cisco VG248 Analog Phone Gateway communicates with Cisco Unified CallManager by using the Skinny Client Control Protocol to allow support for the following supplementary services features for analog phones:

- Call transfer
- Conference
- Call waiting (with calling party ID display)
- Hold (including switch between parties on hold)
- Music on hold
- Call forward all
- Send all calls to voice-messaging system
- Group call pickup
- Voice-messaging system message waiting indication
- Speed dial (maximum of 9 speed dials)
- Last number redial
- Cisco fax relay
- Dynamic port and device status that is available from Cisco Unified CallManager

Cisco VGC Phone Device Types

All Cisco VG248 ports and units appear as distinct devices in Cisco Unified CallManager with the device type “Cisco VGC Phone.” Cisco Unified CallManager recognizes and configures each port as a phone.

Fax and Modem Connectivity

The Cisco VG248 supports legacy fax machines and modems. When using fax machines, the Cisco VG248 uses either the Cisco fax relay or pass-through/up speed technology to transfer faxes across the network with high reliability.

You can connect any modem to the Cisco VG248 by using pass-through mode.

Voice-Mail Connectivity

The Cisco VG248 generates call information by using the Simplified Message Desk Interface (SMDI) format for all calls that are ringing on any of the 48 analog lines that connect to it. It will also pass on SMDI call information from other Cisco VG248s, or from a legacy PBX, to the voice-messaging system. Any commands for message-waiting indicators get sent to Cisco Unified CallManager and to any other attached SMDI hosts.

This mechanism allows for many new configurations when SMDI-based voice-messaging systems are used, including

- You can share a single voice-messaging system between Cisco Unified CallManager and a legacy PBX.
- Voice-messaging system and Cisco VG248 can function remotely in a centralized call-processing model.
- Multiple clusters can use a single voice-messaging system, by using one Cisco VG248 per cluster.
- Configure multiple voice-messaging systems in a single cluster because the Cisco VG248 generates SMDI call information rather than the Cisco Unified CallManager.

Cisco VG248 Time Device

The Cisco VG248 contains a real-time clock that is persistent across power cycles and restarts. The real-time clock gets set for the first time when the device registers with Cisco Unified CallManager. The clock gets set by using the DefineDateTime Skinny message that Cisco Unified CallManager sends. After a power cycle or restart, the clock resets when the Cisco VG248 receives the DefineDateTime message from Cisco Unified CallManager and then resets no more than once per hour thereafter.

Cisco VG248 Configuration File Updates

The Cisco VG248 queries the TFTP server to access the configuration files for the device. The configuration files update whenever you modify the configuration of the Cisco VG248 via Cisco Unified CallManager.

Refer to the “Gateway Configuration” section and the “Cisco Unified IP Phone Configuration” section of the *Cisco Unified CallManager Administration Guide, Release 5.0(4)* and to the *Cisco VG248 Analog Phone Gateway Software Configuration Guide* for more information.

Cisco VG224 Analog Phone Gateway

The Cisco VG224 Analog Phone Gateway has a standalone, 17-inch rack-mounted chassis with 24-FXS ports. This product allows on-premise analog telephones, fax machines, modems, and speaker phones to register with Cisco Unified CallManager.

This gateway supports the SCCP and SIP protocols.

Cisco IAD2400 Series Integrated Access Device

The Cisco IAD2420 integrated access device provides voice, data, and video services over internet protocol (IP) and asynchronous transfer mode (ATM) networks. By using the Cisco IAD 2420, service providers can deliver toll-quality voice and data services over circuit- or packet-switched networks. The Cisco IAD2420 provides an MGCP interface with Cisco Unified CallManager and supports the following capabilities:

- Analog: FXS ports for POTS telephony devices, FXO ports for PSTN connections
- Digital: Digital Access PRI and Digital Access T1 services

MGCP BRI Call Connections

Previously, gateways used H.323 signaling to Cisco Unified CallManager to provide interfaces to the public switched telephone network (PSTN) for BRI ISDN connections. The following list gives drawbacks to using the H.323 protocol:

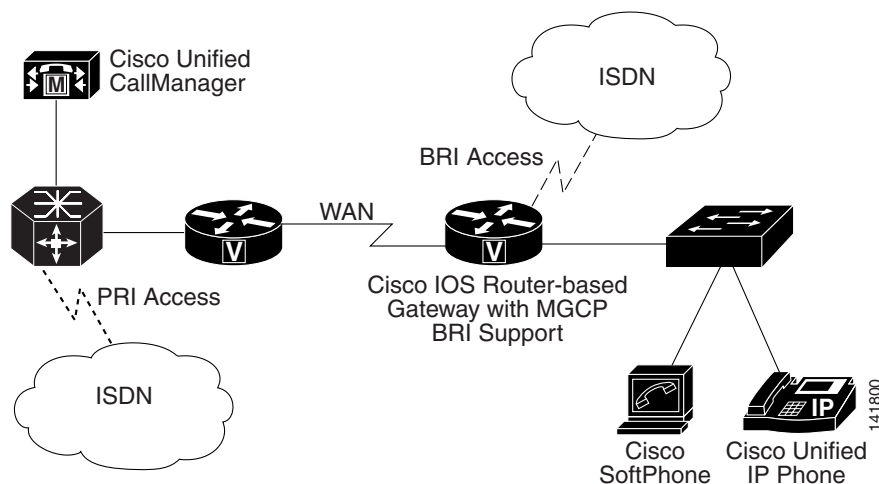
- Deploying and managing a large number of gateways in a private network represents a very time-consuming task because you must provision every H.323 gateway and its dial plan at the gateway.
- Voice clipping occurs when calls to IP phones use the H.323 gateway because the media cut-through times are very high.
- Calls disconnect if the controlling Cisco Unified CallManager fails during a call.

Now, Cisco Unified CallManager can use a Media Gateway Control Protocol (MGCP) gateway to handle BRI ISDN connections to the PSTN and to provide a centrally administered gateway interface. Cisco Unified CallManager uses logical connections to exchange MGCP and ISDN Q.931 messages

with the gateway. This connection uses a User Datagram Protocol (UDP) logical connection for exchanging MGCP messages and a Transmission Control Protocol (TCP) connection for the backhaul ISDN Q.931 messages.

Figure 10-1 shows a typical scenario that centralizes call processing for remote-site BRI trunk gateways that connect to the PSTN. When a call arrives from or goes to the PSTN over the BRI trunk, the Cisco Unified CallManager and the gateway (based on an IOS router) exchange ISDN Q.931 messages across the WAN.

Figure 10-1 Topology Shows a Scenario by Using MGCP BRI Interfaces



For more information about MGCP BRI with Cisco Unified CallManager, refer to the *MGCP-Controlled Backhaul of BRI Signaling in Conjunction with Cisco Unified CallManager* document on the Cisco.com website.



Note

The BRI gateway supports MGCP BRI backhaul for BRI trunk only. It does not support BRI phone or station. The IOS gateway supports BRI phones that use Skinny Client Control Protocol.

Cisco Catalyst 4000 and 6000 Voice Gateway Modules

Several telephony modules for the Cisco Catalyst 4000 and 6000 family switches act as telephony gateways. You can use existing Cisco Catalyst 4000 or 6000 family devices to implement IP telephony in your network by using the following voice gateway modules:

- Install Catalyst 6000 voice gateway modules that are line cards in any Cisco Catalyst 6000 or 6500 series switch.
- Install the Catalyst 4000 access gateway module in any Catalyst 4000 or 4500 series switch.

Cisco Catalyst 6000 8-Port Voice T1/E1 and Services Module

The Cisco Catalyst 6000 8-Port Voice T1/E1 and Services Modules provide the following features:

- 8 ports for providing
 - Digital T1/E1 connectivity to the PSTN (T1/E1 PRI or T1 CAS with the same features as DT-24+/DE-30+)
 - Digital signal processor (DSP) resources for transcoding and conferencing
- MGCP interface to Cisco Unified CallManager
- Connection to a voice-messaging system (using T1 CAS)

Users have the flexibility to use ports on a T1 module for T1 connections or as network resources for voice services. Similarly, the E1 module provides ports for E1 connections or as network resources. The ports can serve as T1/E1 interfaces, or the ports will support transcoding or conferencing.

**Note**

Either module supports DSP features on any port, but T1 modules cannot be configured for E1 ports, and E1 modules cannot be configured for T1 ports.

Similar to the Cisco MGCP-controlled gateways with FXS ports, the Cisco 6608 T1 CAS gateway supports hookflash transfer. Hookflash transfer defines a signaling procedure that allows a device, such as a voice-messaging system, to transfer to another destination. While the device is connected to Cisco Unified CallManager through a T1 CAS gateway, the device performs a hookflash procedure to transfer the call to another destination. Cisco Unified CallManager responds to the hookflash by using a blind transfer to move the call. When the call transfer completes, the voice channel that connected the original call to the device gets released.

**Note**

Only E&M T1 ports support hookflash transfer.

Cisco Catalyst 6000 24 Port FXS Analog Interface Module

The Cisco Catalyst 6000 24 Port FXS Analog Interface Module provides the following features:

- 24 Port RJ-21 FXS module
- V.34/V.90 modem, voice-messaging system, IVR, POTS
- Cisco fax relay
- MGCP interface to Cisco Unified CallManager

The Catalyst 6000 24 Port FXS Analog Interface Module provides 24 FXS ports for connecting to analog phones, conference room speakerphones, and fax machines. You can also connect to legacy voice-messaging systems by using SMDI and by associating the ports with voice-messaging extensions.

The FXS module provides legacy analog devices with connectivity into the IP network. Analog devices can use the IP network infrastructure for toll-bypass applications and to communicate with devices such as SCCP IP phones and H.323 end stations. The FXS module also supports fax relay, which enables compressed fax transmission over the IP WAN and preserves valuable WAN bandwidth for other data applications.

Cisco Communication Media Module

The Cisco Communication Media Module (CMM), which is a Catalyst 6500 line card, provides T1 and E1 gateways that allow organizations to connect their existing TDM network to their IP communications network. The Cisco CMM provides connectivity to the PSTN also. You can configure the Cisco CMM, which provides an MGCP interface to Cisco Unified CallManager, with the following interface and service modules:

- 6-port T1 interface module for connecting to the PSTN or a PBX
- 6-port E1 interface module for connecting to the PSTN or a PBX
- 24-port FXS interface module for connecting to POTS telephony devices

Cisco Catalyst 4000 Access Gateway Module

The Cisco Catalyst 4000 Access Gateway Module provides an MGCP or H.323 gateway interface to Cisco Unified CallManager. You can configure this module with the following interface and service modules:

- 6 ports for FXS and FXO
- 2 T1/E1 ports for Digital Access PRI and Digital Access T1

Cisco Catalyst 4224 Voice Gateway Switch

The Cisco Catalyst 4224 Voice Gateway Switch provides a single-box solution for small branch offices. The Catalyst 4224 provides switching, IP routing, and PSTN voice-gateway services by using onboard digital signal processors (DSPs). The Catalyst 4224 has four slots that you can configure with multiflex voice and WAN interface cards to provide up to 24 ports. These ports can support the following voice capabilities:

- FXS ports for POTS telephony devices
- FXO ports for PSTN connections
- T1 or E1 ports for Digital Access PRI, and Digital Access T1 services

The Cisco Catalyst 4224 Access Gateway Switch provides an MGCP or H.323 interface to Cisco Unified CallManager.

H.323 Gateways

H.323 devices comply with the H.323 communications standards and enable video conferencing over LANs and other packet-switched networks. You can add third-party H.323 devices or other Cisco devices that support H.323 (such as the Cisco 2600 series, 3600 series, or 5300 series gateways).

Cisco IOS H.323 Gateways

Cisco IOS H.323 gateways such as the Cisco 2600, 3600, 1751, 1760, 3810 V3, 7200 7500, AS5300, and VG200 provide full-featured routing capabilities. Refer to the documentation for each of these gateway types for information about supported voice gateway features and configuration.

T.38 Fax Relay

Transporting real-time Group 3 fax documents over internet protocol (IP) uses the International Telecommunications Union Telecommunication Standardization Sector (ITU-T) recommendation T.38 Fax Relay. The T.38 standard defines the IP network protocol that Internet-aware T.38 fax devices and T.38 IP fax gateways use. The T.38 Fax Relay for VoIP H.323 feature provides standards-based, fax relay protocol support for Cisco and other vendor gateways.

The T.38 Fax Relay feature provides a standards-based, fax relay protocol that is available on several Cisco gateways. Because the T.38 Fax Relay protocol is standards based, Cisco gateways and gatekeepers can interoperate with third-party T.38 enabled gateways and gatekeepers in a mixed vendor network that requires real-time fax relay capabilities.

Cisco Unified CallManager handles the T.38 fax call by using a voice connection. When the originating gateway sends a fax, the gateway establishes an initial voice call. The terminating gateway detects the fax tone that the answering fax machine generates. The VoIP H.323 call stack then starts a T.38 mode request by using H.245 procedures. If the opposite end of the call acknowledges the T.38 mode request, the initial audio channel closes, and T.38 Fax Relay channel opens. When the fax transmission finishes, the call disconnects.

Transcoders should be provisioned for use with T.38 Fax Relay either when codec mismatches exist or when fast-connect procedures are employed.

**Note**

Cisco IP Voice Media Streaming Application Service does not support T.38 data transmission. To prevent Cisco IP Voice Media Streaming Application Services from interfering with T.38 fax relay calls, the Cisco IP Voice Media Streaming Application service must be assigned to a Media Resource Group and that Media Resource Group must not be used in any gateways or trunks that are involved in T.38 calls.

Outbound FastStart Call Connections

Calls that are placed from IP phones over large WAN topologies can experience voice clipping when the called party goes off hook to answer the call. When H.323 trunks or gateways are separated from the Cisco Unified CallManager server, significant delays can occur because of the many H.245 messages that are exchanged when a call is set up.

With the FastStart feature, information that is required to complete a media connection between two parties gets exchanged during the H.225 portion of call setup, and this exchange eliminates the need for H.245 messages. The connection experiences one roundtrip WAN delay during call setup, and the calling party does not receive voice clipping when the called party answers the call.

Cisco Unified CallManager uses media termination points (MTP) for making an H.323 outbound FastStart call. Cisco Unified CallManager starts an outbound FastStart call by allocating an MTP and opening the receive channel. Next, the H.323 Fast Connect procedure sends the SETUP message with a FastStart element to the called endpoint. The FastStart element includes information about the receiving channel for the MTP.

The called endpoint accepts the H.323 Fast Connect procedure by sending a CALL PROCEEDING, PROGRESS, ALERT, or CONNECT message that contains a FastStart element. When Cisco Unified CallManager receives the FastStart element, it connects the media immediately and avoids the delays with the usual exchange of H.245 messages.

The called endpoint can refuse the H.323 Fast Connect procedure by not returning the FastStart element in any of the messages up to and including the CONNECT message. In this case, the Cisco Unified CallManager handles the call as a normal call and uses the MTP for subsequent media cut-through.

The Outbound FastStart feature requires an MTP. If an MTP is not available when the call is set up, the call continues without FastStart and with no supplementary services. If you want all calls to use FastStart only, you can set the service parameter called “Fail call if MTP allocation fails,” which is located in the Cluster Wide Parameters (Device-H323) portion of the service parameters for the Cisco Unified CallManager service. When you set this parameter to True, the system rejects calls when no MTP is available.

Related Topic

H.323 Gateway Configuration Settings, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*

Voice Gateway Model Summary

[Table 10-1](#) summarizes Cisco voice gateways that Cisco Unified CallManager supports with information about the supported signaling protocols, trunk interfaces, and port types.

Table 10-1 Overview of Supported Voice Gateways, Protocols, Trunk Interfaces, and Port Types

Gateway Model	Supported Signaling Protocols	Trunk Interfaces	Port Types	Notes
Cisco IOS Integrated Routers				
Cisco 1751 and Cisco 1760	H.323 and SIP	FXS	Loopstart or groundstart	Basic calls only
		FXO	Loopstart or groundstart	
		E&M		
		Analog DID		
		CAMA		
		BRI		
		BRI QSIG		Basic calls only
		T1 CAS (E&M, FXS, FXO)		
		E1 R2		
		T1/E1 QSIG		Basic calls only
		T1/E1 PRI		
	MGCP	FXS	Loopstart only	Basic calls only
		FXO	Loopstart or groundstart	No caller ID
		BRI		User side only; no QSIG support

Table 10-1 Overview of Supported Voice Gateways, Protocols, Trunk Interfaces, and Port Types (continued)

Gateway Model	Supported Signaling Protocols	Trunk Interfaces	Port Types	Notes
		T1 CAS (E&M)		
		T1/E1 QSIG		Supplementary Services
		T1/E1 PRI		
Cisco 2600, 2600XM series, 2691, 3700 series	H.323 and SIP	FXS	Loopstart or groundstart	
		FXO	Loopstart or groundstart	Basic calls only
		E&M		
		Analog DID		
		CAMA		
		BRI		
		BRI QSIG		Basic calls only
		T1 CAS (E&M, FXS, FXO)		
		T1 FGD		
		E1 CAS		
		E1 R2		
		T1/E1 QSIG		Basic calls only
		T1/E1 PRI		
		T1 PRI NFAS		
		T1 PRI (Megacom/SDN)		Per T1 port only; not per call
	MGCP	FXS	Loopstart only	Basic calls only
		FXO	Loopstart or groundstart	No caller ID
		BRI		Only 2600XM/2691 support MGCP BRI; User side only; no QSIG support
		T1 CAS (E&M)		
		T1/E1 QSIG		Supplementary Services
		T1/E1 PRI		
		T1 PRI (Megacom/SDN)		Per call
	SCCP	BRI		DoD STE BRI phones only; single-B-channel

Table 10-1 Overview of Supported Voice Gateways, Protocols, Trunk Interfaces, and Port Types (continued)

Gateway Model	Supported Signaling Protocols	Trunk Interfaces	Port Types	Notes
Cisco 3600 series	H.323 and SIP	FXS	Loopstart or groundstart	Basic calls only
		FXO	Loopstart or groundstart	
		E&M		
		Analog DID		
		CAMA		
		BRI		
		BRI QSIG		Basic calls only
		T1 CAS (E&M, FXS, FXO)		
		T1 FGD		
		E1 CAS		
		E1 R2		
		T1/E1 QSIG		Basic calls only
		T1/E1 PRI		
		T1 PRI NFAS		
		T1 PRI (Megacom/SDN)		Per T1 port only; not per call
	MGCP	FXS	Loopstart only	Basic calls only
		FXO	Loopstart or groundstart	No caller ID
		BRI		Only 3640/3660 and some interface cards support MGCP BRI; User side only; no QSIG support
		T1 CAS (E&M)		
		T1/E1 QSIG		Supplementary Services
		T1/E1 PRI		
		T1 PRI (Megacom/SDN)		Per call
Cisco 2800 and 3800 series	H.323 and SIP	FXS	Loopstart or groundstart	Basic calls only
		FXO	Loopstart or groundstart	
		E&M		

Table 10-1 Overview of Supported Voice Gateways, Protocols, Trunk Interfaces, and Port Types (continued)

Gateway Model	Supported Signaling Protocols	Trunk Interfaces	Port Types	Notes
		Analog DID		
		CAMA		
		BRI		
		BRI QSIG		Basic calls only
		T1 CAS (E&M, FXS, FXO)		
		T1 FGD		
		E1 CAS		
		E1 R2		
		T1/E1 QSIG		Basic calls only
		T1/E1 PRI		
		T1 PRI NFAS		
		T1 PRI (Megacom/SDN)		Per T1 port only; not per call
	MGCP	FXS	Loopstart only	Basic calls only
		FXO	Loopstart or groundstart	No caller ID
		BRI		User side only; no QSIG support
		T1 CAS (E&M)		
		T1/E1 QSIG		Supplementary Services
		T1/E1 PRI		
		T1 PRI (Megacom/SDN)		Per call
	SCCP	FXS		
Cisco 7200 series	H.323	T1 CAS (E&M, FXS, FXO)		
		T1 FGD		
		E1 R2		
		T1/E1 QSIG		Basic calls only
		T1/E1 PRI		
Cisco 5000 series	H.323 and SIP	T1 CAS (E&M, FXS, FXO)		
		T1 FGB		
		T1 FGD		
		E1 R2		

Table 10-1 Overview of Supported Voice Gateways, Protocols, Trunk Interfaces, and Port Types (continued)

Gateway Model	Supported Signaling Protocols	Trunk Interfaces	Port Types	Notes
		T1/E1 QSIG		Basic calls only
		T1/E1 PRI		
Cisco Standalone Voice Gateways				
Cisco VG224 Analog Gateway	H.323, MGCP, and SIP	FXS		Basic calls only
	SCCP	FXS		Supplementary Services
Cisco VG248 Analog Gateway	SCCP	FXS		Supplementary Services
Cisco VG200 Gateway	H.323 and SIP	FXS	Loopstart or groundstart	Basic calls only
		FXO	Loopstart or groundstart	
		E&M		
		Analog DID		
		CAMA		
		BRI		
		BRI QSIG		
		T1 CAS (E&M, FXS, FXO)		
		T1 FGD		
		E1 CAS		
		E1 R2		
		T1/E1 QSIG		Basic calls only
		T1/E1 PRI		
		T1 PRI NFAS		
		T1 PRI (Megacom/SDN)		Per T1 port only; not per call
	MGCP	FXS	Loopstart only	Basic calls only
		FXO	Loopstart or groundstart	No caller ID
		BRI		Only 2600XM/2691 support MGCP BRI; User side only; no QSIG support
		T1 CAS (E&M)		
		T1/E1 QSIG		Supplementary Services

Table 10-1 Overview of Supported Voice Gateways, Protocols, Trunk Interfaces, and Port Types (continued)

Gateway Model	Supported Signaling Protocols	Trunk Interfaces	Port Types	Notes
		T1/E1 PRI		
		T1 PRI (Megacom/SDN)		Per call
Cisco Access Digital Trunk Gateway DE-30+	MGCP	E1 PRI		
		E1 QSIG		Supplementary Services
Cisco Access Digital Trunk Gateway DT-24+	MGCP	T1 CAS (E&M)		
		T1 PRI		
		T1 QSIG		Supplementary Services
Cisco Access Analog Trunk Gateway (AT-2, AT-4, AT-8)	SCCP	FXO	Loop start	
Cisco Access Analog Station Gateway (AS-2, AS-4, AS-8)	SCCP	FXS		Supplementary Services
Cisco Catalyst Voice Gateway Modules				
Cisco Communication Media Module (WS-X6600-24FXS)	MGCP or H.323	FXS		Basic calls only
Cisco Communication Media Module (WS-X6600-6T1)	H.323	T1 CAS (E&M)		
		T1 PRI		
		T1 QSIG		Basic calls only
		T1 PRI NFAS		
	MGCP	T1 CAS (E&M)		
		T1 QSIG		Supplementary Services
		T1 PRI		
Cisco Communication Media Module (WS-X6600-6E1)	H.323	E1 PRI		
		E1 QSIG		Basic calls only
		E1 R2		
	MGCP	E1 PRI		
		E1 QSIG		Supplementary Services
Cisco Catalyst 4000 Access Gateway Module (WS-X4604-GWY)	H.323	FXS	Loopstart or groundstart	Basic calls only

Table 10-1 Overview of Supported Voice Gateways, Protocols, Trunk Interfaces, and Port Types (continued)

Gateway Model	Supported Signaling Protocols	Trunk Interfaces	Port Types	Notes
		FXO	Loopstart or groundstart	
		T1 CAS		
		T1/E1 QSIG		Basic calls only
		T1/E1 PRI		
	MGCP	FXS		Basic calls only
		FXO		
		T1 CAS (E&M)		
		T1/E1 QSIG		Supplementary Services
		T1/E1 PRI		
Cisco Catalyst 4224 Voice Gateway Switch	H.323	FXS		Basic calls only
		FXO		
		BRI		
		T1 CAS		
		E1 R2		
		T1/E1 QSIG		
		T1/E1 PRI		
Cisco Catalyst 6000 8-Port Voice T1/E1 and Services Module (WS-X6608-T1)	MGCP	T1 CAS (E&M)		
		T1 PRI		
		T1 QSIG		Supplementary Services
Cisco Catalyst 6000 8-Port Voice T1/E1 and Services Module (WS-X6608-E1)	MGCP	E1 PRI		
		E1 QSIG		Supplementary Services
Cisco Catalyst 6000 24-Port FXS Analog Interface Module (WS-X6624-FXS)	MGCP	FXS	Loopstart only	Basic calls only

Gateways, Dial Plans, and Route Groups

Gateways use dial plans to access or call out to the PSTN, route groups, and group-specific gateways. The different gateways that are used within Cisco Unified Communications Solutions have dial plans that are configured in different places:

- Configure dial plan information for both Skinny and MGCP gateways in the Cisco Unified CallManager.
- Configure dial plans in Cisco Unified CallManager to access the H.323-based Cisco IOS software gateways. Configure dial peers in the H.323-based gateways to pass the call out of the gateway.

The route group points to one or more gateways and can choose the gateways for call routing based on preference. The route group can serve as a trunk group by directing all calls to the primary device and then using the secondary devices when the primary is unavailable. One or more route lists can point to the same route group.

All devices in a given route group share the same characteristics such as path and digit manipulation. Cisco Unified CallManager restricts the gateways that you can include in the same route group and the route groups that you can include in the same route list. For more information about routing, see the [“Route Plan Overview” section on page 7-4](#).

Route groups can perform digit manipulation that will override what was performed in the route pattern. Configuration information that is associated with the gateway defines how the call is actually placed and can override what was configured in the route pattern.

You can configure H.323 trunks, *not* H.323 gateways, to be gatekeeper-controlled trunks. This means that before a call is placed to an H.323 device, it must successfully query the gatekeeper. See the “Gatekeeper and Trunk Configuration in Cisco Unified CallManager” section in the Cisco Unified CallManager System Guide, Release 5.0(4) for more information.

Multiple clusters for inbound and outbound calls can share H.323 trunks, but MGCP and Skinny-based gateways remain dedicated to a single Cisco Unified CallManager cluster.

Related Topics

- [Dependency Records for Gateways and their Route Groups and Directory Numbers, page 10-16](#)
- [Cisco Voice Gateways, page 10-1](#)

Dependency Records for Gateways and their Route Groups and Directory Numbers

To find route groups or directory numbers that a specific gateway or gateway port is using, click the Dependency Records link that is provided on the Cisco Unified CallManager Administration Gateway Configuration window. The Dependency Records Summary window displays information about route groups and directory numbers that are using the gateway or port. To find out more information about the route group or directory number, click the route group or directory number, and the Dependency Records Details window displays. 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”, “Deleting Gateways”, and “Removing a Directory Number from a Phone” sections in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

Related Topics

- [Gateways, Dial Plans, and Route Groups, page 10-16](#)
- [Cisco Voice Gateways, page 10-1](#)

Gateway Failover and Fallback

This section describes how these Cisco voice gateways handle Cisco Unified CallManager failover and fallback situations. See the following topics:

- [MGCP Gateways, page 10-17](#)
- [IOS H.323 Gateways, page 10-17](#)
- [Cisco VG248 Analog Phone Gateway, page 10-18](#)

MGCP Gateways

To handle Cisco Unified CallManager failover situations, MGCP gateways receive a list of Cisco Unified CallManagers that is arranged according to the Cisco Unified CallManager group and defined for the device pool that is assigned to the gateway. A Cisco Unified CallManager group can contain one, two, or three Cisco Unified CallManagers that are listed in priority order for the gateway to use. If the primary Cisco Unified CallManager in the list fails, the secondary Cisco Unified CallManager gets used. If the primary and secondary Cisco Unified CallManagers fail, the tertiary Cisco Unified CallManager gets used.

Fallback describes the process of recovering a higher priority Cisco Unified CallManager when a gateway fails over to a secondary or tertiary Cisco Unified CallManager. Cisco MGCP gateways periodically take status of higher priority Cisco Unified CallManagers. When a higher priority Cisco Unified CallManager is ready, it gets marked as available again. The gateway reverts to the highest available Cisco Unified CallManager when all calls go idle or within 24 hours, whichever occurs first. The administrator can force a fallback either by stopping the lower priority Cisco Unified CallManager whereby calls get preserved, by restarting the gateway, which preserves calls, or by resetting Cisco Unified CallManager, which terminates calls.

**Note**

Skinny Client Control Protocol (SCCP) gateways handle Cisco Unified CallManager redundancy, failover, and fallback in the same way as MGCP gateways.

IOS H.323 Gateways

Cisco IOS gateways also handle Cisco Unified CallManager failover situations. By using several enhancements to the **dial-peer** and **voice class** commands in Cisco IOS Release 12.1(2)T, Cisco IOS gateways can support redundant Cisco Unified CallManagers. The command, **h225 tcp timeout seconds**, specifies the time that it takes for the Cisco IOS gateway to establish an H.225 control connection for H.323 call setup. If the Cisco IOS gateway cannot establish an H.225 connection to the primary Cisco Unified CallManager, it tries a second Cisco Unified CallManager that is defined in another **dial-peer** statement. The Cisco IOS gateway shifts to the **dial-peer** statement with the next highest **preference** setting.

The following example shows the configuration for H.323 gateway failover:

```
interface FastEthernet0/0
  ip address 10.1.1.10 255.255.255.0
dial-peer voice 101 voip
  destination-pattern 1111
  session target ipv4:10.1.1.101
  preference 0
  voice class h323 1
dial-peer voice 102 voip
  destination-pattern 1111
  session target ipv4:10.1.1.102
  preference 1
  voice class h323 1
voice class h323 1
  h225 timeout tcp establish 3
```



Note

To simplify troubleshooting and firewall configurations, Cisco recommends that you use the new `voip-gateway voip bind srcaddr` command for forcing H.323 always to use a specific source IP address in call setup. Without this command, the source address that is used in the setup might vary and depends on protocol (RAS, H.225, H.245, or RTP).

Cisco VG248 Analog Phone Gateway

The Cisco VG248 Analog Phone Gateway supports the Skinny Client Control Protocol (SCCP) for clustering and failover.

Transferring Calls Between Gateways

Using Cisco Unified CallManager Administration, you can configure gateways as OnNet (internal) gateways or OffNet (external) gateways by using Gateway Configuration or by setting a clusterwide service parameter. Used in conjunction with the clusterwide service parameter, Block OffNet to OffNet Transfer, the configuration determines whether calls can be transferred over a gateway.

To use the same gateway to route both OnNet and OffNet calls, associate the gateway with two different route patterns. Make one gateway OnNet and the other OffNet with both having the Allow Device Override check box unchecked.

Configuring Transfer Capabilities Using Gateway Configuration

Using Cisco Unified CallManager Administration Gateway Configuration, you can configure a gateway as OffNet or OnNet. The system considers the calls that come to the network through that gateway OffNet or OnNet, respectively. Use the Gateway Configuration window field, Call Classification, to configure the gateway as OffNet, OnNet, or Use System Default. See [Table 10-2](#) for description of these settings.

The Route Pattern Configuration window provides a drop-down list box called Call Classification, which allows you to configure a route pattern as OffNet or OnNet. When Call Classification is set to OffNet and the Allow Device Override check box is unchecked, the system considers the outgoing calls that use this route pattern as OffNet (if configured as OnNet and check box is unchecked, then outgoing calls are considered OnNet).

The same gateway can be used to route both OnNet and OffNet calls by associating the gateway with two different route patterns: one OnNet and the other OffNet, with both having the Allow Device Override check box unchecked. For outgoing calls, the outgoing device setting classifies the call as either OnNet or OffNet by determining whether the Allow Device Override check box is checked.

In route pattern configuration, if the Call Classification is set as OnNet, the Allow Device Override check box is checked, and the route pattern is associated with an OffNet gateway, the system considers the outgoing call OffNet.

Table 10-2 Gateway Configuration Call Classification Settings

Setting Name	Description
OffNet	This setting identifies the gateway as being an external gateway. When a call comes in from a gateway that is configured as OffNet, the outside ring gets sent to the destination device.
OnNet	This setting identifies the gateway as being an internal gateway. When a call comes in from a gateway that is configured as OnNet, the inside ring gets sent to the destination device.
Use System Default	This setting uses the Cisco Unified CallManager clusterwide service parameter Call Classification.

Configuring Transfer Capabilities by Using Call Classification Service Parameter

To configure all gateways to be OffNet (external) or OnNet (internal), perform the following two steps:

1. Use the Cisco Unified CallManager clusterwide service parameter Call Classification.
2. Configure individual gateways to Use System Default in the Call Classification field that is on the Gateway Configuration window.

Blocking Transfer Capabilities by Using Service Parameters

Block transfer provides a way of restricting transfer between external devices, so fraudulent activity gets prevented. You can configure the following devices as OnNet (internal) or OffNet (external) to Cisco Unified CallManager:

- H.323 gateway
- MGCP FXO trunk
- MGCP T1/E1 trunk
- Intercluster trunk
- SIP trunk

If you do not want OffNet calls to be transferred to an external device (one that is configured as OffNet), set the Cisco Unified CallManager clusterwide service parameter, Block OffNet to OffNet Transfer, to True.

If a user tries to transfer a call on an OffNet gateway that is configured as blocked, a message displays on the user phone to indicate that the call cannot be transferred.

Related Topics

- Route Pattern Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Gateway Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Trunk Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*

Gateway Configuration Checklist

Table 10-3 provides an overview of the steps that are required to configure gateways in Cisco Unified CallManager, along with references to related procedures and topics.

Table 10-3 **Gateway Configuration Checklist**

Configuration Steps		Procedures and Related Topics
Step 1	Install and configure the gateway or voice gateway module in the network.	Refer to the installation and configuration documentation for the model of gateway that you are configuring.
Step 2	Gather the information that you need to configure the gateway to operate with Cisco Unified CallManager.	Gateway Configuration Settings, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> Port Configuration Settings, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 3	On the gateway, perform any required configuration steps.	Refer to the voice feature software configuration documentation or Cisco IOS documentation for the model of gateway that you are configuring.
Step 4	Add and configure the gateway in Cisco Unified CallManager Administration.	Adding Gateways to Cisco Unified CallManager, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 5	Add and configure ports on the gateway or add and configure the Cisco VG248 Analog Phone Gateway.	Port Configuration Settings, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> Adding a Cisco VG248 Analog Phone Gateway, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> Cisco Unified IP Phone Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 6	For FXS ports, add directory numbers, if appropriate.	Directory Number Configuration Overview, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> Directory Number Configuration Settings, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>

Table 10-3 Gateway Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 7	Configure the dial plan for the gateway for routing calls out to the PSTN or other destinations. This configuration can include setting up a route group, route list, and route pattern for the Gateway in Cisco Unified CallManager or, for some gateways, configuring the dial plan on the gateway itself.	<i>Cisco Unified Communications Solution Reference Network Design</i> <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 8	Reset the gateway to apply the configuration settings.	Resetting and Restarting Gateways, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>

**Tip**

To get to the default web pages for many gateway devices, you can use the IP address of that gateway. Make your hyperlink url = `http://x.x.x.x/`, where x.x.x.x is the dot-form IP address of the device. The web page for each gateway contains device information and the real-time status of the gateway.

MGCP BRI Gateway Configuration Checklist

Table 10-4 provides an overview of the steps that are required to configure a BRI gateway in Cisco Unified CallManager, along with references to related procedures and topics.

Table 10-4 MGCP BRI Gateway Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Install and configure the gateway and voice modules in the network.	Refer to the installation and configuration documentation for the model of gateway that you are configuring.
Step 2	Gather the information that you need to configure the gateway to operate with Cisco Unified CallManager and to configure the trunk interface to the PSTN or external non-IP telephony device.	Gateway Configuration Checklist, page 10-20 Adding a BRI Port to an MGCP Gateway, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 3	On the gateway, perform any required configuration steps.	Refer to the voice feature software configuration documentation or Cisco IOS documentation for the model of gateway that you are configuring.
Step 4	Add and configure the gateway in Cisco Unified CallManager Administration.	Gateway Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 5	Add and configure ports on the gateway.	Gateway Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>

Table 10-4 MGCP BRI Gateway Configuration Checklist (continued)

Configuration Steps	Procedures and Related Topics
Step 6 Configure the dial plan for the gateway for routing calls out to the PSTN or other destinations. This configuration can include setting up a route group, route list, and route pattern for the gateway in Cisco Unified CallManager or, for some gateways, configuring the dial plan on the gateway itself.	<i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> <i>Cisco Unified Communications Solution Reference Network Design (SRND)</i>
Step 7 Reset the gateway to apply the configuration settings.	<i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>

**Tip**

To get to the default web pages for gateway devices, you can use the IP address of that gateway. Make your hyperlink url = <http://x.x.x.x/>, where x.x.x.x specifies the dot-form IP address of the device. The web page for each gateway contains device information and the real-time status of the gateway.

Where to Find More Information

Related Topics

- Understanding IP Telephony Protocols, *Cisco Unified CallManager System Guide, Release 5.0(4)*
- Understanding Cisco Unified CallManager Trunk Types, *Cisco Unified CallManager System Guide, Release 5.0(4)*
- Route Plan Overview, *Cisco Unified CallManager System Guide, Release 5.0(4)*
- Gatekeepers and Trunks, *Cisco Unified CallManager System Guide, Release 5.0(4)*
- Gateway Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Adding Gateways to Cisco Unified CallManager, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Gateway Configuration Settings, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Port Configuration Settings, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Directory Number Configuration Settings, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*

Additional Cisco Documentation

- *Cisco Unified Communications Solution Reference Network Design*
- *Configuring Cisco Unified Communications Voice Gateways*
- *Implementing Fax Over IP on Cisco Voice Gateways*
- *Cisco VG248 Analog Phone Gateway Software Configuration Guide*
- *Cisco VG248 Analog Phone Gateway Hardware Installation Guide*



Cisco Unified IP Phones

Cisco Unified IP Phones as full-featured telephones, can plug directly into your IP network. H.323 clients, CTI ports, and Cisco IP Communicator represent software-based devices that you configure similarly to the Cisco Unified IP Phones. Cisco Unified CallManager Administration allows you to configure phone features such as call forwarding and call waiting for your phone devices. You can also create phone button templates to assign a common button configuration to a large number of phones.

After you have added the phones, you can associate users with them. By associating a user with a phone, you give that user control over that device.

This section covers the following topics:

- [Supported Cisco Unified IP Phones, page 11-2](#)
- [Cisco SIP IP Phones, page 11-8](#)
- [H.323 Clients and CTI Ports, page 11-8](#)
- [Cisco IP Communicator, page 11-9](#)
- [Cisco Unified Personal Communicator, page 11-9](#)
- [Cisco TelePresence, page 11-9](#)
- [Phone Button Templates, page 11-10](#)
- [Softkey Templates, page 11-16](#)
- [Softkey Template Operation, page 11-19](#)
- [Common Phone Profiles, page 11-20](#)
- [Methods for Adding Phones, page 11-20](#)
- [Phone Features, page 11-21](#)
- [Phone Association, page 11-27](#)
- [Phone Administration Tips, page 11-27](#)
- [Phone Failover and Fallback, page 11-30](#)
- [Phone Configuration Checklist, page 11-31](#)
- [Where to Find More Information, page 11-35](#)

Supported Cisco Unified IP Phones

Table 11-1 provides an overview of the features that are available on the following Cisco Unified IP Phones that Cisco Unified CallManager supports:

- Cisco Unified IP Phone model 7900 family (SCCP and SIP protocols)
- Cisco Unified IP Video Phone model 7985
- Cisco Unified IP Phone model 7914 Expansion Module
- Cisco IP Conference Station 7935 and 7936
- Cisco IP Phone model 30 VIP
- Cisco IP Phone model 12 series

For the latest information on features and services that these phone models support, refer to the following documentation:

- Phone administration or user documentation that supports the phone model and this version of Cisco Unified CallManager
- Firmware release notes for your phone model
- Cisco Unified CallManager release notes

Table 11-1 **Supported Cisco Unified IP Phones and Features**

Cisco Unified IP Phone Model	Description
Cisco Unified IP Phone 7970 and Cisco Unified IP Phone 7971	The Cisco Unified IP Phone models 7970 and 7971, full-featured, eight-line business sets, support the SCCP and SIP protocols and the following features: • A backlit, color touchscreen display for easy access to call details and features. • Four fixed feature buttons: – Messages—Accessing voice-messaging messages – Settings—Adjusting phone settings – Services—Accessing services – Directories—Accessing call logs and directories • A Help (?) button for immediate assistance with calling features • Eight programmable buttons to use as line buttons, speed-dial buttons, or for other phone services • Five softkeys for accessing additional call details and functionality (Softkeys change depending on the call state for a total of 16 softkeys.) • An internal, two-way, full-duplex speakerphone and microphone mute The Cisco Unified IP Phone models 7970/71G-GE represent the gigabit ethernet version of the Cisco Unified IP Phone models 7970/71 while Cisco Unified IP Phone models 7970G, 7960G, and 7940G represent the non-gigabit version.

Table 11-1 **Supported Cisco Unified IP Phones and Features (continued)**

Cisco Unified IP Phone Model	Description
Cisco Unified IP Phone 7960 and Cisco Unified IP Phone 7961	The Cisco Unified IP Phone models 7960 and 7961, full-featured, six-line business sets, support the SCCP and SIP protocols and the following features: • A help (?) button • Six programmable buttons to use as line, speed-dial, or feature buttons • Four fixed buttons for accessing voice-messaging messages, adjusting phone settings, accessing services, and accessing directories • Four softkeys for accessing additional call details and functionality (Softkeys change depending on the call state for a total of 16 softkeys.) • A large LCD display that shows call details and softkey functions • An internal, two-way, full-duplex speakerphone and microphone mute
Cisco Unified IP Phone 7940 and Cisco Unified IP Phone 7941	The Cisco Unified IP Phone models 7940 and 7941, two-line business sets with features similar to the Cisco Unified IP Phone model 7960, support the SCCP and SIP protocols and include the following features: • A help (?) button • Two programmable buttons to use as line, speed-dial, or feature buttons • Four fixed buttons for accessing voice-messaging messages, services, and directories and for adjusting phone settings • Four softkeys for accessing additional call details and functionality (Softkeys change depending upon the call state for a total of 16 softkeys.) • A large LCD that shows call details and softkey functions • An internal, two-way, full-duplex speakerphone and microphone mute

Table 11-1 Supported Cisco Unified IP Phones and Features (continued)

Cisco Unified IP Phone Model	Description
Cisco Unified IP Phone 7920	The Cisco Wireless IP Phone model 7920, which is an easy-to-use IEEE 802.11b wireless IP phone, provides comprehensive voice communication in conjunction with Cisco Unified CallManager and Cisco Aironet 1200, 1100, 350, and 340 series of Wi-Fi (IEEE 802.11b) access points. Features include • A pixel-based display for intuitive access to calling features • Two softkeys that dynamically present calling options to the user • A four-way rocker switch that allows easy movement through the displayed information • Volume control for easy decibel-level adjustments of the handset and ringer when in use
Cisco Unified IP Phone 7914 Expansion Module	Cisco Unified IP Phone model 7914 Expansion Module extends the functionality of the Cisco Unified IP Phone model 7960 by providing 14 additional buttons. To configure these buttons as line or speed dials, use Phone Button Template Configuration.  Note You can create the Cisco Unified IP Phone model 7914 Expansion Module phone button template by renaming the phone button template that is used for the standard Cisco Unified IP Phone model 7960. Refer to “Phone Button Template Configuration” in the <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>, for more information. The Cisco Unified IP Phone model 7914 Expansion Module includes an LCD to identify the function of the button and the line status. You can daisy chain two Cisco Unified IP Phone model 7914 Expansion Modules to provide 28 additional lines or speed-dial and feature buttons.
Cisco Unified IP Phone 7912	The Cisco Unified IP Phone model 7912, which is a single-line phone that supports a maximum of two calls at the same time, supports the SCCP and SIP protocols and provides basic-feature functionality for individuals who conduct low to medium telephone traffic. This model, which supports inline power, provides an integrated 10/100 Ethernet switch for connectivity to a collocated PC. This model offers four dynamic softkeys.

Table 11-1 **Supported Cisco Unified IP Phones and Features (continued)**

Cisco Unified IP Phone Model	Description
Cisco Unified IP Phone 7911	The Cisco Unified IP Phone model 7911, which is a single-line phone that supports a maximum of six calls at the same time, supports the SCCP and SIP protocols and provides basic-feature functionality for individuals who conduct low to medium telephone traffic. Similarities exist between the Cisco Unified IP Phone model 7911 menus and the Cisco Unified IP Phone 7970 menus. The Applications Menu button opens up a main applications menu. This model, which supports inline power, provides an integrated 10/100 Ethernet switch for connectivity to a collocated PC. This model offers four dynamic softkeys.
Cisco Unified IP Phone 7910	The Cisco Unified IP Phone model 7910, a single-line, basic-feature phone that is designed primarily for common-use areas with medium telephone traffic such as lobbies or breakrooms, includes the following features: • Four dedicated feature buttons for Line, Hold, Transfer, and Settings • Six programmable feature buttons that you can configure through phone button templates in Cisco Unified CallManager Available features include Call Park, Redial, Speed Dial, Call Pickup, Conference, Forward All, Message Waiting, and Meet-Me Conference. • A two-line LCD (24 characters per line) that indicates the directory number, call status, date, and time • An internal speaker that is designed for hands-free dialing.
Cisco Unified IP Phone 7906	The Cisco Unified IP Phone model 7906, which is a single-line phone that supports a maximum of six calls at the same time, supports the SCCP and SIP protocols and provides basic-feature functionality for individuals who conduct low to medium telephone traffic. Similarities exist between the Cisco Unified IP Phone model 7906 menus and the Cisco Unified IP Phone 7970 menus. The Applications Menu button opens up a main applications menu. This model, which supports inline power, provides an integrated 10/100 Ethernet switch for connectivity to a collocated PC. This model offers four dynamic softkeys.

Table 11-1 **Supported Cisco Unified IP Phones and Features (continued)**

Cisco Unified IP Phone Model	Description
Cisco Unified IP Phone 7905	The Cisco Unified IP Phone model 7905, a low-cost, single-line, basic-feature phone that is designed primarily for common-use areas such as cafeterias, break rooms, lobbies, and manufacturing floors, supports the SCCP and SIP protocols and includes the following features: • LCD that displays features such as time, date, phone number, caller ID, call status, and softkey tabs • Four softkeys that engage the function that displays on the corresponding LCD tabs. (Softkey functions change depending on the status of the phone.) • Three dedicated buttons for Hold, Menu, and Navigation • An internal speaker that is designed for hands-free dialing
Cisco Unified IP Phone model 7902	The Cisco Unified IP Phone model 7902 provides a cost-effective, entry-level IP phone for a lobby, laboratory, manufacturing floor, or another area where only basic calling capability is required. The single-line Cisco Unified IP Phone model 7902 includes the following features: • Fixed feature keys that provide one-touch access to the redial, transfer, conference, and voice-messaging access features • Three dedicated buttons for hold, menu, and volume control • Inline power that allows the phone to receive power over the LAN
Cisco Unified IP Phone 7985	The Cisco Unified IP Phone model 7985G provides business-quality video over the same data network that your computer uses. The video phone provides the same softkey functionality and features as a Cisco IP telephone, which allows you to place and receive calls, put calls on hold, transfer calls, make conference calls, and so on. The Cisco Unified IP Phone model 7985G provides the following features: • Color screen • Support for up to eight line or speed-dial numbers • Context-sensitive online help for buttons and feature

Table 11-1 **Supported Cisco Unified IP Phones and Features (continued)**

Cisco Unified IP Phone Model	Description
Cisco Unified IP Conference Station 7936	The Cisco Unified IP Conference Station 7936, a full-featured, IP-based, hands-free conference station for use on desktops, in offices, and in small- to medium-sized conference rooms, includes the following features: • Three softkeys and menu navigation keys that guide a user through call features and functions including available features Call Park, Call Pickup, Group Call Pickup, Transfer, and Conference (Ad Hoc and Meet-Me). • An LCD that indicates the date and time, calling party name, calling party number, digits dialed, feature, and line status • A digitally tuned speaker and three microphones that allow conference participants to move around while speaking • Microphone mute • Ability to add external microphones to support larger rooms
Cisco IP Conference Station 7935	The Cisco IP Conference Station 7935, a full-featured, IP-based, hands-free conference station for use on desktops, in offices, and in small- to medium-sized conference rooms, includes the following features: • Three softkeys and menu navigation keys that guide a user through call features and functions Available features include Call Park, Call Pickup, Group Call Pickup, Transfer, and Conference (Ad Hoc and Meet-Me). • An LCD that indicates the date and time, calling party name, calling party number, digits dialed, feature, and line status • A digitally tuned speaker and three microphones that allow conference participants to move around while speaking • Microphone mute
Cisco IP Phone 12 SP+	The Cisco IP Phone model 12 SP+ offers many of the same features as PBX or POTS telephones. This IP phone includes the following features: • 12 programmable line and feature buttons • An LED that is associated with each of the 12 feature and line buttons to indicate feature and line status • A two-line LCD (20 characters per line) for call status and identification • An internal, two-way speakerphone and microphone mute

Table 11-1 **Supported Cisco Unified IP Phones and Features (continued)**

Cisco Unified IP Phone Model	Description
Cisco IP Phone 30 VIP	The Cisco IP Phone model 30 VIP offers many of the same features as PBX or POTS telephones. This IP phone includes the following features: • 26 programmable line and feature buttons • An LED that is associated with each of the 26 feature and line buttons to indicate feature and line status • A two-line LCD for displaying date and time, calling party name, calling party number, and digits dialed • An internal, two-way speakerphone with microphone mute • Dedicated feature buttons for Transfer, Hold, and Redial

Cisco SIP IP Phones

Cisco Unified CallManager supports the SIP protocol on the following Cisco Unified IP Phone models:

- Cisco Unified IP Phone 7970/71
- Cisco Unified IP Phone 7960/61
- Cisco Unified IP Phone 7940/41
- Cisco Unified IP Phone 7911/7906
- Cisco Unified IP Phone 7905/12

The administrator uses the Cisco Unified CallManager Administration Phone Configuration window to configure an IP phone for SCCP or SIP. If SIP is chosen, additional Cisco Unified CallManager Administration configuration windows get used to configure the SIP protocol; for example, SIP Profile Configuration. See [Table 11-6](#) for configuration requirements. For information on SIP Profiles and SIP Dial Rules, see SIP Dial Rules Configuration and SIP Profile Configuration in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

H.323 Clients and CTI Ports

Cisco Unified CallManager Administration enables you to configure software-based devices such as H.323 clients and CTI ports. Software-based Cisco Unified CallManager applications such as Cisco SoftPhone, Cisco AutoAttendant, and Cisco IP Interactive Voice Response (IVR) use CTI ports that are virtual devices.

H.323 clients include Microsoft NetMeeting devices.

You configure H.323 clients and CTI ports through the Phone Configuration window in Cisco Unified CallManager Administration like you do phones, but they often require fewer configuration settings.



Note

Cisco recommends that you do not configure CTI ports or devices that use TAPI applications in a line group.

For information on H.323 clients and shared line appearances, see the [“Shared Line Appearance” section on page 8-2](#).

For instructions on how to configure H.323 clients and CTI ports, refer to “Cisco Unified IP Phone Configuration” in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

Cisco IP Communicator

Cisco IP Communicator, a software-based application, allows users to place and receive phone calls by using their personal computers. Cisco IP Communicator depends upon the Cisco Unified CallManager call-processing system to provide telephony features and voice-over-IP capabilities.

This interaction with Cisco Unified CallManager means that Cisco IP Communicator provides the same functionality as a full-featured Cisco Unified IP Phone, while providing the portability of a desktop application. Additionally, it means that you administer Cisco IP Communicator as a phone device by using the Cisco Unified CallManager Administration Phone Configuration window.

Cisco Unified Personal Communicator

Cisco Unified Personal Communicator, a desktop software application, provides access to voice, video, document-sharing, and presence applications – all from a single, rich media interface. Cisco Unified Personal Communicator relies on the Cisco Unified CallManager call-processing system to provide telephony features and voice-over-IP capabilities.

This interaction with Cisco Unified CallManager enables Cisco Unified Personal Communicator to offer integrated softphone capabilities and control of the physical IP phone of the user. Additionally, it means you administer Cisco Unified Personal Communicator as a phone device by using the Cisco Unified CallManager Administration Phone Configuration window.

Cisco TelePresence

The Cisco TelePresence system, a visual meeting room solution that comprises endpoints, IP Telephony infrastructure technology, and user software applications, enables life-size, “you are there” video teleconferencing. The Cisco TelePresence IP Phone represents an integral part of the solution that provides the user interface for making connections to other Cisco TelePresence meeting rooms and for driving the codec, the device that manages the plasma display screens, microphones, speakers, and cameras that create the virtual meeting experience. The Cisco TelePresence IP Phone offers both standard Cisco Unified IP Phone 7970 and Cisco TelePresence meeting connection functionality. As an example, the Cisco TelePresence IP Phone user interface displays a schedule of the meetings for the day and provides softkeys that are designed to enable and enhance the teleconference connections but then can be used during the video teleconference to add audio meeting participants or to make voice calls.

For more information about Cisco TelePresence, see the following system and configuration documentation:

- *Cisco TelePresence System Administrator's Guide*
- *Cisco TelePresence Meeting User's Guide*
- *Cisco Unified CallManager and Cisco TelePresence Configuration*

Phone Button Templates

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 provide 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.

To create a template, you must make a copy of an existing template and assign the template a unique name. You can make changes to the custom templates that you created, and you can change the labels of the default phone button templates. You cannot change the function of the buttons in the default templates. You can rename existing templates and modify them to create new ones, update custom templates to add or remove features, lines, or speed dials, and delete custom templates that are no longer being used. When you update a template, the change affects all phones that use the template.

Renaming a template does not affect the phones that use that template. All Cisco Unified IP Phones that use this template continue to use this template after it is renamed.

Make sure that all phones have at least one line that is assigned to each phone. Normally, this assignment specifies button 1. Phones can have additional lines that are assigned, depending on the Cisco Unified IP Phone model. Phones also generally have several features, such as speed dial, that are assigned to the remaining buttons.

You can delete phone templates that are not currently assigned to any phone in your system if they are not the only template for a given phone model. You cannot delete a template that is assigned to one or more devices or the default template for a model (specified in the Device Defaults Configuration window). You must reassign all Cisco Unified IP Phones that are using the template that you want to delete to a different phone button template before you can delete the template.



Note

The standard phone button template for the Cisco Unified IP Phone model 7960, which supports the Cisco Unified IP Phone model 7914 Expansion Module, includes buttons for both devices (up to 34 buttons).

Choose Dependency Records from the Related Links drop-down list box on the Phone Button Template Configuration window to view the devices that are using a particular template.

Cisco Unified CallManager does not directly control all features on Cisco Unified IP Phones through phone button templates. Refer to the *Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager* and other phone documentation for detailed information about individual Cisco Unified IP Phone 7900 family models.

Default Phone Button Templates

Although all Cisco Unified IP Phones support similar features, you implement these features differently on various models. For example, some models configure features such as Hold or Transfer by using phone button templates; other models have fixed buttons or onscreen program keys for these features that are not configurable. Also, the maximum number of lines or speed dials that are supported differs for some phone models. These differences require different phone button templates for specific models.

Each Cisco Unified IP Phone model comes with a default phone button template. You can use the default templates as is to quickly configure phones. You can also copy and modify the templates to create custom templates.

Custom templates enable you to make features available on some or all phones, restrict the use of certain features to certain phones, configure a different number of lines or speed dials for some or all phones, and so on, depending on how the phone will be used. For example, you may want to create a custom template that can be applied to phones that will be used in conference rooms. [Table 11-2](#) provides descriptions of the standard phone button templates.

Table 11-2 *Default Phone Button Templates Listed by Model*

Phone Button Template Name	Template Description
Standard 7985	The Standard 7985 template uses buttons 1 and 2 for lines and assigns buttons 3 through 8 as speed dials. Access other phone features, such as call park, call forward, redial, hold, resume, voice-messaging system, conferencing, and so on, by using softkeys on the Cisco IP Video Phone 7985.
Standard 7971 SCCP	The Standard 7971 SCCP template uses buttons 1 and 2 for lines and assigns buttons 3 through 8 as speed dials. Access other phone features, such as call park, call forward, redial, hold, resume, voice-messaging system, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7971.
Standard 7971 SIP	The Standard 7971 SIP template uses buttons 1 and 2 for lines and assigns buttons 3 through 8 as speed dials. Access other phone features, such as call park, call forward, redial, hold, resume, voice-messaging system, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7971.
Standard 7970 SCCP	The Standard 7970 SCCP template uses buttons 1 and 2 for lines and assigns buttons 3 through 8 as speed dials. Access other phone features, such as call park, call forward, redial, hold, resume, voice-messaging system, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7970.
Standard 7970 SIP	The Standard 7970 SIP template uses buttons 1 and 2 for lines and assigns buttons 3 through 8 as speed dials. Access other phone features, such as call park, call forward, redial, hold, resume, voice-messaging system, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7970.
Standard 7961 SCCP and Standard 7961G-GE SCCP	The Standard 7961 SCCP template uses buttons 1 and 2 for lines and assigns buttons 3 through 6 as speed dials or lines or for the features privacy and service URL. Access other phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7961.
Standard 7961 SIP	The Standard 7961 SIP template uses buttons 1 and 2 for lines and assigns buttons 3 through 6 as speed dials or lines or for the features privacy and service URL. Access other phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7961.

Table 11-2 *Default Phone Button Templates Listed by Model (continued)*

Phone Button Template Name	Template Description
Standard 7960 SCCP	The Standard 7960 SCCP template uses buttons 1 and 2 for lines and assigns buttons 3 through 6 as speed dials or lines or for the features privacy and service URL. Access other phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7960.
Standard 7960 SIP	The Standard 7960 SIP template uses buttons 1 and 2 for lines and assigns buttons 3 through 6 as speed dials or lines or for the features privacy and service URL. Access other phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7960.
Standard 7941 SCCP and Standard 7941G-GE SCCP	The Standard 7941 SCCP template comes with a preconfigured one-line phone button template (button 1 for line 1 and button 2 for speed dial). Access phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7941.
Standard 7941 SIP	The Standard 7940 SIP template comes with a preconfigured one-line phone button template (button 1 for line 1 and button 2 for speed dial). Access phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7941.
Standard 7940 SCCP	The Standard 7940 SCCP templates comes with a preconfigured one-line phone button template (button 1 for line 1 and button 2 for speed dial). Access phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7940.
Standard 7940 SIP	The Standard 7940 SIP template comes with a preconfigured one-line phone button template (button 1 for line 1 and button 2 for speed dial). Access phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7940.
Standard 7920	The Standard 7920 template uses buttons 1 and 2 for lines and assigns buttons 3 through 6 for speed dials.
Standard 7912 SCCP	The Standard 1912 SCCP template uses button 1 for line 1, buttons 2 through 5 for speed dial, button 6 for Hold, and button 7 for Settings.
Standard 7912 SIP	The Standard 7912 SIP template uses button 1 for line 1, buttons 2 through 5 for speed dial, button 6 for Hold, and button 7 for Settings.
Standard 7911 SCCP	The Standard 7911 SCCP template uses button 1 for line 1, makes button 2 configurable as the Privacy softkey (default specifies None), and assigns buttons 3 through 6 as speed dials. The user accesses speed dials from the Directories menu or the Navigation button on the phone.

Table 11-2 *Default Phone Button Templates Listed by Model (continued)*

Phone Button Template Name	Template Description
Standard 7911 SIP	The Standard 7911 SIP template uses button 1 for line 1, makes button 2 configurable as the Privacy softkey (default specifies None), and assigns buttons 3 through 6 as speed dials. The user accesses speed dials from the Directories menu or the Navigation button on the phone.
Standard 7910	The Standard 7910 template uses button 1 for message waiting, button 2 for conference, button 3 for forwarding, buttons 4 and 5 for speed dial, and button 6 for redial. The Cisco Unified IP Phone 7910 includes fixed buttons for Line, Hold, Transfer, and Settings.
Standard 7906 SCCP	The Standard 7906 SCCP template uses button 1 for line 1, makes button 2 configurable as the Privacy softkey (default specifies None), and assigns buttons 3 through 6 as speed dials. The user accesses speed dials from the Directories menu or the Navigation button on the phone.
Standard 7906 SIP	The Standard 7906 SIP template uses button 1 for line 1, makes button 2 configurable as the Privacy softkey (default specifies None), and assigns buttons 3 through 6 as speed dials. The user accesses speed dials from the Directories menu or the Navigation button on the phone.
Standard 7905 SCCP	The Standard 7905 SCCP template uses button 1 for line 1, buttons 2 through 5 for speed dial, button 6 for Hold, and button 7 for Settings.
Standard 7905 SIP	The Standard 7905 SIP template uses button 1 for line 1, buttons 2 through 5 for speed dial, button 6 for Hold, and button 7 for Settings.
Standard 7902	The Standard 7902 template uses button 1 for line 1, buttons 2 through 5 for speed dial, button 6 for Hold, and button 7 for Settings.
Standard 7936	The Standard 7936 template, which is not configurable for the Cisco Unified IP Conference Station 7936, uses button 1 for line 1.
Standard 7935	The Standard 7935 template, which is not configurable for the Cisco IP Conference Station 7935, uses button 1 for line 1.
Standard 30 SP+	The Standard 30 SP+ template uses buttons 1 through 4 for lines, button 5 for call park, buttons 6 through 8 and 17 through 21 remain undefined, and buttons 9 through 13 and 22 through 25 apply for speed dial; button 14 applies for message-waiting indicator, button 15 for forward, and button 16 for conference. Note For only the Cisco IP Phone model 30 SP+, assign button 26 for automatic echo cancellation (AEC).
Standard 30 VIP	The Standard 30 VIP template uses buttons 1 through 4 for lines, button 5 for call park, buttons 6 through 13 and 22 through 26 for speed dial, button 14 for message-waiting indicator, button 15 for call forward, and button 16 for conference.

Table 11-2 *Default Phone Button Templates Listed by Model (continued)*

Phone Button Template Name	Template Description
Standard 12 Series, including the 12 S, 12 SP, and 12 SP+	The Standard 12 S, Standard 12 SP, and Standard 12 SP+ templates use buttons 1 and 2 for lines, button 3 for redial, buttons 4 through 6 for speed dial, button 7 for hold, button 8 for transfer, button 9 for forwarding, button 10 for call park, button 11 for message waiting, and button 12 for conference.
Standard VGC Phone	The Standard VGC Phone template for the Cisco VG248 Gateway uses button 1 for a line and buttons 2 through 10 for speed dials.
Default VGC Virtual Phone	The Default VGC Virtual Phone template for the Cisco VGC Virtual Phone uses button 1 for line 1.
Standard ATA 186	The Standard ATA 186 template uses button 1 for a line and buttons 2 through 10 for speed dials.
ISDN BRI Phone	The ISDN BRI Phone template uses button 1 for line 1.
Default IP Communicator	The Default IP Communicator template uses buttons 1 and 2 for lines and assigns buttons 3 through 8 as speed dials. Access other phone features, such as call park, call forward, redial, hold, resume, voice-messaging system, conferencing, and so on, by using softkeys (by configuring the softkey template to the phone).
Standard IP-STE	The Standard IP-STE template uses buttons 1 and 2 for lines.
Standard Analog	The Standard Analog template for analog phones uses button 1 for line 1.
Third-Party SIP Device (Advanced)	The Generic SIP Phone - 2 Lines template, which is used for third-party SIP phones, uses buttons 1 and 2 for lines.
Third-Party SIP Device (Basic)	The Generic SIP Phone - 2 Lines template, which is used for third-party SIP phones, uses buttons 1 and 2 for lines.
StandardCN622	The StandardCN622 template, used for the Static SIP Mobile Subscriber, uses buttons 1 through 6 for lines.
Standard Cisco TelePresence	The Standard Cisco TelePresence template, required by Cisco TelePresence, uses buttons 1 and 2 for lines and buttons 3 through 42 for speed dials.

Guidelines for Customizing Phone Button Templates

Use the following guidelines when you are creating custom phone button templates:

- Make sure that phone users receive a quick reference card or getting started guide that describes the most basic features of the custom template. If you create a custom template for employees in your company to use, make sure that it includes the following features and that you describe them on the quick reference card that you create for your users:
 - Cisco Unified IP Phone 7970/71, 7960/61, 7940/41, 7911, 7906—Line (one or more)
 - Cisco Unified IP Phone 7912—Line, speed dial, hold, and settings
 - Cisco Unified IP Phone 7910—Forward all
 - Cisco Unified IP Phone 7905 and 7902—Line, speed dial, hold, and settings
 - Cisco Wireless IP Phone 7920—Line (one or more)

- Cisco IP Phone model 12 SP+—Line (one or more), hold, call park, and forward all
- Cisco IP Phone model 30 VIP—Line (one or more), call park, and forward all
- Cisco VGC Virtual Phone and Cisco ATA 186—Line and speed dials
- Consider the nature of each feature to determine how to configure your phone button template. You may want to assign multiple buttons to speed dial and line; however, you usually require only one of the other phone button features that are described in [Table 11-3](#).

Table 11-3 Phone Button Feature Description

Feature	Description
AEC	If you are configuring a template for the Cisco IP Phone model 30 VIP, you must include one occurrence of this feature and assign it to button 26. Auto echo cancellation (AEC) reduces the amount of feedback that the called party receives when the calling party is using a speakerphone. Users should press the AEC button on a Cisco IP Phone model 30 SP+ when they are using speakerphone. Users do not need to press this button when speakerphone is not in use. This feature requires no configuration for it to work.
Answer/release	In conjunction with a headset apparatus, the user can press a button on the headset apparatus to answer and release (disconnect) calls.
Auto answer	If this feature is programmed on the template, pressing this button causes the speakerphone to go off hook automatically when an incoming call is received. Note You configure this feature for some phones models by using the Phone Button Template window, and you configure this feature for some phone models by using the Phone Configuration window.
Call park	In conjunction with a call park number or range, when the user presses this button, call park places the call at a directory number for later retrieval. You must have a call park number or range that is configured in the system for this button to work, and you should provide that number or range to your users, so they can dial in to the number(s) to retrieve calls.
Conference	Users can initiate an ad hoc conference and add participants by pressing the Conference button. (Users can also use the Join softkey to initiate an ad hoc conference.) Only the person who initiates an ad hoc conference needs a conference button. You must make sure that an ad hoc conference bridge device is configured in Cisco Unified CallManager Administration for this button to work. Refer to the “Conference Bridges” chapter of the <i>Cisco Unified CallManager System Guide, Release 5.0(4)</i>, for more information.
Forward all	Users press this button to forward all calls to the designated directory number. Users can designate forward all in the Cisco Unified IP Phone Configuration windows, or you can designate a forward all number for each user in Cisco Unified CallManager Administration.

Table 11-3 Phone Button Feature Description (continued)

Feature	Description
Hold	Users press this button to place an active call on hold. To retrieve a call on hold, users press the flashing line button or lift the handset and press the flashing line button for the call on hold. The caller on hold receives a tone every 10 seconds to indicate the hold status or music (if the Music On Hold feature is configured). The hold tone feature requires no configuration to work.
Line	Users press this button to dial a number or to answer an incoming call. For this button to work, you must have added directory numbers on the user phone.
Meet-Me conference	When users press this button, they initiate a meet-me conference, and they expect other invited users to dial in to the conference. Only the person who initiates a meet-me conference needs a meet-me button. You must make sure that a meet-me conference device is configured in Cisco Unified CallManager Administration for this button to work.
Message waiting	Users press this button to connect to the voice-messaging system.
None	Use None to leave a button unassigned.
Redial	Users press this button to redial the last number that was dialed on the Cisco Unified IP Phone. This feature requires no configuration to work.
Privacy	Users press this button to activate/deactivate privacy.
Service URL	Users press this button to access a Cisco Unified IP Phone Service such as personal fast dials, stock quotes, or weather.
Speed-dial	Users press this button to speed dial a specified number. System administrators can designate speed-dial numbers in Cisco Unified CallManager Administration. Users can designate speed-dial numbers in the Cisco Unified IP Phone User Options Menu.
BLF/SpeedDial	Users monitor this button for the real-time status of the associated directory number or SIP URI on those devices that support the presence feature. Users press this button to dial the destination.
Transfer	Users press this button to transfer an active call to another directory number. This feature requires no configuration to work.

Softkey Templates

Use softkey templates to manage softkeys that are associated with applications such as Cisco Unified CallManager Assistant or call-processing features such as Cisco Call Back on the Cisco Unified IP Phones. The administrator uses the Softkey Template Configuration windows in Cisco Unified CallManager Administration to create and update softkey templates.

Cisco Unified CallManager supports two types of softkey templates: standard and nonstandard. Standard softkey templates in the Cisco Unified CallManager database contain the recommended selection and positioning of the softkeys for an application. Cisco Unified CallManager provides the following standard softkey templates:

- Standard User
- Standard Feature
- Standard Assistant
- Standard Shared Mode Manager
- Standard Manager

**Note**

The default process does not assign a softkey template to the Cisco Unified IP Phone. The administrator must assign standard or nonstandard softkey templates to the Cisco Unified IP Phone by assigning the templates individually to each phone or by assigning the device pool to each phone.

The administrator creates a nonstandard softkey template by using the Softkey Template Configuration windows in Cisco Unified CallManager Administration. To create a nonstandard softkey template, the administrator copies a standard softkey template and makes changes. The administrator can add and remove applications that are associated with any nonstandard softkey template. Additionally, the administrator can configure softkey sets for each call state for a nonstandard softkey template.

The Softkey Template Configuration window lists the standard and nonstandard softkey templates and uses different icons to differentiate between standard and nonstandard templates.

The administrator assigns softkey templates in the following Cisco Unified CallManager Administration configuration windows:

- Device Pool Configuration
- Phone Configuration (SIP and SCCP)
- User Device Profile Configuration
- Default Device Profile Configuration

Add Application

The administrator can add a standard softkey template that is associated with a Cisco application to a nonstandard softkey template. When the administrator clicks the Add Application button from the Softkey Template Configuration window, a separate window displays and allows the administrator to choose the standard softkey template that is to be added to the end of the nonstandard softkey template. Duplicate softkeys get deleted from the end of the set that is moving to the front of the set.

**Tip**

To refresh the softkeys for an application in the nonstandard softkey template, choose the standard softkey template that is already associated with the nonstandard softkey template. For example, if the administrator originally copied the Standard User template and deleted some buttons, choose the Standard User softkey template by clicking on the Add Application button. This adds the buttons that are included in the chosen softkey template.

The number of softkeys in any given call state cannot exceed 16. A message displays, and the add application procedure stops when the maximum number of softkeys is reached. The administrator must manually remove some softkeys from the call state before trying to add another application to the template.

The Delete Application button allows the administrator to delete application softkey templates that are associated with a nonstandard softkey template. Only the softkeys that are associated with the application get deleted. When softkeys are commonly shared between applications, they remain in the softkey template until the last application that shares the softkeys is removed from the softkey template.

Configure Softkey Layout

The administrator can configure softkey sets for each call state for a nonstandard softkey template. When the administrator chooses Configure Softkey Layout from the Related Links drop-down list box on the Softkey Template Configuration window and clicks **Go**, Softkey Layout Configuration displays.

The Softkey Layout Configuration pane contains the following fields:

- **Call states**—This drop-down list box displays the different call states of a Cisco Unified IP Phone. You cannot add, update, or delete call states. The call state that gets chosen from the drop-down list box indicates the softkeys that are available for that call state. [Table 11-4](#) lists the call states.

Table 11-4 **Call States**

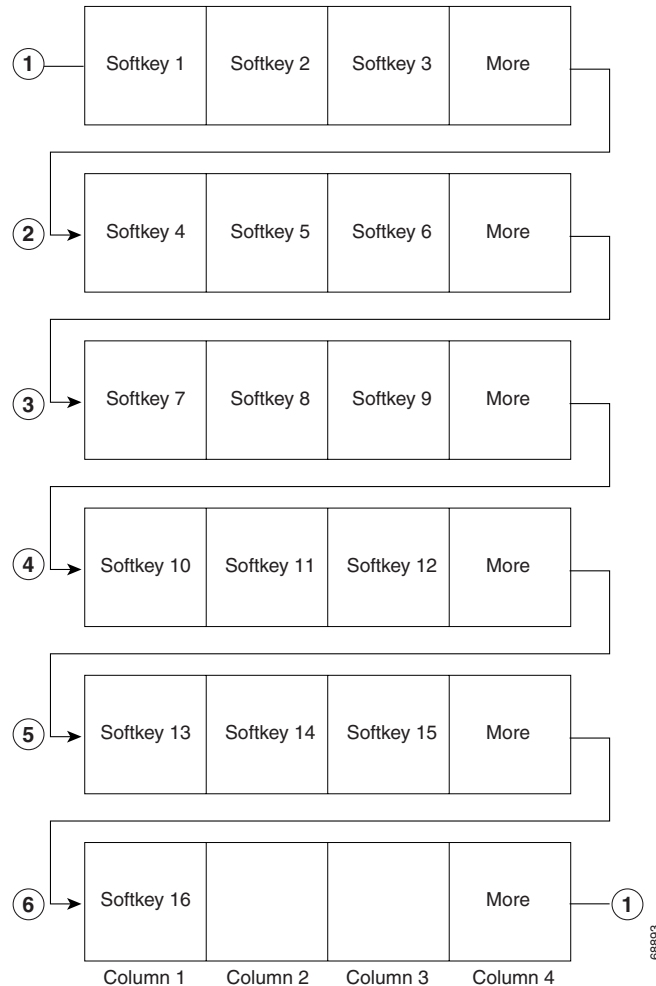
Call State	Description
Connected	Displays when call is connected
Connected Conference	Consultation call for conference in connected call state
Connected Transfer	Consultation call for transfer in connected call state
Digits After First	Off-hook call state after user enters the first digit
Off Hook	Dial tone presented to phone
Off Hook With Feature	Off-hook call state for transfer or conference consultation call
On Hold	Call on hold
On Hook	No call exists for that phone.
Remote In Use	Another device that shares the same line uses call.
Ring In	Call received and ringing
Ring Out	Call initiated and the destination ringing

- **Unselected Softkeys**—Lists softkeys that are associated with a call state. This field lists the unselected, optional softkeys of the call state that displays in the Select a Call State to Configure drop-down list box. The softkeys that are listed in this field get added to the Selected Softkeys field by using the right arrows. You can add the Undefined softkey more than once to the Selected Softkey list. Choosing Undefined results in a blank softkey on the Cisco Unified IP Phone.
- **Selected Softkeys**—Lists softkeys that are associated with the chosen call state. This field lists the chosen softkeys of the call state that displays in the Select a Call State to Configure drop-down list box. The maximum number of softkeys in this field cannot exceed 16. See [Figure 11-1](#) for a sample softkey layout.

**Note**

Cisco recommends that a softkey remain in the same position for each call state. This provides the user with consistency and ease of use; for example, the More softkey always appears in the fourth softkey position from the left for each call state.

Figure 11-1 Sample Softkey Layout



Softkey Template Operation

For applications such as Cisco Unified CallManager Assistant to support softkeys, ensure softkeys and softkey sets are configured in the database for each device that uses the application.

You can mix application and call-processing softkeys in any softkey template. A static softkey template associates with a device in the database. When a device registers with Cisco Unified CallManager, the static softkey template gets read from the database into call processing and then gets passed to the device to be used throughout the session (until the device is no longer registered or is reset). When a device resets, it may get a different softkey template or softkey layout because of updates that the administrator makes.

Softkeys support a field called application ID. An application, such as Cisco Unified CallManager Assistant, activates/deactivates application softkeys by sending a request to the device through the Cisco CTIManager and call processing with a specific application ID.

When a user logs in to the Cisco IP Manager Assistant service and chooses an assistant for the service, the application sends a request to the device, through Cisco CTIManager and call processing, to activate all its softkeys with its application ID.

At any time, several softkey sets may display on a Cisco Unified IP Phone (one set of softkeys for each call).

The softkey template that is associated with a device (such as a Cisco Unified IP Phone) in the database designates the one that is used when the device registers with call processing. Perform the association of softkey templates and devices by using Softkey Template configuration in Cisco Unified CallManager Administration. See “Softkey Template Configuration” in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

Common Phone Profiles

Cisco Unified CallManager uses common phone profiles to define phone attributes that are associated with Cisco Unified IP Phones. Having these attributes in a profile instead of adding them individually to every phone decreases the amount of time that administrators spend configuring phones and allows the administrator to change the values for a group of phones. Common phone profiles specify the following attributes:

- Profile name
- Profile description
- Local phone unlock password
- End user access to phone background image setting

The common phone profile remains a required field when phones are configured; therefore, you must create the common phone profile before you create a phone. Cisco Unified CallManager provides a Standard Common Phone Profile that you can copy and modify to create a new common phone profile. You cannot, however, modify nor delete the Standard Common Phone Profile.

For information on configuring common phone profiles, see “Common Phone Profile Configuration” in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

Methods for Adding Phones

You can automatically add phones that support either the SCCP or SIP protocols to the Cisco Unified CallManager database by using autoregistration, manually by using the phone configuration windows, or in groups with the Bulk Administration Tool (BAT).

By enabling autoregistration before you begin installing phones, 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. For information on enabling autoregistration, refer to “Enabling Autoregistration” in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*. During autoregistration, Cisco Unified CallManager assigns the next available sequential directory number to the phone. In many cases, you may not want to use autoregistration; for example, if you want to assign a specific directory number to a phone or if you plan to implement authentication or encryption, as described in the *Cisco Unified CallManager Security Guide*.

**Tip**

Cisco Unified CallManager automatically disables autoregistration if you configure the clusterwide security mode for authentication and encryption through the Cisco CTL client.

If you do not use autoregistration, you must manually add phones to the Cisco Unified CallManager database or use the Bulk Administration Tool (BAT). BAT enables system administrators to perform batch add, modify, and delete operations on large numbers of Cisco Unified IP Phones. Refer to the *Cisco Unified CallManager Bulk Administration Guide* for detailed instructions on using BAT.

User/Phone Add

You can use the End User, Phone, DN, and LA Configuration window to add a new phone at the same time that you add a new end user. You can associate a directory number (DN) and line appearance (LA) for the new end user by using the same window. To access the End User, Phone, DN, and LA Configuration window, choose the **User Management > User/Phone Add** menu option. See “User/Phone Add Configuration” in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*, for configuration details.

**Note**

The End User, Phone, DN, and LA Configuration window only allows addition of a new end user and a new phone. The window does not allow entry of existing end users or existing phones.

Phone Features

Cisco Unified CallManager enables you to configure the following phone features on Cisco Unified IP Phones: barge, privacy release, call back, call park, call pickup, immediate divert, malicious call identification, quality report tool, service URL, and speed dial and abbreviated dial.

For information about features that are related to directory numbers, see the “[Directory Number Features](#)” section on page 8-5. The following features get configured for directory numbers: call forward and call waiting.

Barge and Privacy

The Barge and Privacy features work together. Both features work with shared lines only.

Barge adds a user to a call that is in progress. Pressing the Barge or cBarge softkey automatically adds the user (initiator) to the shared-line call (target), and the users currently on the call receive a tone. Barge supports built-in conference and shared conference bridges.

Privacy allows a user to allow or disallow other users of shared-line devices to view the device call information or to allow another user to barge in to its active calls.

For more information about Barge and Privacy, refer to Barge and Privacy in the *Cisco Unified CallManager Features and Services Guide, Release 5.0(4)*.

Call Forward

Call forward allows a user to configure a Cisco Unified IP Phone, so all calls that are destined for it ring another phone. The following types of call forward exist:

- Call forward all—Forwards all calls.
- Call forward busy—Forwards calls only when the line is in use and busy trigger setting is reached.

- Call forward no answer—Forwards calls when the phone is not answered after the configured no answer ring duration or if the destination is unregistered.
- Call forward no coverage—Forward calls when ringing either exhausts or times out and the associated hunt-pilot for coverage specifies Use Personal Preferences for its final forwarding.

You can configure each call forward type for internal and external calls and can forward calls to voice-messaging system or a dialed destination number by configuring the calling search space.

Cisco Unified CallManager includes a secondary Calling Search Space (CSS) configuration field for Call Forward All (CFA). The secondary CSS for CFA combines with the existing CSS for CFA to allow support of the alternate CSS system configuration. When CFA is activated, only the primary and secondary CSS for CFA gets used to validate the CFA destination and redirect the call to the CFA destination. If these fields are empty, the null CSS gets used. Only the CSS fields that are configured in the primary CSS for CFA and secondary CSS for CFA fields get used. If CFA is activated from the phone, the CFA destination gets validated by using the CSS for CFA and the secondary CSS for CFA, and the CFA destination gets written to the database. When a CFA is activated, the CFA destination always gets validated against the CSS for CFA and the secondary CSS for CFA.

The administrator configures call forward information display options to the original dialed number or the redirected dialed number, or both. The administrator enables or disables the calling line ID (CLID) and calling name ID (CNID). The display option gets configured for each line appearance.

The call forward busy trigger gets configured for each line appearance in a cluster and cannot exceed the maximum number of calls that are configured for a line appearance. The call forward busy trigger determines how many active calls exist on a line before the call forward busy setting gets activated (for example, 10 calls).

The call forward no answer ring duration gets configured for each line appearance in a cluster, and the default specifies 12 seconds. The call forward no answer ring duration determines how long a phone rings before the call forward no answer setting gets activated.

**Tip**

Keep the busy trigger slightly lower than the maximum number of calls, so users can make outgoing calls and perform transfers.

Configure call forward in the Directory Number Configuration window in Cisco Unified CallManager Administration.

Cisco Unified CallManager provides a service parameter (CFA Destination Override) that allows the administrator to override Call Forward All (CFA) when the target of the CFA calls the initiator of the CFA, so the CFA target can reach the initiator for important calls. In other words, when the user to whom calls are being forwarded (the target) calls the user whose calls are being forwarded (the initiator), the phone of the initiator rings instead of the call being forwarded back to the target. The override works whether the CFA target phone number is internal or external.

When the CFA Destination Override service parameter is set to False (the default value), no override occurs. Ensure the service parameter is set to True for CFA override to work. See “Service Parameters Configuration” in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*, for information about configuring service parameters.

**Note**

CFA override only takes place if the CFA destination matches the calling party and the CFA Destination Override service parameter is set to True. If the service parameter is set to True and the calling party does not match the CFA destination, CFA override does not take place, and the CFA remains in effect.

Call Park

Call park allows a user to place a call on hold, so anyone who is configured to use call park on the Cisco Unified CallManager system can retrieve it.

For example, if a user is on an active call at extension 1000, the user can park the call to a call park extension such as 1234, and another user can dial 1234 to retrieve the call.

To use call park, you must add the call park extension (in this case, 1234) in Cisco Unified CallManager Administration when you are configuring phone features. For more information about call park, refer to “Call Park” in the *Cisco Unified CallManager Features and Services Guide, Release 5.0(4)*.

Call Pickup

Cisco Unified CallManager provides the following types of call pickup:

- Call pickup—Allows you to answer a ringing phone in your designated call pickup group.
- Group call pickup—Allows you to answer incoming calls in another pickup group.
- Other group call pickup—Allows you to answer incoming calls in a pickup group that is associated with your own group.

All three types of call pickup can operate automatically or manually. If the service parameter, `AutoCallPickupEnabled`, is enabled, the Cisco Unified CallManager automatically connects you to the incoming call after you press one of the following softkeys on the phone:

- Pickup—For call pickup (calls in your own pickup group)
- GPickup—For group call pickup (calls in another pickup group)
- OPickup—For other group call pickup (calls in a pickup group that is associated with your own pickup group)

After the call pickup feature is automated, you need to use only one keystroke for a call connection except for group call pickup. You dial the DN of that other pickup group after you press the GPickup softkey on the phone.



Note

CTI applications support monitoring of the party whose call is picked up. CTI applications do not support monitoring of the pickup requester or the destination of the call that is picked up. Hence, Cisco Unified CallManager Assistant does not support auto call pickup (one-touch call pickup).

You configure the call pickup feature when you are configuring phone features in Cisco Unified CallManager.

When you are adding a line, you can indicate the call pickup group. The call pickup group indicates a number that can be dialed to answer calls to this directory number (in the specified partition). For more information about call pickup, refer to “Call Pickup Group” in the *Cisco Unified CallManager Features and Services Guide, Release 5.0(4)*.

Call Select

The Select softkey allows a user to select a call for feature activation or to lock the call from other devices that share the same line appearance. Pressing the Select softkey on a selected call deselects the call.

When the call gets selected by a device, it gets put in the Remote-In-Use state on all other devices that share the line appearance. No one can select a call that is in the Remote-In-Use state. In other words, selecting a call instance will lock it from other devices that share the same line appearance.

A special display symbol identifies selected calls.

Conference List

The conference list feature provides a list of participant directory numbers that are in an ad hoc conference. The name of the participant displays if it is configured in Cisco Unified CallManager Administration.

Any participant can invoke the conference list feature on the phone and can view the participants. The conference controller can invoke the conference list feature and can view and remove any participant in the conference by using the Remove softkey.

Direct Transfer

Using the DirTrfr and Select softkeys, a user can transfer any two established calls to remove the calls from the IP phone. For more information about Direct Transfer, see the [“Making and Receiving Multiple Calls Per Directory Number”](#) section on page 8-7.

Onhook Call Transfer

The Call Transfer feature supports the onhook (hangup) action as a possible last step to complete a call transfer. You must set the Transfer On-hook Enabled service parameter, which enables onhook call transfer, to True for onhook call transfer to succeed. If the service parameter is set to False, the onhook action ends the secondary call to the third party.

In the existing implementation, if user B has an active call on a particular line (from user A) and user B has not reached the maximum number of calls on this line, the Cisco Unified IP Phone provides a Transfer softkey to user B. If user B presses the Transfer softkey (or Transfer button, if available) once, user B receives dial tone and can make a secondary call: user B dials the number of a third-party (user C). Cisco Unified CallManager provides a Transfer softkey to user B again. If user B presses the Transfer softkey again (or Transfer button, if available), the transfer operation completes.

With the onhook call transfer implementation, user B can hang up after dialing the number of user C, and the transfer completes. Both the existing and new implementations work in the case of a blind transfer (user B disconnects before user C answers) and also in the case of a consult transfer (user B waits for user C to answer and announces the call from user A).

The previous implementation remains unchanged: user B can press the Transfer softkey twice to complete the transfer.

Immediate Divert

The Immediate Divert feature allows the invoker to immediately divert a call to a voice-messaging system. Managers and assistants, or anyone who shares lines, use this feature. When the call gets diverted, the line becomes available to make or receive new calls.

If the Use Legacy iDivert service parameter is set to False, the invoker can select a party voice mailbox to which to divert an incoming call. The invoker can choose between the original called party voice mailbox or the voice mailbox of the invoker.

To access the Immediate Divert feature, use the iDivert softkey. Configure this softkey by using the Softkey Template Configuration window of Cisco Unified CallManager Administration. The softkey template gets assigned to phones that are in the Cisco Unified CallManager system.

For more information about Immediate Divert, refer to the [Immediate Divert](#) chapter of this document.

Join

By using the Join softkey, a user can join up to 15 established calls (for a total of 16) to create a conference. For more information about Join, see the [“Making and Receiving Multiple Calls Per Directory Number”](#) section on page 8-7.

Malicious Call Identification (MCID)

The MCID feature provides a useful method for tracking troublesome or threatening calls. When a user receives this type of call, the Cisco Unified CallManager system administrator can assign a new softkey template that adds the Malicious Call softkey to the user phone. For POTS phones that are connected to a SCCP gateway, users can use a hookflash and enter a feature code of *39 to invoke the MCID feature.

For more information about MCID, refer to the “Malicious Call Identification” chapter in the *Cisco Unified CallManager Features and Services Guide, Release 5.0(4)*.

Quality Report Tool

The Quality Report Tool (QRT), a voice-quality and general problem-reporting tool for Cisco Unified IP Phones, allows users to easily and accurately report audio and other general problems with their IP phone. QRT gets loaded as part of the Cisco Unified CallManager installation, and the Cisco Extended Functions (CEF) service supports it.

As system administrator, you enable QRT functionality by creating, configuring, and assigning a softkey template to associate the QRT softkey on a user IP phone. You can choose from two different user modes, depending upon the level of user interaction that you want with QRT. You then define how the feature will work in your system by configuring system parameters and setting up Cisco Unified CallManager Serviceability tools. You can create, customize, and view phone problem reports by using the QRT Viewer application.

Support for the QRT feature extends to any model IP phone that includes the following capabilities:

- Support for softkey templates
- Support for IP phone services
- Controllable by CTI
- Contains an internal HTTP server



Note

For more information, refer to the following URL for the appropriate Cisco Unified IP Phone guide for your phone model:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm.

When users experience problems with their IP phones, they can report the type of problem and other relevant statistics by pressing the QRT softkey on the Cisco Unified IP Phone during one of the following call states:

- Connected
- Connected Conference
- Connected Transfer
- On Hook

From a supported call state, and using the appropriate problem classification category, a user can then choose the reason code that best describes the problem that is being reported for the IP phone. A customized phone problem report provides you with the specific information.

For detailed information about configuring and using the Quality Report Tool feature, refer to “Quality Report Tool” in the *Cisco Unified CallManager Features and Services Guide, Release 5.0(4)*. For more information about configuring and using the QRT Viewer, refer to the *Cisco Unified CallManager Serviceability Administration Guide*.

For information about the user interface, refer to the appropriate Cisco Unified IP Phone Guide for your model IP phone and the *Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager*.

Call Diagnostics and Voice-Quality Metrics

You can configure Cisco Unified IP Phones to collect call diagnostics and voice-quality metrics by setting a service parameter in Cisco Unified CallManager Administration as described in the following steps:

1. From Cisco Unified CallManager Administration, choose **System > Service Parameters**.
2. In Clusterwide Parameters (Device - General), locate the Call Diagnostics Enabled service parameter.
3. From the drop-down list box, choose one of the following states:
 - Enabled Only When CDR Enabled Flag is True
 - Enabled Regardless of CDR Enabled Flag
4. Click **Save**.

For more information about configuring service parameters in Cisco Unified CallManager Administration, refer to “Service Parameters Configuration” in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*. For information on configuring Cisco Unified IP Phones in Cisco Unified CallManager Administration, refer to “Cisco Unified IP Phone Configuration” in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*. For information on configuring the Cisco Unified IP Phones for which call diagnostics and voice-quality metrics are available, refer to the Cisco Unified IP Phone user and administration documentation.

Service URL

You can also configure a Cisco Unified IP Phone Service URL, such as the extension mobility service, to a phone button. When the button gets pressed, the service gets invoked.

To configure a service URL on a phone button for the user, the administrator performs the following steps:

1. Using Cisco Unified IP Phone Services Configuration, create a service.
2. Using Phone Button Configuration, create a custom phone button template to include the service URL feature.
3. Using Phone Configuration, add the custom phone button template to each phone that requires the service URL button.
4. Using Phone Configuration, subscribe to each appropriate service.
5. Using Phone Configuration, add the service URL button.
6. Notify the users to configure services for their phone by using the Add/Update your Service URL Buttons link on the User Options Menu.

Speed Dial and Abbreviated Dial

Cisco Unified CallManager supports the configuration of up to 99 speed-dial entries, which are accessed through phone buttons and abbreviated dialing.

When the user configures up to 99 speed-dial entries, part of the speed-dial entries can get assigned to the speed-dial buttons on the IP phone; the remaining speed-dial entries get used for abbreviated dialing. When a user starts dialing digits, the AbbrDial softkey displays, and the user can access any speed-dial entry by entering the appropriate index. For information about configuring speed dials, see “Configuring Speed-Dial Buttons” in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

Phone Association

Users can control some devices, such as phones. Applications that are identified as users control other devices, such as CTI ports. When users have control of a phone, they can control certain settings for that phone, such as speed dial and call forwarding. For more information on associating phones with users, refer to the “Associating Devices to an End User” section in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

Phone Administration Tips

The following sections contain information that may help you configure phones in Cisco Unified CallManager Administration.

Phone Search

The following sections describe how to modify your search to locate a phone. If you have thousands of Cisco Unified IP Phones in your network, you may need to limit your search to find the phone that you want. If you are unable to locate a phone, you may need to expand your search to include more phones.

**Note**

Be aware that the phone search is not case sensitive.

Searching by Device Name

When you enter the MAC address of the device in the MAC Address field when you are adding the phone, you can search by using that value as the Device Name in the Find and List Phones window.

Searching by Description

If you enter a user name and/or extension in the Description field when you are adding the phone, you can search by using that value in the Find and List Phones window.

Searching by Directory Number

To search for a phone by its directory number (DN), choose Directory Number. Choose a search criterion (such as begins with or ends with) and either choose a directory number from the drop-down list box below the **Find** button or enter a search string. Click the **Find** button to perform the search.

**Note**

Some directory numbers do not associate with phones. To search for those directory numbers, which are called unassigned DN, use the Route Plan Report window or use the Directory Number Configuration Find/List window.

Searching by Calling Search Space

If you choose calling search space, the options that are available in the database display; you can choose one of these options from the drop-down list box below the **Find** button.

Searching by Device Pool

If you choose device pool, the options that are available in the database display (for example, Default); you can choose one of these options from the drop-down list box below the **Find** button.

Searching by Device Type

To search for a phone by its device type, choose Device Type and either enter a device type or choose a device type from the drop-down list box below the **Find** button.

Searching by Call Pickup Group

To search for a phone by its call pickup group, choose Call Pickup Group. If you choose Call Pickup Group, the options that are available in the database display; you can choose one of these options from the drop-down list box below the **Find** button. Alternatively, click the **Find** button only.

Searching by LSC Status

If you choose LSC status, the options that are available in the database display (for example, Operation Pending); you can choose one of these options from the drop-down list box below the **Find** button.

Searching by Authentication String

To search for a phone by an authentication string, choose Authentication String and enter an authentication string.

Searching by Device Protocol

To search for a phone by the protocol, choose Device Protocol and either enter a protocol, such as SIP, or choose a protocol from the drop-down list box below the **Find** button.

Searching by Security Profile

To search for a phone by its security profile, choose Security Profile and either enter a security profile name or choose a security profile from the drop-down list box below the **Find** button.

Search Within Results

To refine your search results, you can search for additional information. For example, if you search for phones by the device protocol, you may want to search within the device protocol results for phones that belong to a specific device pool. After you perform an initial search, check the Search Within Results check box. You can enter additional, or different, search criteria in the drop-down list boxes. Click **Find** again to search within the previous results.

Finding All Phones in the Database

To find all phones that are registered in the database, choose Device Name from the list of fields; choose “is not empty” from the list of patterns; then, click the Find button.



Note

The list in the Find and List Phones window does not include analog phones and fax machines that are connected to gateways (such as a Cisco VG200). This list shows only phones that are configured in Cisco Unified CallManager Administration.

Messages Button

By performing the following actions, you can configure a voice-messaging access number for the messages button on Cisco Unified IP Phone models 7970, 7960, and 7940, so users can access the voice-messaging system by simply pressing the messages button:

1. Configure the voice-mail pilot number by choosing **Voice Mail > Voice Mail Pilot**.
2. Configure the voice-mail profile by choosing **Voice Mail > Voice Mail Profile**.

3. Choose the appropriate profile from the Voice Mail Profile field on the Directory Number Configuration window. By default, this field uses the default voice-mail profile that uses the default voice-mail pilot number configuration.

**Note**

Typically, you can edit the default voice-mail pilot and default voice-mail profiles to configure voice-messaging service for your site.

For more information on configuring a voice-messaging service, refer to the “Voice Mail Connectivity to Cisco Unified CallManager” chapter in the *Cisco Unified CallManager System Guide, Release 5.0(4)*.

**Note**

For the Cisco IP Phone models 12 SP+ and 30 VIP, you can use phone button templates to configure a button with the message-waiting feature for access to a voice-messaging service.

Directories Button

The Cisco Unified IP Phone models 7970, 7960, and 7940 can display a directory of employee names and phone numbers. Although you access this directory from the directories button on the IP phone, you must configure it before users can access it. To use the corporate directory, you must enter users into a Lightweight Directory Access Protocol (LDAP) directory that is configured with Cisco Unified CallManager.

The URL Directories enterprise parameter defines the URL that points to the global directory for display on Cisco Unified IP Phone models 7970, 7960, and 7940. The XML device configuration file for the phone stores this URL.

**Tip**

If you are using IP addresses rather than DNS for name resolution, make sure that the URL Directories enterprise parameter value uses the IP address of the server for the hostname.

If the phone URL was not updated correctly after the URL Directories enterprise parameter was changed, try stopping and restarting the Cisco TFTP service; then, reset the phone.

Cisco Unified CallManager User Options

Cisco Unified IP Phone users access Cisco Unified CallManager User Options through their web browser, so they can configure a variety of features on their phone. Some of the configurable features include user locale, user password, call forward, speed dial, and personal address book. By setting enterprise parameters as either True or False, administrators can configure which features are made available to users; for example, the administrator can set the Show Speed Dial Settings enterprise parameter to False, and users cannot configure speed dials on their phones.

For more information on how to access and use Cisco Unified CallManager User Options, refer to the phone guide for the specific Cisco Unified IP Phone.

Maximum Phone Fallback Queue Depth Service Parameter

The Cisco CallManager service uses the Maximum Phone Fallback Queue Depth service parameter to control the number of phones to queue on the higher priority Cisco Unified CallManager when that Cisco Unified CallManager is available for registration. The default specifies 10 phones per second. If a primary Cisco Unified CallManager fails, the phones fail over to the secondary Cisco Unified CallManager. The failover process happens as fast as possible by using the priority queues to regulate the number of devices that are currently registering.

When the primary Cisco Unified CallManager recovers, the phones get returned to that Cisco Unified CallManager; however, you do not need to remove a phone from a working Cisco Unified CallManager, in this case the secondary system, as fast as possible because the phone remains on a working system. The queue depth gets monitored (using the Maximum Phone Fallback Queue Depth service parameter setting) to determine whether the phone that is requesting registration gets registered now or later. If the queue depth is greater than 10 (default), the phone stays where it is and tries later to register to the primary Cisco Unified CallManager.

In the Service Parameters Configuration window, you can modify the Maximum Phone Fallback Queue Depth service parameter. If the performance value is set too high (the maximum setting specifies 500), phone registrations could slow the Cisco Unified CallManager real-time response. If the value is set too low (the minimum setting specifies 1), the total time for a large group of phones to return to the primary Cisco Unified CallManager will be long.

Dependency Records

If you need to find what directory numbers a specific phone is using or to what phones a directory number is assigned, choose Dependency Records from the Related Links drop-down list box on the Cisco Unified CallManager Administration Phone Configuration or Directory Number Configuration window. The Dependency Records Summary window displays information about directory numbers that are using the phone. To find more information about the directory number, click the directory number, and the Dependency Records Details window displays. 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 and the “Removing a Directory Number from a Phone” section in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

Phone Failover and Fallback

This section describes how phones fail over and fall back if the Cisco Unified CallManager to which they are registered becomes unreachable. This section also covers conditions that can affect calls that are associated with a phone, such as reset or restart.

Cisco Unified CallManager Fails or Becomes Unreachable

The active Cisco Unified CallManager designation applies to the Cisco Unified CallManager from which the phone receives call-processing services. The active Cisco Unified CallManager usually serves as the primary Cisco Unified CallManager for that phone (unless the primary machine is not available).

If the active Cisco Unified CallManager fails or becomes unreachable, the phone attempts to register with the next available Cisco Unified CallManager in the Cisco Unified CallManager Group that is specified for the device pool to which the phone belongs.

The phone device reregisters with the primary Cisco Unified CallManager as soon as it becomes available after a failure. See the “[Maximum Phone Fallback Queue Depth Service Parameter](#)” section on [page 11-30](#) for information about phone registration during failover.

**Note**

Phones do not fail over or fall back while a call is in progress.

Phone is Reset

If a call is in progress, the phone does not reset until the call finishes.

Phone Configuration Checklist

[Table 11-5](#) provides steps to manually configure an SCCP phone in Cisco Unified CallManager Administration. If you are using autoregistration, Cisco Unified CallManager adds the phone and automatically assigns the directory number.

[Table 11-6](#) provides steps to manually configure a SIP phone in Cisco Unified CallManager Administration. If you are using autoregistration, Cisco Unified CallManager adds the phone and automatically assigns the directory number.

Table 11-5 Phone Configuration Checklist for SCCP Protocol

Configuration Steps		Procedures and Related Topics
Step 1	Gather the following information about the phone: • Model • 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	Phone Search, page 11-27
Step 2	Add and configure the phone.	Configuring Cisco Unified IP Phones, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 3	Add and configure lines (DNs) on the phone. You can also configure phone features such as call park, call forward, and call pickup.	Configuring a Directory Number, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 4	Configure speed-dial buttons. You can 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 can change the speed-dial settings on their phones by using Cisco Unified IP Phone User Options.	Configuring Speed-Dial Buttons, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>

Table 11-5 Phone Configuration Checklist for SCCP Protocol (continued)

Configuration Steps		Procedures and Related Topics
Step 5	Configure Cisco Unified IP Phone services. You can configure services for Cisco Unified IP Phone models 7970/71, 7960/61, 7940/41, 7912, and 7905 and Cisco IP Communicator if you want to provide services for users or if you are configuring phones that do not have a specific user who is assigned to them. Users can change the services on their phones by using Cisco Unified CallManager User Options.	Configuring Cisco Unified IP Phones, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 6	Customize phone button templates and softkey templates, if required. Configure templates for each phone.	Configuring Phone Button Templates, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> Configuring Cisco Unified IP Phones, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> Adding Nonstandard Softkey Templates, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 7	Configure the Busy Lamp Field feature, if required. You must use customized phone button templates to configure BLF/SpeedDial buttons.	BLF/SpeedDial Configuration Settings, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 8	Assign services to phone buttons, if required.	Adding a Cisco Unified IP Phone Service to a Phone Button, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 9	Provide power, install, verify network connectivity, and configure network settings for the Cisco Unified IP Phone.	<i>Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager</i>
Step 10	Associate user with the phone (if required).	Associating Devices to an End User, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 11	Make calls with the Cisco Unified IP Phone.	Refer to the user guide for your Cisco Unified IP Phone.

Table 11-6 lists the configuration steps for Cisco Unified IP Phones that support SIP. For third-party SIP phones, see the [Third-Party SIP Phone Configuration Checklist](#) in the *Cisco Unified CallManager Administration Guide*.

Table 11-6 Phone Configuration Checklist for SIP Protocol

Configuration Steps		Procedures and Related Topics
Step 1	Gather the following information about the phone: • Model (7905, 7911, 7912, 7940, 7941, 7960, 7961, 7970, 7971) • 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	Phone Search, page 11-27
Step 2	If configuring the SIP phone in a secure mode, configure the SIP Phone Port on the Cisco Unified CallManager Configuration window.	Cisco Unified CallManager Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 3	If security is required, complete the SIP Security Profile Configuration. The SIP Security Profile gets added to the SIP phone by using the Phone Configuration window.	Phone Security Profile Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> Configuring Cisco Unified IP Phones, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 4	Configure the SIP Profile. The SIP Profile gets added to the SIP phone by using the Phone Configuration window.	Configuring SIP Profiles, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> Configuring Cisco Unified IP Phones, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 5	If you are using NTP for the timing synchronization, configure the NTP server by using the Phone NTP Reference Configuration window. Add the NTP server to Date/Time Group Configuration and then assign the date/time group to the device pool. Add the device pool to the SIP phone by using the Phone Configuration window.	Configuring the Phone NTP References, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> Configuring a Date/Time Group, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> Configuring a Device Pool, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> Configuring Cisco Unified IP Phones, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>

Table 11-6 Phone Configuration Checklist for SIP Protocol (continued)

Configuration Steps		Procedures and Related Topics
Step 6	If you want the digits to be collected before sending them to Cisco Unified CallManager, configure a SIP Phone Dial plan. Add the SIP Dial Rule to the SIP phone by using the Phone Configuration window.	Configuring SIP Dial Rules, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> Configuring Cisco Unified IP Phones, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 7	Add and configure the SIP phone.	Configuring Cisco Unified IP Phones, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 8	Add and configure lines (DNs) on the phone. You can also configure phone features such as call park, call forward, and call pickup.	Configuring a Directory Number, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 9	Configure speed-dial buttons. You can 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 can change the speed-dial settings on their phones by using Cisco Unified CallManager User Options.	Configuring Speed-Dial Buttons, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 10	Configure Cisco Unified IP Phone services. You can configure services for Cisco Unified IP Phone models 7970/71, 7960/61, 7940/41, 7912, 7911, and 7905 and Cisco IP Communicator if you want to provide services for users or if you are configuring phones that do not have a specific user who is assigned to them. Users can change the services on their phones by using the Cisco Unified CallManager User Options window.	Configuring Cisco Unified IP Phones, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 11	Customize phone button templates and softkey templates, if required. Configure templates for each phone.	Configuring Phone Button Templates, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> Configuring Cisco Unified IP Phones, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> Adding Nonstandard Softkey Templates, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 12	Configure the Busy Lamp Field feature, if required. You must use customized phone button templates to configure BLF/SpeedDial buttons.	BLF/SpeedDial Configuration Settings, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 13	Assign services to phone buttons, if required.	Adding a Cisco Unified IP Phone Service to a Phone Button, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 14	Provide power, install, verify network connectivity, and configure network settings for the Cisco Unified IP Phone.	<i>Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager</i>

Table 11-6 Phone Configuration Checklist for SIP Protocol (continued)

Configuration Steps		Procedures and Related Topics
Step 15	Associate user with the phone (if required).	Associating Devices to an End User, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 16	Make calls with the Cisco SIP IP Phone.	Refer to the user guide for your Cisco SIP IP Phone.

Where to Find More Information

Related Topics

- [Understanding Directory Numbers, page 8-1](#)
- Voice Mail Connectivity to Cisco Unified CallManager, *Cisco Unified CallManager System Guide, Release 5.0(4)*
- Enabling Autoregistration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Configuring Cisco Unified IP Phones, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Associating Devices to an End User, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- User/Phone Add Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Phone Button Template Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Common Phone Profile Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Configuring SIP Dial Rules, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Configuring SIP Profiles, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Configuring the Phone NTP References, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Service Parameters Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Barge and Privacy, *Cisco Unified CallManager Features and Services Guide, Release 5.0(4)*
- Call Park, *Cisco Unified CallManager Features and Services Guide, Release 5.0(4)*
- Call Pickup Group, *Cisco Unified CallManager Features and Services Guide, Release 5.0(4)*
- [Immediate Divert](#), *Cisco Unified CallManager Release 5.1(1) New and Changed Information Guide*
- Quality Report Tool, *Cisco Unified CallManager Features and Services Guide, Release 5.0(4)*
- Presence, *Cisco Unified CallManager Features and Services Guide, Release 5.0(4)*

Additional Cisco Unified CallManager Documentation

- Phone administration documentation that supports your phone model and this version of Cisco Unified CallManager
- Cisco Unified IP Phone user documentation

- Firmware release notes for your phone model
- *Cisco Unified CallManager Bulk Administration Guide*
- *Cisco Unified CallManager Security Guide*
- *Cisco Unified CallManager Assistant User Guide*
- *Cisco IP Communicator Administration Guide*



PART 4

Cisco Unified CallManager Features and Services Guide





Music On Hold

The integrated Music On Hold (MOH) feature allows users to place on-net and off-net users on hold with music that is streamed from a streaming source. The Music On Hold feature allows two types of hold:

- End-user hold
- Network hold, which includes transfer hold, conference hold, and call park hold

Music On Hold also supports other scenarios where recorded or live audio is needed.

This chapter covers the following topics:

- [Understanding Music On Hold, page 12-1](#)
- [Music On Hold Server, page 12-8](#)
- [Music On Hold Audio Sources, page 12-8](#)
- [Music On Hold System Requirements and Limits, page 12-12](#)
- [Music On Hold Failover and Fallback, page 12-13](#)
- [Music On Hold Configuration Checklist, page 12-14](#)
- [Monitoring Music On Hold Performance, page 12-15](#)
- [Music On Hold Audio Source Configuration, page 12-16](#)
- [Fixed Music On Hold Audio Source Configuration, page 12-21](#)
- [Music On Hold Server Configuration, page 12-23](#)
- [Music On Hold Audio File Management Configuration, page 12-28](#)
- [Related Topics, page 12-31](#)

Understanding Music On Hold

The following sections explain the Music On Hold feature by providing definitions, service characteristics, feature functionality with examples, and supported features.

Additional Information

See the [“Related Topics”](#) section on page 12-31.

Music On Hold Definitions

In the simplest instance, music on hold takes effect when phone A is talking to phone B, and phone A places phone B on hold. If Music On Hold (MOH) resource is available, phone B listens to music that is streamed from a music on hold server.

The following definitions provide important information for the discussion that follows:

- **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.
- **Media resource group**—A logical grouping of media servers. You may associate a media resource group with a geographical location or a site as desired. You can also form media resource groups to control server usage or desired service type (unicast or multicast).
- **Media resource group list**—A list that comprises prioritized media resource groups. An application can select required media resources from among ones that are available according to the priority order that is defined in a media resource group list.
- **Audio source ID**—An ID that represents an audio source in the music on hold server. The audio source can be either a file on a disk or a fixed device from which a source stream music on hold server obtains the streaming data. One cluster can support up to 51 audio source IDs (1 to 51). Each audio source (represented by an audio source ID) can stream as unicast and multicast mode, if needed.
- **Holding party**—In an active, two-party call, the party that initiates a hold action (either user hold or network hold). Example: if party A is talking to party B, and party A presses the Hold softkey to initiate a hold action, party A is the holding party.
- **Held party**—In an active, two-party call, the party that does not initiate a hold action but is involved. Example: if party A is talking to party B, and party A presses the Hold softkey to initiate a hold action, party B is the held party.

The following audio source ID selection rules apply for selecting audio source IDs and media resource group lists:

- The system administrator, not the end user, defines (configures) audio source IDs.
- The system administrator chooses (configures) audio source IDs for device(s) or device pool(s).
- Holding parties define which audio source ID applies to held parties.
- Cisco Unified CallManager implements four levels of prioritized audio source ID selection with level four as highest priority and level one as lowest priority.
 - The system selects audio source IDs at level four, which is directory/line-based, if defined. (Devices with no line definition, such as gateways, do not have this level.)
 - If no audio source ID is defined in level four, the system searches any selected audio source IDs in level three, which is device based.
 - If no level four nor level three audio source IDs are selected, the system selects audio source IDs that are defined in level two, which is DevicePool-based.
 - If all higher levels have no audio source IDs selected, the system searches level one for audio source IDs, which are clusterwide parameters.

The following media resource group list selection rules apply:

- Held parties determine the media resource group list that a Cisco Unified CallManager uses to allocate a music on hold resource.
- Two levels of prioritized media resource group list selection exist:
 - Level two media resource group list provides the higher priority level, which is device based. Cisco Unified CallManager uses the media resource group list at the device level if such a media resource group list is defined.
 - Level one media resource group list provides the lower priority level, which is an optional DevicePool parameter. Cisco Unified CallManager uses the DevicePool level media resource group list only if no media resource group list is defined in the device level for that device.
- If no media resource group lists are defined, Cisco Unified CallManager uses the system default resources. System default resources comprise resources that are not assigned to any existing media resource group. Be aware that system default resources are always unicast.

Additional Information

See the [“Related Topics” section on page 12-31](#).

Music On Hold Characteristics

The integrated Music On Hold feature allows users to place on-net and off-net users on hold with music that is streamed from a streaming source. This source makes music available to any possible on-net or off-net device that is placed on hold. On-net devices include station devices and applications that are placed on hold, consult hold, or park hold by an interactive voice response (IVR) or call distributor. Off-net users include those who are connected through Media Gateway Control Protocol (MGCP)/skinny gateways, IOS H.323 gateways, and IOS Media Gateway Control Protocol gateways. The system also makes the Music On Hold feature available for Cisco IP POTS phones that connect to the Cisco IP network through FXS ports on IOS H.323/Media Gateway Control Protocol and for Cisco Media Gateway Control Protocol/skinny gateways.

The integrated Music On Hold feature covers media server, data base administration, call control, media resource manager, and media control functional areas.

The music on hold server provides the music resources/streams. These resources register with the Cisco Unified CallManager during the initialization/recovery period.

Database administration provides a user interface to allow the Cisco Unified CallManager administrator to configure the Music On Hold feature for the device(s). Database administration also provides Cisco Unified CallManager call control with configuration information.

Call control controls the music on hold scenario logic.

The media resource manager processes the registration request from the music on hold server and allocates/deallocates the music on hold resources under the request of call control.

Media control controls the establishment of media stream connections, which can be one-way or two-way connections.

You must ensure that an end device is provisioned with information related to music on hold before music on hold functions for that device. Initializing a Cisco Unified CallManager creates a media resource manager. The music on hold server(s) registers to the media resource manager with its music on hold resources.

When an end device or feature places a call on hold, Cisco Unified CallManager connects the held device to a music resource. When the held device is retrieved, it disconnects from the music on hold resource and resumes normal activity.

Additional Information

See the [“Related Topics” section on page 12-31](#).

Music On Hold Functionality

For music on hold to function, you must perform the actions in the following list:

- Configure music on hold servers.
- Configure audio sources. For the examples that follow, configure and provision the following audio sources: *Thank you for holding* and *Pop Music 1*.



Note Define audio sources first and then set up the music on hold servers, especially when multicast will be used. The user interface allows either step to take place first.



Note If an audio source is configured for multicast, the MOH server always transmits the audio stream, regardless of whether devices are held.

- Configure media resource groups. If multicast is desired, check the Use Multicast for MOH Audio check box.
- Configure media resource group lists.
- Assign media resource group lists and audio sources to device pools.
- Assign media resource group lists and audio sources to devices (to override assignments made to device pools).
- Assign audio sources to lines (to override device settings).

Using the preceding configuration actions, if you define music on hold functionality as follows, the examples that follow demonstrate music on hold functionality for user hold, transfer hold, and call park.

Media Resource Groups

MOH designates a music on hold server. MRG designates a media resource group.

- MRG_D comprises MOH_D.
- MRG_S_D comprises MOH_S and MOH_D.

Media Resource Group Lists

MRGL designates a media resource group list.

- MRGL_D comprises MRG_D.
- MRGL_S_D comprise MRG_S_D and MRG_D (prioritized order).

Nodes

- Dallas node comprises phone D and MOH_D.
- San Jose node comprises phone S and MOH_S.

- Assign phone D audio source ID 5, *Thank you for holding* or plain music (for both user and network hold), and MRGL_D.
- Assign phone S audio source ID 1, *Pop Music 1* (for both user and network hold), and MRGL_S_D.

User Hold Example

Phone D calls phone S, and phone S answers. Phone D presses the Hold softkey. Result: Phone S receives *Thank you for holding* announcement or plain music that is streaming from MOH_S. (MOH_S has available streams.) When phone D presses the Resume softkey, phone S disconnects from the music stream and reconnects to phone D.

Transfer Hold Example

Transfer hold serves as an example of network hold.

Phone D calls phone S, and phone S answers. Phone D presses the Transfer softkey. Phone S receives *Thank you for holding* announcement or plain music that is streaming from MOH_D. (MOH_S has no available streams, while MOH_D does.) After phone D completes the transfer action, phone S disconnects from the music stream and gets redirected to phone X, the transfer destination.

Call Park Example

Call park serves as an example of network hold.

Phone D calls phone S, and phone S answers. Phone S presses the CallPark softkey. Phone D receives a beep tone. (MOH_D has no available streams.) Phone X picks up the parked call. Phone S gets redirected to phone X (phone D and phone X are conversing).

Additional Information

See the [“Related Topics” section on page 12-31](#).

Supported Music On Hold Features

Music on hold supports the following features, which are listed by category. Feature categories include music on hold server characteristics, server scalability, server manageability, server redundancy, database scalability, and manageability.

Music On Hold Server Characteristics

- Servers stream music on hold from music on hold data source files that are stored on their disks.
- Servers stream music on hold from an external audio source (for example, looping tape recorder, radio, or CD).
- Music on hold servers can use a single music on hold data source for all source streams and, hence, all connected streams. When multiple music on hold servers are involved, the local server of each music on hold server always stores the music on hold data source files. Cisco Unified CallManager does not support distribution of fixed-device (hardware) audio sources across music on hold servers within a media resource group.
- Music on hold data source files have a common filename across all music on hold servers.
- Music on hold data source files must be uploaded to each server in the cluster.

- Each audio source receives a feed from either a designated file or a designated fixed source (for example, radio or CD).
- A designated fixed source comprises a single device, which is either enabled or disabled.
- The audio driver on the local machine makes a single fixed source available to the music on hold server.
- Music on hold servers support the G.711 (a-law and mu-law), G.729a, and wideband codecs.
- Music on hold servers register with one primary Cisco Unified CallManager server.

Server Scalability

- Music on hold supports from 1 to 500 simplex unicast streams per music on hold server.
- Music on hold supports multiple Cisco-developed media-processing applications, including Interactive Voice Response (IVR) and AutoAttendant (AA). Cisco Unified CallManager facilitates this support.
- Music on hold server simultaneously supports up to 50 music on hold data source files as sources.
- Music on hold server supports one fixed-device stream source in addition to the file stream sources. This source is the fixed audio source, which is configured on the Music On Hold (MOH) Fixed Audio Source Configuration window. This source requires the additional Cisco USB Music-On-Hold-capable adapter.

Server Manageability

- From Cisco Unified CallManager Serviceability windows, you can activate the music on hold server application, Cisco IP Media Streaming Application, on any standard media convergence server (MCS) as a service.
- You can activate music on hold application on the same media convergence server (MCS) as other media applications, so music on hold and the other media application(s) co-reside on the MCS.
- You can install music on hold server application on multiple media convergence servers (MCS) in a cluster.
- The administrator can specify the source for each source stream that the server provides.
- Administration of stream sources takes place through a browser.

Server Redundancy

- Music on hold servers support Cisco Unified CallManager lists. The first entry on the list serves as the primary server, and subsequent Cisco Unified CallManagers on the list serve as backup Cisco Unified CallManagers in prioritized order.
- Music on hold servers can maintain a primary and backup connection to Cisco Unified CallManagers from their Cisco Unified CallManager list.
- Music on hold servers can re-home to backup Cisco Unified CallManagers by following the standard procedures that are used by other servers and phones on the cluster.
- Music on hold servers can re-home to their primary server by following standard procedures for other media servers on the cluster.

Cisco Unified CallManager/Database Requirements

- When a Cisco Unified CallManager is handling a call and places either endpoint in the call on hold, the Cisco Unified CallManager can connect the held endpoint to music on hold. This feature holds true for both network hold and user hold. Network hold includes transfer, conference, call park, and so forth.
- A media resource group for music on hold supports having a single music source stream for all connected streams.
- The system supports having music on hold server(s) at a central site without music on hold server(s) at remote sites. Remote site devices that require music on hold service can obtain service from a media resource group across the WAN when service is not available locally.
- You can distribute music on hold servers to any site within a cluster.
- A music on hold server can use a single music on hold data source for all source streams and, hence, all connected streams. When multiple music on hold servers are involved, the music on hold data source may be a file that is stored locally on each server.
- The system can detect when the primary media resource group that supplies music on hold for a device is out of streams and can select a stream from the secondary or tertiary media resource group that is specified for that device.
- When connecting a device to music on hold, the system can insert a transcoder when needed to support low-bandwidth codecs.

Database Scalability

- Cisco Unified CallManager can support from 1 to 500 unicast sessions per music on hold server.
- A cluster can support from 1 to more than 20 music on hold servers.
- A cluster can support from 1 to more than 10,000 simultaneous music on hold streams across the cluster.
- A cluster can support from 1 to 500 or more media resource groups for music on hold.
- A media resource group for music on hold can support from 1 to 20 or more music on hold servers.

Manageability

- The administrator can select media resource group list per device.
- The administrator can select music on hold source stream per device/DN.
- The administrator can select music on consult (network hold) source stream per device/DN.
- The administrator can configure which music on hold servers are part of a specified media resource group.
- The administrator can designate a primary, secondary, and tertiary music on hold/consult servers for each device by configuring media resource groups and media resource group lists.
- The administrator can provision multiple music on hold servers.
- The administrator can provision any device that is registered with the system such that any music on hold server can service it in the system.
- All music on hold configuration and administration take place through a browser.
- The administrator specifies the user hold and network hold audio sources for each device pool. These default audio sources may function as either file based or fixed device based.

- The administrator can designate a music on hold server as either unicast or multicast, provided that resources exist to support multicast.
- The administrator can reset all music on hold servers.

Additional Information

See the [“Related Topics”](#) section on page 12-31.

Music On Hold Server

The music on hold server uses the Station Stimulus (Skinny Client) messaging protocol for communication with Cisco Unified CallManager. A music on hold server registers with the Cisco Unified CallManager as a single device and reports the number of simplex, unicast audio streams that it can support. The music on hold server advertises its media type capabilities to the Cisco Unified CallManager as G.711 mu-law and a-law, G.729a, and wideband. Cisco Unified CallManager starts and stops music on hold unicast streams by sending skinny client messages to the music on hold server.

A music on hold server handles up to 500 simplex, unicast audio streams. A media resource group includes one or more music on hold servers. A music on hold server supports 51 audio sources, with one audio source that is sourced from a fixed device that uses the local computer audio driver, and the rest that are sourced from files on the local music on hold server.

You may use a single file for multiple music on hold servers, but the fixed device may be used as a source for only one music on hold server. The music on hold audio source files get stored in the proper format for streaming. Cisco Unified CallManager allocates the simplex unicast streams among the music on hold servers within a cluster.

The music on hold server uses the media convergence server series hardware platform. A Cisco USB sound adapter that is installed on the same computer as the music on hold server application provides the external fixed audio source, which can be a looping tape recorder, radio, or CD.

The music on hold server, which is actually a component of the Cisco IP Voice Media Streaming application, supports standard device recovery and database change notification.

Each music on hold server uses the local hard disk to store copies of the Music On Hold audio source files. Each audio source file gets distributed to the server(s) when the file is added through the Cisco Unified CallManager Administration interface.

**Note**

The administrator must upload Music On Hold audio source files to each MOH server.

Additional Information

See the [“Related Topics”](#) section on page 12-31.

Music On Hold Audio Sources

When the administrator imports an audio source file, the Cisco Unified CallManager Administration window interface processes the file and converts the file to the proper format(s) for use by the music on hold server.

The recommended format for audio source files includes the following specifications:

- 16-bit PCM wav file
- Stereo or mono
- Sample rates of 48 kHz, 32 kHz, 16 kHz, or 8 kHz

Additional Information

See the [“Related Topics” section on page 12-31](#).

Default Music On Hold Sample

Cisco Unified CallManager includes a default music on hold sample that automatically downloads with Cisco Unified CallManager software for customer use.

Additional Information

See the [“Related Topics” section on page 12-31](#).

Creating Audio Sources

Most standard wav files serve as valid input audio source files, including the following file types:

- 16-bit PCM (stereo/mono)
- 8-bit CCITT a-law or mu-law (stereo/mono)

**Note**

The Music On Hold feature does not support the MP3 format.

In creating an audio source, the following sequence takes place:

- The administrator imports the audio source file into the Cisco Unified CallManager cluster. This step may take some time to transfer the file and convert the file to the proper format(s) for the music on hold server to use.
- The administrator must import the audio source file to the MOH server in each cluster prior to assigning an audio source number to the audio source file.
- The music on hold server uses the local audio source file(s).
- The music on hold server streams the files by using a kernel mode RTP driver as Cisco Unified CallManager needs or requests.

Additional Information

See the [“Related Topics” section on page 12-31](#).

Storing Audio Source Files

In previous releases, Cisco Unified CallManager did not limit the amount of space that MOH files used. The MOH upload tool does not limit the number of uploaded files or the file size. The modified upload JSP pages check the disk usage of existing MOH files and only permit uploads if sufficient space is found.

The following considerations also apply:

- Cisco Unified CallManager supports up to five MOH audio sources on 36- or 40-gigabyte, disk-based systems. Systems with 72- or 80-gigabyte disks support the entire 50 audio streams.
- To increase the number of audio sources that Cisco Unified CallManager supports, install a larger disk during upgrade.

**Note**

The smallest node on the cluster controls MOH capacity.

Additional Information

See the [“Related Topics”](#) section on page 12-31.

Managing Audio Sources

After music on hold audio sources are created, their management occurs entirely through Cisco Unified CallManager Administration. Choose **Media Resources > Music On Hold Audio Source** to display the Music On Hold (MOH) Audio Source Configuration window. For a given audio source, use this window to add, update, or delete a music on hold audio source. For each audio source file, assign a music on hold audio source number and music on hold audio source name and decide whether this audio source will play continuously and allow multicasting. For an audio source, this window also displays the music on hold audio source file status. Refer to the [“Finding a Music On Hold Audio Source”](#) section on page 12-17 for details.

**Note**

The Music On Hold Audio Source Configuration window uploads audio source files only to a particular server. The window does not provide for automatic copying of audio source files to any other servers. You must manually upload audio source files to subscriber servers by accessing the Cisco Unified CallManager application on each server.

Additional Information

See the [“Related Topics”](#) section on page 12-31.

Multicast and Unicast Audio Sources

Multicast music on hold conserves system resources. Multicast allows multiple users to use the same audio source stream to provide music on hold. Multicast audio sources associate with an IP address.

Unicast music on hold, the system default, uses a separate source stream for each user or connection. Users connect to a specific device or stream.

For administrators, multicast entails managing devices, IP addresses, and ports. In contrast, unicast entails managing devices only.

For multicast, administrators must define at least one audio source to allow multicasting. To define music on hold servers for multicast, first define the server to allow multicasting.

For multicast, an address comprises a combination of an IP address and a port number. Each audio source for multicast requires a set of addresses: one for each format on each MOH server. When configuring the MOH server for multicast, specify whether addresses should be assigned by incrementing the port or the IP address.

**Caution**

Cisco strongly recommends incrementing multicast on IP address instead of port number to avoid network saturation in firewall situations. This results in each multicast audio source having a unique IP address and helps to avoid network saturation.

The Max Hops field in the Music On Hold (MOH) Server Configuration window indicates the maximum number of routers that an audio source is allowed to cross. If max hops is set to zero, the audio source must remain in its own subnet. If max hops is set to one, the audio source can cross up to one router to the next subnet. Cisco recommends setting max hops to two.

A standards body reserves IP addresses. Addresses for IP multicast range from 224.0.1.0 to 239.255.255.255. The standards body, however, assigns addresses in the range 224.0.1.0 to 238.255.255.255 for public multicast applications. Cisco strongly discourages using public multicast addresses for music on hold multicast. Instead, Cisco recommends using an IP address in the range that is reserved for administratively controlled applications on private networks (239.0.0.0 to 239.255.255.255).

Valid port numbers for multicast include even numbers that range from 16384 to 32767. (The system reserves odd values.)

Multicast functions only if both media resource groups and media resource group lists are defined to include a multicast music on hold server. For media resource groups, you must include a music on hold server that is set up for multicast. Such servers are labeled as *(MOH)[Multicast]*. Also, check the Use Multicast for MOH Audio check box when defining a media resource group for multicast.

For media resource group lists, which are associated with device pools and devices, define the media resource group list, so the media resource group set up for multicast is the first group in the list. This recommended practice facilitates the device efforts to find the multicast audio source first.

In music on hold processing, the held device (the device placed on hold) determines the media resource to use, but the holding device (the device that initiates the hold action) determines the audio source to use.

Multicast MOH Direction Attribute for SIP Service Parameter

The Multicast MOH Direction Attribute for SIP service parameter determines whether Cisco Unified CallManager sets the direction attribute of the Session Description Protocol (SDP) in its multicast Music on Hold (MOH) INVITE message to sendOnly or recvOnly.

If your deployment uses SIP phone loads 8.4 and earlier for Cisco Unified IP Phone models 7940 and 7960, or SIP phone loads 8.1(x) and earlier for Cisco Unified IP Phone models 7906, 7911, 7941, 7961, 7970, and 7971, set this parameter to sendOnly. Otherwise, leave this parameter set to the default value, recvOnly.

Additional Information

See the [“Related Topics”](#) section on page 12-31.

Multicast Configuration Checklist

Table 12-1 provides a checklist for configuring various Cisco Unified CallManager services to allow multicasting. You must perform all steps for multicast to be available.

Table 12-1 Multicast Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Configure a music on hold server to enable multicast audio sources.  Caution Cisco strongly recommends incrementing multicast on IP address in firewall situations. This results in each multicast audio source having a unique IP address and helps to avoid network saturation.	Music On Hold Server Configuration Settings, page 12-26
Step 2	Configure an audio source to allow multicasting.	Music On Hold Audio Source Configuration Settings, page 12-19
Step 3	Create a media resource group and configure it to use multicast for MOH audio.	Media Resource Group Configuration Settings, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 4	Create a media resource group list with a multicast media resource group as the primary media resource group.	Media Resource Group List Configuration Settings, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 5	Choose the media resource group list that was created in Step 4 for either a device pool or for specific devices.	Media Resource Group List Configuration Settings, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>

Additional Information

See the [“Related Topics”](#) section on page 12-31.

Music On Hold System Requirements and Limits

The following system requirements and limits apply to the Music On Hold feature:

- All audio streaming devices that are using the Music On Hold feature support simplex streams. The music on hold server supports up to 500 simplex streams.
- The music on hold (MOH) server, a part of the Cisco IP Voice Media Streaming application, gets installed with Cisco Unified CallManager. Use the Cisco Unified CallManager Serviceability application to activate the MOH server. Because only one Cisco IP Voice Media Streaming application may be activated on a media convergence server, you can enable only one MOH server per server. You can activate the Cisco IP Voice Media Streaming application, however, on multiple servers to provide multiple MOH servers for the cluster.
- For a Cisco Unified CallManager cluster, you may define up to 50 audio sources. A Cisco Unified CallManager Administration window supports import, addition, update, and deletion of each audio source. The music on hold server also supports one fixed input source. The system supports the following codecs: G.711 a-law/mu-law, G.729a, and wideband.

**Note**

Because the G.729a codec is designed for human speech, using it with music on hold for music may not provide acceptable audio quality.

- For each cluster, you may define up to 50 audio sources from files as well as one fixed audio source. A Cisco Unified CallManager Administration window supports addition, update, and deletion of each audio source. All servers use local copies of the same 50 or fewer files. You must set up the fixed audio source that is configured per cluster on each server.
- For each cluster, you may define at most 20 music on hold servers. The Cisco Unified CallManager Administration window allows import, addition, update, and deletion of music on hold servers. The window allows administrators to specify the following characteristics for each server:
 - Name
 - Node (server host name)
 - Device pool
 - Maximum number of unicast and multicast streams
 - Sources to multicast
 - For each multicast source: IP address, port, and time to live (maximum number of router hops)
- Cisco Unified CallManager Administration allows definition of at least 500 media resource groups per cluster. Each media resource group may include any combination of at least 20 media resources, including music on hold servers, media termination points, transcoders, and conference devices. Music on hold servers in one cluster support at least 10,000 simultaneous music on hold streams. See “Media Resource Groups” in the *Cisco Unified CallManager System Guide, Release 5.0(4)*, for details of media resource groups.
- Cisco Unified CallManager Administration allows definition of media resource group lists. See “Media Resource Group Lists” in the *Cisco Unified CallManager System Guide, Release 5.0(4)*, for details of media resource group lists.
- Modifications to the Cisco Unified CallManager Administration device configuration windows for phones and gateways allow the selection of a media resource group list, hold stream source, and consult stream source as optional parameters for a device.
- Modifications to the Cisco Unified CallManager Administration Directory Number configuration windows allow selection of a user hold source and a network hold source.
- Modifications to the Cisco Unified CallManager Administration Service Parameters allows entry to a clusterwide, default music on hold stream source (default specifies 1) and default media resource group type (default specifies unicast).
- The number of streams that the music on hold server can use may decrease if the annunciator, software MTP, or software conference bridge is in use on the same MCS server.

Additional Information

See the [“Related Topics” section on page 12-31](#).

Music On Hold Failover and Fallback

The music on hold server supports Cisco Unified CallManager lists and failover as implemented by the software conference bridge and media termination point. Upon failover, the system maintains connections to a backup Cisco Unified CallManager if one is available.

Cisco Unified CallManager takes no special action when a music on hold server fails during an active music on hold session. The held party receives nothing from this point, but this situation does not affect normal call functions.

Additional Information

See the “[Related Topics](#)” section on page 12-31.

Music On Hold Configuration Checklist

[Table 12-2](#) provides a checklist for configuring music on hold.

Table 12-2 Music On Hold Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	The Cisco IP Voice Media Streaming application gets installed automatically upon installation of Cisco Unified CallManager. To provide an MOH server, you must use the Cisco Unified CallManager Serviceability application to activate the Cisco IP Voice Media Streaming application. When a server gets added, the Cisco Unified CallManager automatically adds the media termination point, conference bridge, annunciator, and music on hold devices to the database. Note During installation, Cisco Unified CallManager installs and configures a default music on hold audio source if one does not exist. Music on hold functionality can proceed by using this default audio source without any other changes.	<i>Installing Cisco Unified CallManager Release 5.0(4)</i>
Step 2	Run the music on hold audio translator.  Caution If the audio translator translates files on the same server as the Cisco Unified CallManager, serious problems may occur. The audio translator tries to use all available CPU time, and Cisco Unified CallManager may experience errors or slowdowns.	Music On Hold Audio Sources, page 12-8
Note	The installation program performs the following actions automatically. If the user manually adds the music on hold components, ensure the following steps are performed.	
Step 3	Configure the music on hold server.	Configuring a Music On Hold Server, page 12-24
Step 4	Add and configure audio source files.	Finding a Music On Hold Audio Source, page 12-17

Additional Information

See the “[Related Topics](#)” section on page 12-31.

Monitoring Music On Hold Performance

Perform the activities in [Table 12-3](#) to monitor music on hold performance.

Table 12-3 **Music On Hold Performance Monitoring**

Monitoring Activity		Detailed Information
Step 1	Use the Cisco Unified CallManager Serviceability Real-Time Monitoring Tool (RTMT) to check resource usage and device recovery state.	Viewing Music On Hold Server Performance, page 12-15 <i>Cisco Unified CallManager Serviceability Administration Guide</i> and <i>Cisco Unified CallManager Serviceability System Guide</i> document another method of viewing this information.
Step 2	Search the event log for Cisco IP Voice Media Streaming application entries.	<i>Cisco Unified CallManager Serviceability Administration Guide</i> <i>Cisco Unified CallManager Serviceability System Guide</i>
Step 3	Verify that the Cisco IP Voice Media Streaming application service is running.	Additional Information, page 12-16 <i>Cisco Unified CallManager Serviceability Administration Guide</i> and <i>Cisco Unified CallManager Serviceability System Guide</i> document another method of viewing this information.
Step 4	Search the Media Application trace (CMS) to see what music on hold-related activity that it detects.	<i>Cisco Unified CallManager Serviceability Administration Guide</i> and <i>Cisco Unified CallManager Serviceability System Guide</i>

Additional Information

See the [“Related Topics”](#) section on page 12-31.

Viewing Music On Hold Server Performance

To view music on hold server perfmon counters, use the Cisco Unified CallManager Serviceability Real-Time Monitoring Tool (RTMT).

[Table 12-4](#) details the performance monitoring counters that display in the Cisco Unified CallManager Serviceability Real-Time Monitoring Tool Performance window.

Table 12-4 Music On Hold Performance Counters

Performance Counter Name	Description
MOHConnectionState	Indicates primary and secondary Cisco Unified CallManager: • 1 = Primary • 2 = Secondary • 0 = Not connected
MOHAudioSourcesActive	Specifies total number of active audio sources, including each supported codec type. If audio Source 1 has mu-law and G.729 enabled, count for this audio source may show 2.
MOHStreamsActive	Specifies total number of active streams. Two potential overhead streams exist for each audio source/codec type: one for actual audio source, another for multicast.
MOHStreamsAvailable	Specifies total number of available simplex streams. Total represents total number of streams that are available in device driver for all devices.
MOHConnectionsLost	Specifies number of times that connection has been lost for the corresponding Cisco Unified CallManager.
MOHStreamsTotal	Specifies total number of streams that are processed.

See the *Cisco Unified CallManager Serviceability System Guide* for additional information about the Real-Time Monitoring Tool.

Additional Information

See the [“Related Topics”](#) section on page 12-31.

Checking Service States

To check whether the music on hold service is running, use Performance Management.

Additional Information

See the [“Related Topics”](#) section on page 12-31.

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.

Use the following topics to configure Music On Hold audio sources:

- [Finding a Music On Hold Audio Source, page 12-17](#)
- [Configuring a Music On Hold Audio Source, page 12-18](#)
- [Deleting a Music On Hold Audio Source, page 12-19](#)
- [Music On Hold Audio Source Configuration Settings, page 12-19](#)

Additional Information

See the [“Related Topics” section on page 12-31](#).

Finding a Music On Hold Audio Source

Because you might have multiple Music On Hold audio sources in your network, Cisco Unified CallManager lets you search for Music On Hold audio sources on the basis of specified criteria. Follow these steps to search for a specific Music On Hold audio source in the Cisco Unified CallManager database.



Note

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

Procedure

Step 1 Choose **Media Resources > Music On Hold Audio Source**.

The Find and List Music On Hold Audio Sources window displays.

Step 2 From the first drop-down list box, choose on the following criteria:

- MOH Audio Stream Number
- MOH Audio Source Name



Note

To find all Music On Hold audio sources that are registered in the database, leave the text box blank and click **Find**.

Step 3 From the second drop-down list box, choose a search pattern for your 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 MOH audio sources 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 Music On Hold audio sources from the Find and List Music On Hold Audio Sources window by checking the check boxes next to the appropriate Music On Hold audio sources and clicking **Delete Selected**. You can choose all of the Music On Hold audio sources in the window by clicking **Select All**.

Deletion does not remove the Music On Hold audio source files. Deletion only removes the association with the MOH Audio Stream number.

- Step 5** From the list of records that match your search criteria, click the name of the Music On Hold audio source that you want to view.
- The Music On Hold Audio Source Configuration window displays with the Music On Hold audio source that you choose.

Additional Information

See the [“Related Topics” section on page 12-31](#).

Configuring a Music On Hold Audio Source

Perform the following procedure to add or update a Music On Hold audio source. Use this procedure to associate an existing audio source with an audio stream number or to upload a new custom audio source.

**Note**

If a new version of an audio source file is available, you must perform the update procedure to use the new version.

Procedure

- Step 1** Choose **Media Resources > Music On Hold Audio Source**.
- The Find and List Music On Hold Audio Sources window displays.
- Step 2** Perform one of the following tasks:
- To add a new Music On Hold audio source, click **Add New**.
The Music On Hold Audio Source Configuration window displays.
 - To update a Music On Hold audio source, locate a specific Music On Hold audio source as described in [“Finding a Music On Hold Audio Source” section on page 12-17](#)
- Step 3** Enter the appropriate settings as described in [Table 12-5](#).
- Step 4** Click **Save**.
- If you added a Music On Hold Audio Source, the list box at the bottom of the window now includes the new Music On Hold audio source.

**Note**

The MOH Audio Source File Status pane tells you about the MOH audio translation status for the added source.

Additional Information

See the [“Related Topics” section on page 12-31](#).

Deleting a Music On Hold Audio Source

Perform the following procedure to delete an existing Music On Hold audio source.

**Note**

Deletion does not remove the Music On Hold audio source files. Deletion only removes the association with the MOH Audio Stream number.

Procedure

-
- Step 1** Choose **Media Resources > Music On Hold Audio Source**.
- The Find and List Music On Hold Audio Sources window displays.
- Step 2** To locate a specific Music On Hold audio source, enter search criteria and click **Find**.
- A list of Music On Hold audio sources that match the search criteria displays.
- Step 3** Perform one of the following actions:
- Check the check boxes next to the Music On Hold audio sources that you want to delete and click **Delete Selected**.
 - Delete all Music On Hold audio sources in the window by clicking **Select All** and then clicking **Delete Selected**.
 - From the list, choose the name of the Music On Hold audio source that you want to delete and click **Delete**.
- A confirmation dialog displays.
- Step 4** Click **OK**.
- The association of the chosen Music On Hold audio source with an audio stream number gets deleted.
-

Additional Information

See the [“Related Topics” section on page 12-31](#).

Music On Hold Audio Source Configuration Settings

[Table 12-5](#) describes the configuration settings that are used for configuring Music On Hold audio sources.

Table 12-5 Music On Hold Audio Source Configuration Settings

Field	Description
Music On Hold Audio Source Information	
MOH Audio Stream Number	Use this field to choose the stream number for this MOH audio source. To do so, click the drop-down arrow and choose a value from the list that displays. For existing MOH audio sources, this value displays in the MOH Audio Source title.
MOH Audio Source File	Use this field to choose the file for this MOH audio source. To do so, click the drop-down arrow and choose a value from the list that displays.
Upload File	To upload an MOH audio source file that does not display in the drop-down list box, click the Upload File button. In the Upload File popup window that displays, enter the path to a file that specifies an audio source file. If you do not know the path and file name, search for the file by clicking the Browse... button to the right of the File field. After you locate the audio source file, click the Upload button to complete the upload. After the audio file gets uploaded, the Upload Result window tells you the result of the upload. Click Close to close this window. Note Uploading a file uploads the file to the Cisco Unified CallManager server and performs audio conversions to create codec-specific audio files for MOH. Depending on the size of the original file, processing may take several minutes to complete. Note Uploading an audio source file to an MOH server uploads the file only to one MOH server. You must upload an audio source file to each MOH server in a cluster by using Cisco Unified CallManager Administration on each server. MOH audio source files do <i>not</i> automatically propagate to other MOH servers in a cluster.
MOH Audio Source Name	Enter a unique name in this field for the MOH audio source. This name can comprise up to 50 characters. Valid characters include letters, numbers, spaces, dashes, dots (periods), and underscores.
Play continuously (repeat)	To specify continuous play of this MOH audio source, check this check box. Note Cisco recommends checking this check box. If continuous play of an audio source is not specified, only the first party placed on hold, not additional parties, will receive the MOH audio source.
Allow Multicasting	To specify that this MOH audio source allows multicasting, check this check box.

Table 12-5 Music On Hold Audio Source Configuration Settings (continued)

Field	Description
MOH Audio Source File Status	This pane displays information about the source file for a chosen MOH audio source. For an MOH audio source, the following attributes display: • Input File Name • Error Code • Error Text • Duration (in) Seconds • Disk Space KB • Low Date Time • High Date Time • Output File List – ULAW wav file name and status – ALAW wav file name and status – G.729 wav file name and status – Wideband wav file name and status • Date MOH Audio Translation completed
MOH Server Reset Information	To reset all MOH servers, click the Reset button. Note Cisco Unified CallManager makes Music On Hold unavailable while the servers reset.
MOH Audio Sources	
(list of MOH audio sources)	For each MOH audio source that has been added, the MOH audio source name displays in this list box. Click the name of an MOH audio source to configure that MOH audio source.

Additional Information

See the [“Related Topics” section on page 12-31](#).

Fixed Music On Hold Audio Source Configuration

The music on hold server supports one fixed-device stream source in addition to the file stream sources. This source represents the fixed audio source, which gets configured in the Fixed Music On Hold (MOH) Audio Source Configuration window. The fixed audio source gets sourced from a fixed device that uses the local computer audio driver.

For each cluster, you may define one fixed audio source. You must set up the fixed audio source that is configured per cluster on each MOH server. To do so, use the Cisco USB MOH sound adapter, which must be ordered separately.

Use the following topics to configure the fixed Music On Hold audio source:

- [Configuring the Fixed Music On Hold \(MOH\) Audio Source, page 12-22](#)
- [Deleting a Fixed Music On Hold \(MOH\) Audio Source, page 12-22](#)
- [Fixed Music On Hold \(MOH\) Audio Source Configuration Settings, page 12-23](#)

Configuring the Fixed Music On Hold (MOH) Audio Source

Perform the following procedure to configure the fixed music on hold audio source.

Procedure

-
- Step 1** Choose **Media Resources > Fixed MOH Audio Source**.
The Fixed MOH Audio Source Configuration window displays.
- Step 2** To configure and enable a fixed music on hold (MOH) audio source, enter the appropriate settings as described in [Table 12-6](#).
- Step 3** Click **Save**.
The Fixed MOH Audio Source Configuration window displays an *Update Successful* status message.
-

Additional Information

See the [“Related Topics”](#) section on page 12-31.

Deleting a Fixed Music On Hold (MOH) Audio Source

Perform the following procedure to delete an existing fixed music on hold audio source.

Procedure

-
- Step 1** Choose **Media Resources > Fixed MOH Audio Source**.
The Fixed MOH Audio Source Configuration window displays.
- Step 2** If the fixed MOH audio source that displays is enabled (that is, the Enable check box has been checked), you can delete this fixed MOH audio source.
To delete this fixed MOH audio source, click **Delete**.
A confirmation dialog box displays.
- Step 3** Click **OK**.
The chosen fixed music on hold audio source gets deleted from the database.
-

Additional Information

See the [“Related Topics”](#) section on page 12-31.

Fixed Music On Hold (MOH) Audio Source Configuration Settings

Table 12-6 describes the configuration settings that are used for configuring the fixed music on hold (MOH) audio source.

Table 12-6 Fixed Music On Hold (MOH) Audio Source Configuration Settings

Field	Description
Fixed MOH Audio Source Information	
Source ID	This field displays the stream number for this fixed MOH audio source.
Name	Enter a unique name in this field for the fixed MOH audio source. This name can comprise up to 50 characters. Valid characters include letters, numbers, spaces, dashes, dots (periods), and underscores.
Allow Multicasting	To specify that this fixed MOH audio source allows multicasting, check this check box.
Enable (If checked, Name is required.)	To enable this fixed MOH audio source, check this check box.

Additional Information

See the [“Related Topics” section on page 12-31](#).

Music On Hold Server Configuration

You can configure servers for music on hold for a media resource group. Use the following topics to configure music on hold servers:

- [Finding a Music On Hold Server, page 12-23](#)
- [Configuring a Music On Hold Server, page 12-24](#)
- [Resetting or Restarting a Music On Hold Server, page 12-25](#)
- [Music On Hold Server Configuration Settings, page 12-26](#)

For any music on hold server that you configure, you may trace the configuration of that server. Refer to the *Cisco Unified CallManager Serviceability Administration Guide* and the *Cisco Unified CallManager Serviceability System Guide* for more information.

Additional Information

See the [“Related Topics” section on page 12-31](#).

Finding a Music On Hold Server

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

Procedure**Step 1** Choose **Media Resources > Music On Hold Server**.

The Find and List Music On Hold Servers window displays. Use the two drop-down list boxes to search for a music on hold server.

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

- Name
- Description
- Device Pool Name

**Tip**

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

Step 3 From the second Find Music On Hold Servers 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 music on hold servers within the search results, click the **Search Within Results** check box and enter your search criteria as described in this step.

Step 5 From the list of records that match your search criteria, click the name of the music on hold server that you want to view.

The Music On Hold (MOH) Server Configuration window displays with the music on hold server that you choose.

Additional Information

See the [“Related Topics” section on page 12-31](#).

Configuring a Music On Hold Server

Perform the following procedure to update a music on hold server.

**Note**

You cannot add nor delete a music on hold server.

Procedure

-
- Step 1** Choose **Media Resources > Music On Hold Server**.
- The Find and List Music On Hold Servers window displays. Use the two drop-down list boxes to search for a music on hold server.
- Step 2** To update a music on hold server, click the music on hold server that you want to update. The Music On Hold (MOH) Server Configuration window displays.
- Step 3** Enter or update the appropriate settings as described in [Table 12-7](#).
- Step 4** To update this music on hold server, click **Save**.
- The music on hold server gets updated in the database.
-

Additional Information

See the [“Related Topics” section on page 12-31](#).

Resetting or Restarting a Music On Hold Server

Perform the following procedure to reset an existing music on hold server.

Procedure

-
- Step 1** Locate the music on hold server by using the procedure in the [“Finding a Music On Hold Server” section on page 12-23](#).
- Step 2** Click the music on hold server that you want to reset.
- Step 3** Click the **Reset** button.
- A popup window displays an information message.
- Step 4** After reading the message, click **Restart** to restart the music on hold server or click **Reset** to reset the music on hold server.
- Step 5** To close the popup window, click **Close**.
-

Additional Information

See the [“Related Topics” section on page 12-31](#).

Music On Hold Server Configuration Settings

Table 12-7 describes the configuration settings that are used for configuring Music On Hold servers.

Table 12-7 Music On Hold Server Configuration Settings

Field	Description
Device Information	
Host Server	For existing music on hold servers, this field serves for display only.
Music On Hold Server Name	Enter a unique name for the music on hold server in this required field. This name can comprise up to 15 characters. Valid characters include letters, numbers, spaces, dashes, dots (periods), and underscores.
Description	Enter a description for the music on hold server. This description can comprise up to 50 characters. Ensure Description does not contain ampersand (&), double quotes ("), brackets ([]), less than (<), greater than (>), or the percent sign (%).
Device Pool	Use this required field to choose a device pool for the music on hold server. To do so, click the drop-down arrow and choose a device pool from the list that displays.
Location	Choose the appropriate location for this MOH server. 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 MOH server consumes.
Maximum Half Duplex Streams	Enter a number in this required field for the maximum number of unicast music on hold streams that this music on hold server supports. This value determines the maximum number of devices that can be on unicast music on hold that is streamed from this music on hold server at any given time. Valid values range from 0 to 500.
Maximum Multicast Connections	Enter a number in this required field for the maximum number of multicast music on hold streams that this music on hold server supports. This value determines the maximum number of devices that can be on multicast music on hold that is streamed from this music on hold server at any given time. Valid values range from 1 to 999999.
Fixed Audio Source Device	Enter the device name of the fixed audio source device. This device serves as the per-server override that is used if the server has a special sound device installed.
Run Flag	Use this required field to choose a run flag for the music on hold server. To do so, click the drop-down arrow and choose Yes or No . Choosing No disables the music on hold server.

Table 12-7 Music On Hold Server Configuration Settings (continued)

Field	Description
Multicast Audio Source Information	
Enable Multicast Audio Sources on this MOH Server	Check or uncheck this check box to enable or disable multicast of audio sources for this music on hold server. Note If this MOH server belongs to a multicast media resource group, a message asks you to enable multicast on this MOH server or to update the specified media resource group(s) either by removing this MOH server or by changing the multicast setting of each listed group.
Base Multicast IP Address	If multicast support is needed, enter the base multicast IP address in this field. Valid IP addresses for multicast range from 224.0.1.0 to 239.255.255.255. Note IP addresses between 224.0.1.0 and 238.255.255.255 fall in the reserved range of IP multicast addresses for public multicast applications. Use of such addresses may interfere with existing multicast applications on the Internet. Cisco strongly recommends using IP addresses in the range that is reserved for administratively controlled applications on private networks (239.0.0.0 - 239.255.255.255).
Base Multicast Port Number	If multicast support is needed, enter the base multicast port number in this field. Valid multicast port numbers include even numbers that range from 16384 to 32766.
Increment Multicast on	Click Port Number to increment multicast on port number. Click IP Address to increment multicast on IP address. Note Use multicast by incrementing IP address as the preferred method in firewall situations. This results in each multicast audio source having a unique IP address and helps to avoid network saturation.
Selected Multicast Audio Sources	
	Only audio sources for which the Allow Multicasting check box was checked display in this listing. If no such audio sources exist, the following message displays: There are no Music On Hold Audio Sources selected for Multicasting. Click Configure Audio Sources in the top right corner of the page to select Multicast Audio Sources. From the Related Links drop-down list box, choose Configure Audio Sources and click Go.
No.	This field designates music on hold audio stream number that is associated with a particular multicast audio source. Only audio sources that are defined as allowing multicasting display.

Table 12-7 **Music On Hold Server Configuration Settings (continued)**

Field	Description
Audio Source Name	This field designates name of audio source that is defined as allowing multicasting.
Max Hops	For each multicast audio source, enter the maximum number of router hops through which multicast packets should pass. Valid values range from 1 to 15. Note Using high values can lead to network saturation. This field also gets identified as <i>Time to Live</i> .

Additional Information

See the “[Related Topics](#)” section on page 12-31.

Music On Hold Audio File Management Configuration

You can manage the audio files that the Music On Hold feature uses as audio sources. The **Media Resources > MOH Audio File Management** menu option allows the administrator to perform the following functions:

- Display a list of the MOH audio files that are stored on the system.
- Upload new MOH audio files.
- Delete MOH audio files.

Use the following topics to manage the music on hold audio source audio files:

- [Displaying Music On Hold Audio Files, page 12-28](#)
- [Uploading a Music On Hold Audio File, page 12-29](#)
- [Deleting a Music On Hold Audio File, page 12-30](#)

Additional Information

See the “[Related Topics](#)” section on page 12-31.

Displaying Music On Hold Audio Files

Use the following procedure to display a list of music on hold audio files that are stored on the system.

Procedure

-
- Step 1** In Cisco Unified CallManager Administration, choose **Media Resources > MOH Audio File Management**.

The Music On Hold Audio File Management window displays.

For each entry in the list of records, the following information displays:

- Check box—If the audio file can be deleted, a check box displays in the first column of the display.
- File Name—This column displays the audio file name.
- Length—This column displays the audio file length in minutes and seconds.
- File Status—This column displays the file status, including the following values:
 - Translation Complete—Files with this status uploaded successfully and are available for use as audio files for a music on hold audio source.
 - In Use—After you add a music on hold audio source that uses this audio file as its MOH audio source file, the file status for this audio file changes to *In Use*. You cannot delete files with this file status.

Additional Information

See the [“Related Topics”](#) section on page 12-31.

Uploading a Music On Hold Audio File

Perform the following procedure to upload a music on hold audio file. Uploading the audio file makes it available for use as a music on hold audio source. If you use the **Media Resources > Music On Hold Audio Source** menu option to add a new audio source, the addition makes the newly uploaded audio file available in the MOH Audio Source File drop-down list box.

Procedure

-
- Step 1** Choose **Media Resources > MOH Audio File Management**.
- The Music On Hold Audio File Management window displays.
- Step 2** Click the **Upload File** button.
- The Upload File popup window displays.
- Step 3** Choose one of the following options:
- If you know the path to a file that specifies an audio file, enter the path in the File field.
 - If you do not know the path and file name, search for the audio file by clicking the **Browse...** button to the right of the File field. After you find the audio file, click the desired audio file and click **Open**. The path to the chosen audio file displays in the File field of the Upload File popup window.
- Step 4** To upload the specified audio file, click **Upload**.
- After the audio file gets uploaded, the Upload Result window tells you the result of the upload.



Note

Uploading a file uploads the file to the Cisco Unified CallManager server and performs audio conversions to create codec-specific audio files for MOH. Depending on the size of the original file, processing may take several minutes to complete.

**Note**

Uploading an audio source file to an MOH server uploads the file only to one MOH server. You must upload an audio source file to each MOH server in a cluster by using Cisco Unified CallManager Administration on each server. MOH audio source files do *not* automatically propagate to other MOH servers in a cluster.

Step 5 To close the Upload Result window, click **Close**.

The newly uploaded audio file gets added to the list of audio files in the MOH Audio File Management window.

Additional Information

See the [“Related Topics” section on page 12-31](#).

Deleting a Music On Hold Audio File

Perform the following procedure to delete an existing music on hold audio file.

**Note**

You cannot delete MOH audio files that specify the *In Use* state. To delete such files, first use the **Media Resources > Music On Hold Audio Source** menu option to find MOH audio sources that use this audio file. Either delete those MOH audio sources or modify them, so they use a different audio file.

Procedure

Step 1 Choose **Media Resources > MOH Audio File Management**.

The Music On Hold Audio File Management window displays.

Step 2 Click the check box to the left of a music on hold audio file that you want to delete.

**Note**

You can click several audio files to delete multiple audio files at once. You can also click the **Select All** button to select all audio files for deletion. Use the **Clear All** button to deselect audio files that you have selected.

Step 3 Click the **Delete Selected** button.

A popup window warns that this file will be deleted permanently.

Step 4 To complete the deletion, click **OK**.

The audio file gets deleted from the list of music on hold audio files.

Additional Information

See the [“Related Topics” section on page 12-31](#).

Related Topics

- [Understanding Music On Hold, page 12-1](#)
- [Music On Hold Definitions, page 12-2](#)
- [Music On Hold Characteristics, page 12-3](#)
- [Music On Hold Functionality, page 12-4](#)
- [Supported Music On Hold Features, page 12-5](#)
- [Music On Hold System Requirements and Limits, page 12-12](#)
- [Music On Hold Failover and Fallback, page 12-13](#)
- [Music On Hold Configuration Checklist, page 12-14](#)
- [Monitoring Music On Hold Performance, page 12-15](#)
- [Viewing Music On Hold Server Performance, page 12-15](#)
- [Media Resource Group Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0\(4\)*](#)
- [Media Resource Group List Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0\(4\)*](#)

Music On Hold Audio Sources

- [Music On Hold Audio Sources, page 12-8](#)
- [Storing Audio Source Files, page 12-9](#)
- [Finding a Music On Hold Audio Source, page 12-17](#)
- [Configuring a Music On Hold Audio Source, page 12-18](#)
- [Deleting a Music On Hold Audio Source, page 12-19](#)
- [Music On Hold Audio Source Configuration Settings, page 12-19](#)

Fixed Music On Hold Audio Source

- [Fixed Music On Hold Audio Source Configuration, page 12-21](#)
- [Configuring the Fixed Music On Hold \(MOH\) Audio Source, page 12-22](#)
- [Deleting a Fixed Music On Hold \(MOH\) Audio Source, page 12-22](#)
- [Fixed Music On Hold \(MOH\) Audio Source Configuration Settings, page 12-23](#)

Music On Hold Servers

- [Music On Hold Server, page 12-8](#)
- [Music On Hold Server Configuration, page 12-23](#)
- [Finding a Music On Hold Server, page 12-23](#)
- [Configuring a Music On Hold Server, page 12-24](#)
- [Resetting or Restarting a Music On Hold Server, page 12-25](#)
- [Music On Hold Server Configuration Settings, page 12-26](#)

Music On Hold Audio File Management

- [Music On Hold Audio File Management Configuration, page 12-28](#)
- [Displaying Music On Hold Audio Files, page 12-28](#)
- [Uploading a Music On Hold Audio File, page 12-29](#)
- [Deleting a Music On Hold Audio File, page 12-30](#)

Additional Cisco Documentation

- *Installing Cisco Unified CallManager Release 5.0(4)*
- *Upgrading Cisco Unified CallManager Release 5.0(4)*
- *Cisco Unified CallManager Serviceability Administration Guide*
- *Cisco Unified CallManager Serviceability System Guide*



Immediate Divert

The Immediate Divert (iDivert) feature allows you to immediately divert a call to a voice-messaging system. When the call gets diverted, the line becomes available to make or receive new calls.

Although immediate divert is not available to CTI applications, the CTI feature Transfer to Voicemail performs the same function as immediate divert but performs the function for CTI applications that third-party developers develop.

Access the Immediate Divert feature by using the iDivert softkey. Configure this softkey by using the Softkey Template Configuration window of Cisco Unified CallManager Administration. The softkey template gets assigned to phones that are in the Cisco Unified CallManager system.

This chapter provides the following information about immediate divert:

- [Introducing Immediate Divert, page 13-1](#)
- [System Requirements for Immediate Divert, page 13-2](#)
- [Immediate Divert Scenarios with Use Legacy Immediate Divert Service Parameter Set to False, page 13-5](#)
- [Installing and Activating Immediate Divert, page 13-9](#)
- [Configuring Immediate Divert, page 13-9](#)
- [Setting the Service Parameters for Immediate Divert, page 13-10](#)
- [Related Topics, page 13-11](#)

Introducing Immediate Divert

Consider immediate divert, a Cisco Unified CallManager supplementary service, as available for general use within the system. Immediate divert does not require the user to log in to make the iDivert softkey available on the phone.

Legacy iDivert allows diversion of a call to the voice mailbox of the party that invokes the iDivert feature. Enhanced iDivert allows diversion of a call to either the voice mailbox of the party that invokes the iDivert feature or to the voice mailbox of the original called party.

You can divert inbound calls that are in the call offering, call on hold, or call active states. You can divert outbound calls in the call active or call hold states. The diverted party receives the greeting of the voice-messaging system of the party to whom the call gets diverted.

When enhanced iDivert mode is active for incoming calls, the user to whom a call is presented can invoke immediate divert to divert the call either to the voice mailbox of the user or to the voice mailbox of the original called party. After the invoking user presses the iDivert softkey, a screen on the invoking user phone identifies both the original called party and the invoking user. The user selects one of the two names, and the call gets redirected to the voice mailbox of the selected party.

**Note**

When users invoke the Immediate Divert feature to divert an incoming call, they receive the choice of the original called party only if the Use Legacy Immediate Divert clusterwide service parameter is set to False. See the [“Setting the Service Parameters for Immediate Divert” section on page 13-10](#).

Immediate divert coexists with the Transfer to Voicemail feature.

System Requirements for Immediate Divert

Immediate divert requires the following software component to operate:

- Cisco Unified CallManager 5.0 or later

The following SCCP and SIP phones support immediate divert by using the iDivert softkey that is configured in any Cisco Unified CallManager softkey template:

- Cisco Unified IP Phones (Models 7905, 7911, 7912, 7920, 7940, 7941, 7960, 7961, 7970, 7971)

The following voice-messaging systems support immediate divert:

- Voice-messaging systems such as Unity that use the skinny protocol
- Voice-messaging systems such as Octel that use SMDI

Call-Processing Requirements for Immediate Divert

The following sections describe call-processing requirements for immediate divert:

- [Softkey Requirements, page 13-2](#)
- [Requirements for Incoming Calls, page 13-3](#)
- [Requirements for Outgoing Calls, page 13-3](#)

Softkey Requirements

Because the iDivert softkey does not automatically get configured in a softkey template, use the Softkey Template Configuration window in Cisco Unified CallManager Administration to configure the iDivert softkey in any available softkey template. You can configure the iDivert softkey in the following call states:

- Connected
- On hold
- Ring in

**Note**

The ring-in state in the softkey template represents the call-offering state in the phone call state.

Use the Phone Configuration window in Cisco Unified CallManager Administration to assign the softkey template that contains the iDivert softkey to a phone.

For information about softkey template configuration, see Softkey Template Configuration in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*. For information about assigning softkey templates to phones, see Cisco Unified IP Phone Configuration in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

Requirements for Incoming Calls

The following list gives called party types in the call-forwarding chain that immediate divert supports:

- Party A calls party B.
- Party B forwards to party C.
- Party C forwards to party D.

Party B represents the original called party. Party C represents the last redirecting party. Party D represents the last called party.

Immediate divert supports the following incoming call states:

- Call offering
- Call on hold
- Call active

When the called party presses the iDivert softkey and the Use Legacy Immediate Divert clusterwide service parameter is set to True, immediate divert redirects the incoming call to the voice-messaging mailbox that is associated with the called party. You can administer a voice-messaging mailbox for the called party through the voice-messaging profile that is assigned to the directory number of the called party.

When the called party presses the iDivert softkey and the Use Legacy Immediate Divert clusterwide service parameter is set to False, immediate divert may allow the called party to select the destination voice mailbox. A screen gets presented to the called party if the call had previously diverted (see the [“Interactions” section on page 13-6](#)). The called party can choose to divert the call to the voice-messaging mailbox of the original called party or to the voice-messaging mailbox that is associated with the called party. You may administer a voice-messaging mailbox for the original called party or for the called party through the voice-messaging profile that is assigned to the associated directory numbers.

For information about voice messaging, see Cisco Voice-Mail Pilot Configuration and Voice-Mail Profile Configuration in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*, and Voice Mail Connectivity to Cisco Unified CallManager in the *Cisco Unified CallManager System Guide, Release 5.0(4)*.

Requirements for Outgoing Calls

Immediate divert supports the following outgoing call states:

- Call on hold
- Call active

When the calling party presses the iDivert softkey, immediate divert redirects an outgoing call to the voice-messaging mailbox that is associated with the calling party. You may administer a voice-messaging mailbox for the calling party through the voice-messaging profile that is assigned to the directory number of the calling party.

For information about voice messaging, see Cisco Voice-Mail Pilot Configuration and Voice-Mail Profile Configuration in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*, and Voice Mail Connectivity to Cisco Unified CallManager in the *Cisco Unified CallManager System Guide, Release 5.0(4)*.

Immediate Divert Phone Display Messages

Immediate divert displays the following messages on the IP phone to indicate the status of an immediate divert action:

- Key is not active—The voice-messaging profile of the user who pressed iDivert does not have a voice-messaging pilot.
- Temporary failure—The voice-messaging system does not work, or a network problem exists.
- Busy—This message indicates that a voice-messaging system is busy.

Using Immediate Divert

The following scenarios provide examples of using the Immediate Divert feature. Scenario 1 through scenario 6 assume that the Use Legacy Immediate Divert clusterwide service parameter is set to True. Scenario 7 through scenario 8 assume that the Use Legacy Immediate Divert clusterwide service parameter is set to False. Scenario 9 assumes the Use Legacy Immediate Divert clusterwide service parameter is set to False and the Auto Call Pickup Enabled clusterwide service parameter is set to False.

Immediate Divert Scenarios with Use Legacy Immediate Divert Service Parameter Set to True

Scenario 1: Called Party Presses iDivert Softkey

1. Party A calls Manager A.
2. Manager A presses the iDivert softkey (call-offering state).
3. Immediate divert diverts the call to Manager A voice-messaging mailbox.
4. Party A receives the voice-messaging mailbox greeting of Manager A.

Scenario 2: Voice-Messaging Profile of an Original Called Party Does Not Have Voice-Messaging Pilot

1. Party A calls Party B.
2. The call gets forwarded to the personal line of Assistant B.
3. Assistant B presses the iDivert softkey (call-offering state).
4. Immediate divert diverts the call to Assistant B voice-messaging mailbox. Party B does not have a voice-messaging pilot number that is configured, but Assistant B does.
5. Party A receives the voice-messaging mailbox greeting of Assistant B.

Scenario 3: Manager A Forwards a Call to Manager B

1. Party A calls Manager A.
2. Manager A has line forwarded to Manager B.
3. Manager B presses the iDivert softkey (call-offering state).

4. Immediate divert diverts the call to Manager B voice-messaging mailbox.
5. Party A receives the voice-messaging mailbox greeting of Manager B.

Scenario 4: Voice-Messaging Port That Is Defined in a Voice-Messaging Profile Is Busy

1. Party A calls Party B.
2. Party B presses the iDivert softkey (call offering state).
3. Immediate divert cannot divert the call to the voice-messaging mailbox because the voice-messaging port is busy.
4. Party B sees the message Busy on the IP phone.
5. The original call remains in the call-offering state.

Scenario 5: Calling Party Calls a Call Center That Uses a Hunt Pilot Number

1. Party A calls Hunt List A.
2. Hunt List A member presses the iDivert softkey (call offering state), which is greyed out.
3. Immediate divert cannot divert the call to the voice-messaging mailbox because Hunt List A does not have a voice-messaging profile.
4. Hunt List A member sees the *Key is Not Active* message on the IP phone display.

Scenario 6: Calling Party B Transfers a Call to Party C on Different Cisco Unified CallManager Cluster

1. Party A calls Party B.
2. Party B transfers the call to Party C on a different Cisco Unified CallManager cluster.
3. Party C answers the incoming call.
4. Party C presses the iDivert softkey.
5. Party A receives the voice-messaging mailbox greeting of Party C.

Immediate Divert Scenarios with Use Legacy Immediate Divert Service Parameter Set to False

Scenario 7: Calling Party A Calls Party B, and Party B Forwards the Call to Party C

1. Party A calls Party B.
2. Party B phone forwards the call to Party C.
3. Party C gets presented with the incoming call and presses the iDivert softkey.
4. Party C presses the iDivert softkey.
5. Party C IP Phone displays a message that offers the choice of diverting to Party B voice-messaging mailbox or Party C voice-messaging mailbox.
6. Party C chooses the voice-messaging mailbox of Party B.
7. Party A receives the voice-messaging mailbox greeting of Party B.

Scenario 8: Calling Party Calls a Call Center That Uses a Hunt Pilot Number

1. Party A calls Hunt List A.
2. Hunt List A member presses the iDivert softkey (call offering state).

3. Immediate divert diverts the call to the voice-messaging mailbox of the hunt list A member that invokes the iDivert feature.
4. Party A receives the voice-messaging mailbox greeting of Hunt List A member.

Scenario 9: Auto Call Pickup Enabled Clusterwide Service Parameter is Set to False, And a User is in a Call Pickup Group

1. Party B, Party C, and Party D exist in the same call pickup group.
2. Party A calls Party B.
3. Party B IP phone rings but Party B does not answer the call.
4. Party C uses call pickup to answer the call.
5. If Party C presses the iDivert softkey during alerting state, connected state, or on hold state, the IP phone display gets presented to Party C. Party C can choose between two options: iDivert the call to the original called party voice-messaging mailbox (Party B) or iDivert the call to the last called party voice-messaging mailbox (Party C).



Note

If the Use Legacy Immediate Divert clusterwide service parameter is set to False, and the Auto Call Pickup Enabled clusterwide service parameter is set to True, and a user of a call pickup group uses call pickup to answer a call, the IP phone display will not present any choices to the user when the iDivert softkey is pressed.

Interactions and Restrictions

The following sections describe the interactions and restrictions for immediate divert:

- [Interactions, page 13-6](#)
- [Restrictions, page 13-8](#)

Interactions

The following sections describe how immediate divert interacts with Cisco Unified CallManager applications and call processing:

- [Multilevel Precedence and Preemption \(MLPP\), page 13-7](#)
- Setting the Service Parameters for Call Park, *Cisco Unified CallManager Features and Services Guide, Release 5.0(4)*
- [Call Forward, page 13-7](#)
- [Call Detail Records \(CDR\), page 13-7](#)
- [Conference, page 13-7](#)
- [Hunt List, page 13-7](#)

Multilevel Precedence and Preemption (MLPP)

The following interactions occur between immediate divert and MLPP:

- Immediate divert diverts calls to voice-messaging mailboxes regardless of the type of call (for example, a precedence call).
- When Alternate Party Diversion (call precedence) is activated, Call Forward No Answer (CFNA) gets deactivated.

Call Forward

When the Forward No Answer setting on the Directory Number Configuration window is not configured, call forward uses the clusterwide CFNA timer service parameter, Forward No Answer Timer. If a user presses the iDivert softkey at the same time as the call is being forwarded, the call gets diverted to an assigned call forward directory number (because the timer was too short), not the voice-messaging mailbox. To solve this situation, set the CFNA timer service parameter to enough time (for example, 60 seconds). If the iDivert screen has been presented to the iDivert invoker and the CFNA timer expires, the call forwards onward.

Call Detail Records (CDR)

Immediate divert uses the immediate divert code number in the Onbehalf of fields (for example, joinOnbehalfOf and lastRedirectRediectOnBehalfOf) in CDR.

Conference

When a conference participant presses the iDivert softkey, the remaining conference participants receive the voice-messaging mailbox greeting of the immediate divert initiator. Conference types include Ad Hoc, Meet-Me, Barge, cBarge, and Join.

Hunt List

Immediate divert works as follows for DN's that are members of a line group:

- Ensure the iDivert softkey is enabled
- For calls that reach the phone directly through a hunt list pilot (as part of the hunting algorithms), the iDivert softkey will appear grayed out if the Use Legacy Immediate Divert clusterwide parameter is set to True; otherwise, it does not appear grayed out.
- For calls that do not reach the phone directly through a hunt list pilot (as part of the hunting algorithms), the iDivert softkey does not appear grayed when the Use Legacy Immediate Divert clusterwide parameter is set to True or False. (This includes scenarios where a call was made to a hunt list pilot, the hunt list was exhausted, and the call followed the forwarding disposition to the DN that also happens to be a member of a hunt group. This would represent a case where a call reaches a member of a hunt group indirectly through a hunt list pilot.)

Restrictions

The following restrictions apply to immediate divert:

- Immediate divert supports QSIG devices (QSIG-enabled H-323 devices, MGCP PRI QSIG T1 gateways, and MGCP PRI QSIG E1 gateways), depending on the setting of the Use Legacy Immediate Divert and Allow QSIG During iDivert clusterwide service parameters. See the [“Setting the Service Parameters for Immediate Divert” section on page 13-10](#) for details. When iDivert is allowed over QSIG trunks, follow these guidelines: when you use QSIG integration with your voice-messaging system, a voice mail profile that includes either a voice mail pilot or a voice mail mask or both should leave the “Make this the default Voice Mail Profile for the System” check box unchecked. Ensure the default Voice Mail Profile setting is always set to No Voice Mail.
- When Call Forward All (CFA) and Call Forward Busy (CFB) are activated, the system does not support immediate divert (CFA and CFB have precedence over immediate divert).
- When it reaches a voice-messaging system over a local/SCCP connection, iDivert can detect a busy condition on the voice-messaging ports. (The call cannot divert to a busy voice-messaging system, but the original call gets maintained. Busy will display on the phone on which iDivert was invoked to indicate that the call was not diverted.) When a voice-messaging system is reached over a QSIG or SIP trunk, iDivert can be detected, but the call does not get maintained. When the Allow QSIG During iDivert clusterwide service parameter is set to True, or the Use Legacy Immediate Divert clusterwide service parameter is set to False, immediate divert supports access to voice-messaging systems that can be reached over QSIG/SIP trunks. When the Allow QSIG During iDivert clusterwide service parameter is set to False, and the Use Legacy Immediate Divert clusterwide service parameter is set to True, immediate divert does not support access to voice-messaging systems over QSIG or SIP trunks. Immediate divert cannot divert a call to a busy voice-messaging port; however, voice-messaging ports can exist as members of a route/hunt list, thus reducing the busy port scenario.
- If the Use Legacy Immediate Divert clusterwide service parameter is set to True, members of a hunt list can invoke iDivert if the call is direct. They cannot invoke iDivert if they are reached as a member of a line group. The message, Key is Not Active, displays on the IP phone.
- When Cisco Unified CallManager goes down, users cannot leave voice messages unless a media path was established between a redirected party and the voice-messaging system before the Cisco Unified CallManager went down.
- System does not support using Malicious Caller ID and Immediate Divert features together.
- CTI applications do not have immediate divert available (applications use Transfer to Voicemail).
- Use the Call Park Display Timer service parameter to control the timer for the immediate divert text display on the IP phones. When the service parameter gets changed, the text display timer for immediate divert also gets changed.
- See the [“Multilevel Precedence and Preemption \(MLPP\)” section on page 13-7](#) for restrictions about using MLPP.
- A race condition in connection with the Forward No Answer Timeout exists when the iDivert softkey gets pressed. For example, if a manager presses the iDivert softkey immediately after the Forward No Answer timeout, call forward forwards the call to a preconfigured directory number. However, if the manager presses the iDivert softkey before the Forward No Answer timeout, immediate divert diverts the call to the voice-messaging mailbox of the manager.

- The calling and called parties can divert the call to their voice-messaging mailboxes if both simultaneously press the iDivert softkey. The voice-messaging mailbox of the calling party would contain a portion of the outgoing greeting of the called party. Similarly, the voice-messaging mailbox of the called party would contain a portion of the outgoing greeting of the calling party.
- When one participant in a conference presses the iDivert softkey, all remaining participants receive an outgoing greeting of the participant who pressed iDivert. Conference types include Meet-Me, Ad Hoc, cBarge, and Join.
- If the last action on a call was Auto Pickup, Call Transfer, Call Park, Call Park Reversion, Conference, Meet-Me Conference, or any application that performs a split or join operation, enhanced iDivert does not present a screen to a called party to choose the voice-messaging mailbox. Instead, enhanced iDivert immediately diverts the call to the voice-messaging mailbox that is associated with the called party.
- When iDivert is allowed over QSIG trunks, follow these guidelines: when you use QSIG integration with your voice-messaging system, a voice mail profile that includes either a voice mail pilot or a voice mail mask or both should leave the “Make this the default Voice Mail Profile for the System” check box unchecked. Ensure the default Voice Mail Profile setting always gets set to No Voice Mail.

Installing and Activating Immediate Divert

Immediate Divert, a system feature, comes standard with Cisco Unified CallManager software. Immediate divert does not require special installation.

Configuring Immediate Divert

This section contains the following information:

- [Immediate Divert Configuration Checklist, page 13-9](#)
- [Setting the Service Parameters for Immediate Divert, page 13-10](#)

Immediate Divert Configuration Checklist

[Table 13-1](#) provides a checklist to configure immediate divert.

Table 13-1 Immediate Divert Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	Change the Call Park Display Timer clusterwide service parameter if the default is not appropriate.	Setting the Service Parameters for Immediate Divert, page 13-10
Step 2	Change the Use Legacy Immediate Divert clusterwide service parameter if the default is not appropriate.	Setting the Service Parameters for Immediate Divert, page 13-10
Step 3	Change the Allow QSIG During iDivert clusterwide service parameter if the default is not appropriate.	Setting the Service Parameters for Immediate Divert, page 13-10
Step 4	Change the Immediate Divert User Response Timer service parameter if the default is not appropriate.	Setting the Service Parameters for Immediate Divert, page 13-10

Table 13-1 Immediate Divert Configuration Checklist (continued)

Configuration Steps		Related procedures and topics
Step 5	Using the Directory Number Configuration window, associate a voice-mail profile to each user who will have access to immediate divert. Note This step assumes that voice-mail profiles and pilots are configured. See Configuring a Voice-Mail Profile and Configuring the Voice-Mail Pilot Number. in the <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> .	Configuring a Directory Number, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 6	Assign the iDivert softkey to the Standard User or Standard Feature softkey template. Assign the softkey in the On Hook, Connected, On Hold, and Ring In states.	Softkey Template Configuration, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 7	Using the Phone Configuration window, assign the Standard User or Standard Feature softkey template, to which you added the iDivert softkey, to each device that has immediate divert access. Tip To make the iDivert softkey available to many users, configure a softkey template with the iDivert softkey; then, assign that softkey template to a device pool and, finally, assign that device pool to all users who need iDivert.	Configuring Cisco Unified IP Phones, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 8	Notify users that the Immediate Divert feature is available.	Refer to the phone documentation for instructions on how users access immediate divert on their Cisco Unified IP Phone.

Setting the Service Parameters for Immediate Divert

The behavior of the Immediate Divert feature depends on the setting for various service parameters. Descriptions of the service parameters that affect the Immediate Divert feature follow.

Call Park Display Timer Clusterwide Service Parameter

Immediate divert uses the Cisco Unified CallManager clusterwide service parameter Call Park Display Timer. The default for this service parameter specifies 10 seconds. Use the Call Park Display Timer service parameter to control the timer for the immediate divert text display on the IP phones. When the service parameter gets changed, the text display timer for immediate divert also changes. Set this timer for each server in a cluster that has the Cisco CallManager service and immediate divert configured.

For information about text displays, see the [“Immediate Divert Phone Display Messages”](#) section on page 13-4.

Use Legacy Immediate Divert Clusterwide Service Parameter

Immediate divert allows diversion of an incoming call to either the voice mailbox of the original called party or to the voice mailbox of the user that invokes the iDivert feature only if the Use Legacy Immediate Divert clusterwide service parameter is set to False. If the Use Legacy Immediate Divert service parameter is set to True, the user that invokes the iDivert feature can divert an incoming call only to his own voice mailbox.

Setting the Use Legacy Immediate Divert service parameter to False allows access to voice-messaging systems that are reached over QSIG.

Allow QSIG During iDivert Clusterwide Service Parameter

Immediate divert diverts calls to voice-messaging systems that can be reached over QSIG, SIP, and QSIG-enabled H.323 devices if the Allow QSIG During iDivert clusterwide service parameter is set to True.

Immediate Divert User Response Timer Service Parameter

The value of the Immediate Divert User Response Timer service parameter determines the length of time that the invoker of the iDivert softkey is given to choose the party to whom to divert a call. If the invoker does not choose a party, the call remains connected.

Where to Find More Information

Additional Cisco Documentation

- Cisco Unified IP Phone administration documentation for Cisco Unified CallManager
- Cisco Unified IP Phone user documentation

Additional Information

See the [“Related Topics” section on page 13-11](#).

Related Topics

- Cisco Unified IP Phone Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Softkey Template Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Cisco Voice-Mail Pilot Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Voice-Mail Profile Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Voice Mail Connectivity to Cisco Unified CallManager, *Cisco Unified CallManager System Guide, Release 5.0(4)*



Cisco Unified CallManager Attendant Console

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.

The attendant console installs on a PC with IP connectivity to the Cisco Unified CallManager system. The attendant console works with a Cisco Unified IP Phone that is registered to a Cisco Unified CallManager system. Multiple attendant consoles can connect to a single Cisco Unified CallManager system. When a server fails, the attendant console automatically connects to another server in the cluster.

The application registers with and receives call-dispatching, login, line state, and directory services from the Cisco CallManager Attendant Console Server service on the Cisco Unified CallManager server. Cisco Unified CallManager Attendant Console receives calls that are made to a virtual directory number that is called a pilot point and directs calls to a list of destinations in a hunt group. You can configure the order in which members of the hunt group receive calls and whether Cisco Unified CallManager Attendant Console queues calls when all attendants are busy.

This section contains the following topics:

- [Introducing Cisco Unified CallManager Attendant Console, page 14-1](#)
- [System Requirements for Cisco Unified CallManager Attendant Console, page 14-12](#)
- [Interactions and Restrictions, page 14-13](#)
- [Installing and Activating Cisco Unified CallManager Attendant Console, page 14-16](#)
- [Configuring Cisco Unified CallManager Attendant Console, page 14-16](#)
- [Dependency Records, page 14-40](#)
- [Related Topics, page 14-40](#)
- [Related Topics, page 14-40](#)

Introducing Cisco Unified CallManager Attendant Console

The following sections provide information about the Cisco Unified CallManager Attendant Console feature:

- [Understanding Cisco Unified CallManager Attendant Console Users, page 14-2](#)
- [Understanding Pilot Points and Hunt Groups, page 14-2](#)

- [Understanding Call Queuing](#), page 14-9
- [Understanding the Cisco Unified CallManager Attendant Console Directory](#), page 14-9
- [Understanding the Cisco CallManager Attendant Console Server Service](#), page 14-10
- [Cisco Unified CallManager Attendant Console Redundancy](#), page 14-11
- [Firewall Support for Attendant Console](#), page 14-12

Understanding Cisco Unified CallManager Attendant Console Users

Before a user can log in to an attendant console to answer and direct calls, you must add the user as an attendant console user and optionally assign a password to the user. You can add or delete attendant console users and modify user IDs and password information in the Cisco Unified CallManager Attendant Console User Configuration window in Cisco Unified CallManager Administration.

**Note**

Be aware that attendant console user IDs and passwords are not the same as directory users and passwords that are entered in the End User Configuration window in Cisco Unified CallManager Administration.

If a user cannot log in to the attendant console, make sure that Cisco CallManager and Cisco CallManager Attendant Console Server services are both running. Verify that the user has been added in the Cisco Unified CallManager Attendant Console User Configuration area of Cisco Unified CallManager Administration and that the correct user name and password are specified in the Login dialog box in the attendant console client application.

In addition to configuring Cisco Unified CallManager Attendant Console users, you must configure one Attendant Console application user and associate the attendant phones with the user. If you do not configure this user, the attendant console cannot interact with CTIManager. For information on setting up the Attendant Console application user in Cisco Unified CallManager Administration, see the [“Enabling Device Security for Cisco Unified CallManager Attendant Console”](#) section on page 14-21.

You must also create an application user for device authorization and associate phone with that application user.

Understanding Pilot Points and Hunt Groups

A pilot point, a virtual directory number that is never busy, alerts the Cisco Unified CallManager Attendant Console to receive and direct calls to hunt group members. A hunt group comprises a list of destinations that determine the call redirection order.

**Note**

Cisco Unified CallManager Attendant Console does not route calls to an instance of a shared line on attendant phone if any other instances of the shared line are in use.

For Cisco Unified CallManager Attendant Console to function properly, make sure that the pilot point number is unique throughout the system (it cannot be a shared line appearance). When configuring the pilot point, you must choose one of the following routing options:

- **First Available Hunt Group Member**—Cisco Unified CallManager Attendant Console goes through the members in the hunt group in order until it finds the first available destination for routing the call. You can choose this routing option from the Pilot Point Configuration window in Cisco Unified CallManager Administration.
- **Longest Idle Hunt Group Member**—This feature arranges the members of a hunt group in order from longest to shortest idle time. Cisco Unified CallManager Attendant Console finds the member with the longest idle time and, if available, routes the call. If not, Cisco Unified CallManager Attendant Console continues to search through the group. This feature evenly distributes the incoming call load among the members of the hunt group. You can choose this routing option from the Pilot Point Configuration window in Cisco Unified CallManager Administration.

If the voice-mail number is the longest idle member of the group, Cisco Unified CallManager Attendant Console routes the call to a voice-messaging system without checking the other members of the group first.

- **Circular Hunting**—Cisco Unified CallManager Attendant Console maintains a record of the last hunt group member to receive a call. When a new call arrives, Cisco Unified CallManager Attendant Console routes the call to the next hunt group member in the hunt group.
- **Broadcast Hunting**—When a call arrives at the pilot point, Cisco Unified CallManager Attendant Console answers the call, places the call on hold, adds the call to the queue, and displays the call in the Broadcast Calls window on attendant PCs. While on hold, the caller receives music on hold, if it is configured. Any attendant can answer the call from the Broadcast Calls window.

**Note**

In the Pilot Point Configuration window in Cisco Unified CallManager Administration, you must choose a device pool that is associated with the pilot point for pilot point redundancy to work.

When you update a pilot point, make sure that you reset the pilot point. Call processing continues to occur when you reset it.

When a call comes into a pilot point, Cisco Unified CallManager Attendant Console uses the hunt group list and the selected call routing method for that pilot point to determine the call destination. During hunt group configuration, you must specify one of the following options for each hunt group member:

- **Directory number (device member)**

If a directory number is specified, Cisco Unified CallManager Attendant Console only checks whether the line is available (not busy) before routing the call.

- **Attendant console user plus a line number (user member)**

When you specify a user and line number, the user can log in to and receive calls on any Cisco Unified IP Phone in the cluster that the attendant console controls.

If a user and line number are specified, Cisco Unified CallManager Attendant Console confirms the following details before routing the call:

- That the user is logged in to the attendant console
- That the user is online
- That the line is available

The attendant can only answer calls on the line number that you specify if that line number is configured on the phone that the attendant used to log in to the attendant console.

**Caution**

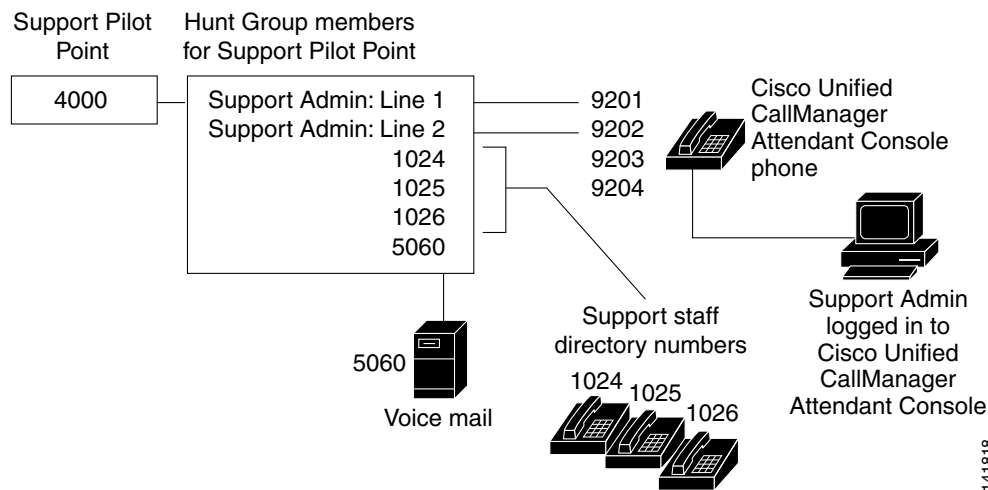
To handle overflow conditions, configure your hunt groups, so Cisco Unified CallManager Attendant Console route calls to one or more attendant consoles or voice-messaging numbers. To ensure that the voice-messaging number can handle more than one call at a time, check the Always Route Member check box in the Hunt Group Configuration window.

You can also handle overflow conditions by enabling call queuing. For more information about call queuing, see [“Understanding Call Queuing”](#) section on page 14-9.

Example 1 Pilot Points and Hunt Groups Working Together

Assume a pilot point named Support exists at directory number 4000. The hunt group for the Support pilot point contains the following members:

- Support Admin, Line 1 and Support Admin, Line 2 (Support Admin represents the attendant console login for the administrative assistant for Support.)
- Three directory numbers for support staff; that is, 1024, 1025, and 1026, listed in the hunt group in that order
- A voice-messaging number, 5060, which is the final member of the hunt group

Figure 14-1 Pilot Point and Hunt Group Example

As shown in [Figure 14-1](#), the following example describes a simple call-routing scenario where the user chose First Available Hunt Member during the configuration of the pilot point:

1. The Cisco Unified CallManager Attendant Console receives a call and directs it to the Support Pilot Point, directory number 4000.
2. Because 4000 is a pilot point and First Available Hunt Group Member is chosen as the call-routing option, the Cisco Unified CallManager Attendant Console that is associated with the pilot point checks the members of the hunt group in order, beginning with Support Admin, Line 1.

Cisco Unified CallManager Attendant Console determines that the Support Admin user is not online, directory number 1024 is busy, directory number 1025 is busy, and directory number 1026 is available.

3. Cisco Unified CallManager Attendant Console routes the call to the first available directory number, which is 1026. Because 1026 is available, the Cisco Unified CallManager Attendant Console never checks the 5060 number.

Understanding Linked Hunt Groups

Linking hunt groups together allows the Cisco Unified CallManager Attendant Console to search through more than one hunt group when calls are routed. When configured properly, pilot points create a link between hunt groups. Cisco Unified CallManager Attendant Console searches each hunt group according to the call-routing method that was chosen during configuration.

Consider the following guidelines when you are linking hunt groups together:

- Configure the individual pilot points and hunt groups first.
- For all except the last hunt group, make sure that the final member of the hunt group is the pilot point for the next hunt group. The pilot point from each group creates a link between the hunt groups, as seen in [Figure 14-2](#).
- To handle overflow conditions, choose a voice-messaging or auto-attendant number as the final member of the last linked hunt group in the chain. If Cisco Unified CallManager Attendant Console cannot route the call to any other members in the hunt groups, the call goes immediately to the voice-messaging number in the final hunt group.
- Check the Always Route Member check box in the Hunt Group Configuration window for only the final member of each hunt group.



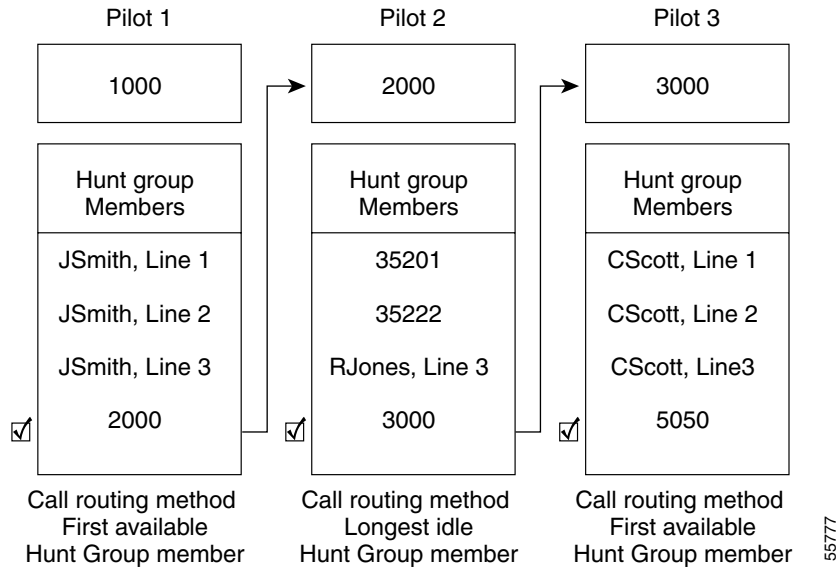
Caution

Cisco strongly recommends that you do *not* link the last hunt group back to the first hunt group.

Example 2 *Linked Hunt Groups Working Together*

Consider the following information that is shown in [Figure 14-2](#):

- Three pilot points that are numbered 1, 2, and 3 exist at directory numbers 1000, 2000, and 3000, respectively.
- The last hunt group member of Pilot 1 acts as the pilot point for Pilot 2, while the last hunt group member of Pilot 2 serves as the pilot point for Pilot 3.
- During hunt group configuration, the administrator checked Always Route Member for the last member of each hunt group.
- Each hunt group contains four members, including the linked pilot point.
- JSmith, RJones, and CScott designate attendant console users that are specified as user/line pairs in the hunt groups.
- In Pilot 2, two directory numbers, 35201 and 35222, exist.
- The final hunt group member of Pilot 3, voice-messaging number 5050, handles overflow conditions. The administrator checked Always Route Member when he configured this final hunt group member.

Figure 14-2 Linked Hunt Group Example

As represented in [Figure 14-2](#), the following example describes a simple call-routing scenario for linked hunt groups:

1. The Cisco Unified CallManager Attendant Console receives a call and directs it to the first pilot point of the chain, directory number 1000.
2. Because 1000 is a pilot point and First Available Hunt Group Member is chosen as the call-routing method, Cisco Unified CallManager Attendant Console checks the members in the hunt group in order, beginning with JSmith, Line 1. Cisco Unified CallManager Attendant Console determines that the first three members of the hunt group are unavailable and, therefore, routes the call to directory number 2000, the link to Pilot 2.
3. When the call reaches Pilot 2, Cisco Unified CallManager Attendant Console attempts to route the call to the longest idle hunt group member. Because directory numbers 35201 and 35222 are busy, and RJones, Line 3, is offline, Cisco Unified CallManager Attendant Console routes the call to the last member of the group, directory number 3000, the link to Pilot 3.
4. Cisco Unified CallManager Attendant Console searches through Pilot 3 to find the first available member who is not busy. When Cisco Unified CallManager Attendant Console determines that CScott, Line 2, is the first available member, Cisco Unified CallManager Attendant Console routes the call to that line. Cisco Unified CallManager Attendant Console never checks voice-messaging number 5050.

Understanding Circular Hunt Groups

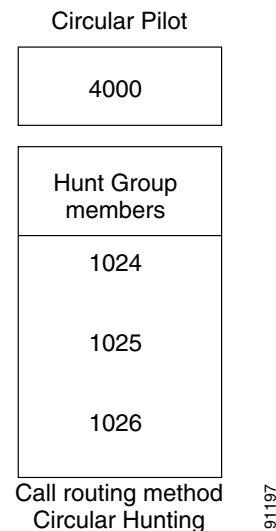
Circular hunt groups enable Cisco Unified CallManager Attendant Console to route calls on the basis of last hunt group member to receive a call. Each hunt group maintains a record of which hunt group member receives a call. When a new call arrives, Cisco Unified CallManager Attendant Console dispatches the call to the next hunt group member in the hunt group. In other words, Cisco Unified CallManager Attendant Console routes the first call to a hunt group to the first hunt group member, the second call to the second hunt group member, and so on. After the last hunt group member receives a call, Cisco Unified CallManager Attendant Console routes calls beginning with the first hunt group member again.

If you want to use circular hunting for linked hunt groups, set each of the pilot points of the linked hunt groups to circular hunting.

Example 3 Circular Hunting

Assume a pilot point that is named Circular exists at directory number 4000 and that you chose the Circular Hunting routing algorithm when you configured the pilot point. The hunt group for this pilot point contains the three directory numbers; that is, 1024, 1025, and 1026, listed in the hunt group in that order. Because the Always Route check box is not checked for any of the hunt group members, Cisco Unified CallManager Attendant Console determines whether the directory number is busy before routing the call.

Figure 14-3 Circular Hunting Example



As shown in [Figure 14-3](#), the following example describes a simple call-routing scenario where the user configured a Circular pilot point:

1. The Cisco Unified CallManager Attendant Console receives a call and directs it to the Circular pilot point, directory number 4000.
2. Because 4000 is a pilot point and Circular Hunting is chosen as the call-routing option, Cisco Unified CallManager Attendant Console routes the call to the first hunt group member, which is directory number 1024.
3. Cisco Unified CallManager Attendant Console receives another call and directs it to the Circular pilot point, directory number 4000.
4. Because Circular Hunting is chosen as the call-routing option and directory number 1024 received the last call, Cisco Unified CallManager Attendant Console attempts to route the call to the next hunt group member, which is directory number 1025.
5. Cisco Unified CallManager Attendant Console determines that directory number 1025 is busy and routes the call to the next hunt group member, directory number 1026.
6. Cisco Unified CallManager Attendant Console receives another call and directs it to the Circular pilot point, directory number 4000.

7. Because Circular Hunting is chosen as the call-routing option and directory number 1026 received the last call, Cisco Unified CallManager Attendant Console attempts to route the call to the next hunt group member, which is directory number 1024.

Understanding Broadcast Hunting

Broadcast hunting enables Cisco Unified CallManager Attendant Console to answer calls and place them into a queue. The attendant console displays the queued calls to all available attendants after inserting the calls into the queue and to all attendants that become available while the call is in the queue.



Note

The attendant console only broadcasts calls to attendants that are set up as user/line number hunt group members in the broadcast hunting pilot point.

The queued calls appear in the Broadcast Calls window on the attendant PC. While in the queue, the callers receive music on hold if you have chosen an audio source from the Network Hold Audio Source and the User Hold MOH Audio Source drop-down list boxes in the Device Pool window or the Pilot Point Configuration window.

Any attendant in the hunt group that is online can answer the queued calls. Cisco Unified CallManager Attendant Console does not automatically send the calls to an attendant. When an attendant answers a call, Cisco Unified CallManager Attendant Console removes the call from the Broadcast Calls window and displays it in the Call Control window of the attendant who answered the call.

You can specify the following values for each broadcast hunting pilot point:

- **Queue Size**—This field specifies the number of calls that are allowed in the queue. If the queue is full, Cisco Unified CallManager Attendant Console routes calls to the “always route” hunt group member that is specified on the Hunt Group Configuration window. If you do not specify an always route member, Cisco Unified CallManager Attendant Console drops the call when the queue size limit is reached.
- **Hold Time**—This field specifies the maximum time (in seconds) that Cisco Unified CallManager Attendant Console keeps a call in the queue. If the call is in the queue for longer than the “HoldTime,” the call gets redirected to the “AlwaysRoute” member. If you do not configure an always route member, the call remains in the queue until an attendant becomes available.

Example 14-4 Broadcast Hunting Example

Assume a pilot point named Service exists at directory number 1000 and supports broadcast hunting. The hunt group for this pilot contains the following members:

- Three user/line number pairs for service staff; that is, Mary Brown/Line #1, Joe Williams/Line #2, and Doris Jones/Line #1, listed in the hunt group in that order
- A voice-messaging number, 7060, which is the final member of the hunt group

The following example describes a simple call-routing scenario where the user chose Broadcast Hunting during the configuration of the pilot point:

1. The Cisco Unified CallManager Attendant Console receives a call and directs it to the Service Pilot Point, directory number 1000.
2. Because Broadcast is chosen as the call-routing option for the Service pilot point, the Cisco Unified CallManager Attendant Console that is associated with the pilot point checks the queue. Cisco Unified CallManager Attendant Console determines that the queue is not full and routes the call to the queue. The caller receives music on hold.

3. Cisco Unified CallManager Attendant Console checks the members of the hunt group in order, beginning with Mary Brown/Line #1. Cisco Unified CallManager Attendant Console determines that Mary Brown/Line #1 is available, Joe Williams/Line #2 is busy, and Doris Jones/Line #1 is available and, therefore, broadcasts the call to Mary Brown/Line #1 and Doris Jones/Line #1.
4. Mary Brown answers the call, and Cisco Unified CallManager Attendant Console removes the call from the queue.

Understanding Call Queuing

You can configure a pilot point to support call queuing, so when a call comes to pilot point and all hunt groups members are busy, Cisco Unified CallManager Attendant Console sends calls to a queue. While in the queue, the callers receive music on hold if you have chosen an audio source from the Network Hold Audio Source and the User Hold MOH Audio Source drop-down list boxes in the Device Pool window or the Pilot Point Configuration window. The attendants cannot view the queued calls. When a hunt group member becomes available, Cisco Unified CallManager Attendant Console redirects the call to that hunt group member.

You enable queuing for a pilot point by checking the Queuing Enabled check box on the Pilot Point Configuration window. You must also enter a value in the Queue Size field and the Hold Time (in Seconds) field. The queue size specifies the number of calls that are allowed in the queue. If the queue is full, Cisco Unified CallManager Attendant Console routes calls to the “always route” hunt group member that is specified on the Hunt Group Configuration window. If you do not specify an always route member, Cisco Unified CallManager Attendant Console drops the call when the queue size limit is reached. The hold time specifies the maximum time (in seconds) that Cisco Unified CallManager Attendant Console keeps a call in the queue. If the call is in the queue for longer than the “HoldTime,” the call gets redirected to “AlwaysRoute” member. If the “AlwaysRoute” member is not configured, no action occurs.

Understanding the Cisco Unified CallManager Attendant Console Directory

The attendant console server reads and caches directory entries at startup. After an initial handshake determines whether the directory entries changed since the previous log in, the attendant console downloads the directory user list. The attendant console also downloads the user list when the interval in the Directory Reload Interval field in the Attendant Settings dialog box expires or when the user clicks the Reload button in the Directory window.

The attendant console searches the following files (in order) for the user list:

- User list file that is specified in the Path Name of Local Directory File in the Attendant Settings dialog box on the attendant PC
- AutoGenerated.txt file that is generated by the Cisco Unified CallManager Attendant Console service and stored in the userlist directory on the Cisco Unified CallManager Attendant Console server when the Cisco CallManager Attendant Console Server service starts and when the directory sync period expires if the Directory Sync Period service parameter does not equal zero. The attendant console saves the file as CorporateDirectory.txt.

To modify the Directory Sync Period service parameter, choose **System > Service Parameters**. Choose the appropriate server from the Server drop-down list box and choose the Cisco CallManager Attendant Console Server service from the Service drop-down list box.

- CorporateDirectory.txt file that you import using the Cisco Unified CM Attendant Console User File Upload window (**Application > Cisco Unified CM Attendant Console > Cisco Unified CM Attendant Console User File Upload**). If you import a CorporateDirectory.txt file, it replaces the AutoGenerated.txt file created by the system.

The user list file exists in comma separate value (CSV) format and contains the following information:

- Last Name
- First Name
- Telephone Number
- Department

**Note**

Directory entries without telephone numbers do not display in the attendant console Directory window.

The attendant console server also stores per-attendant information such as speed-dial groups/entries and window positions in the database, which ensures that each attendant can use the per-attendant settings from any PC into which the attendant logs.

Additional Information

See the [“Related Topics” section on page 14-40](#).

Understanding the Cisco CallManager Attendant Console Server Service

The attendant console application registers with and receives call-dispatching services from the Cisco CallManager Attendant Console Server service. The CallManager Attendant Console Server service provides communication among Cisco Unified CallManager servers, attendant consoles, and the Cisco Unified IP Phones that are used with the attendant consoles.

**Note**

If you use the attendant console in a cluster environment, make sure that all Cisco Unified CallManagers within a cluster have the Cisco CallManager Attendant Console Server service activated and running. You must manually activate the service through Cisco Unified CallManager Serviceability. Attendant console redundancy requires this setup to work properly; however, not all Cisco CallManager Attendant Console Servers are required to have a route point.

Cisco CallManager Attendant Console Server handles attendant console requests for the following items:

- Call dispatching from pilot point to the appropriate hunt group destination
- Line status (unknown, available, on hook, or off hook)
- User directory information (Cisco CallManager Attendant Console Server stores and periodically updates directory information for fast lookup by the attendant console.)

**Note**

Cisco CallManager Attendant Console Server only monitors the status of internal devices and phones. An attendant console user cannot see line state for a phone that is connected to a gateway.

Cisco Unified CallManager Attendant Console Redundancy

Every time that the attendant opens the Cisco Unified CallManager Attendant Console, the following events occur:

- Cisco Unified CallManager Attendant Console connects to a Cisco Unified CallManager Attendant Console server and downloads the list of Cisco Unified CallManager servers in the attendant phone device pool.
- Cisco Unified CallManager Attendant Console caches the list of servers into the GlobalSettings.xml file that is located in C:\Program Files\Cisco\CallManager Attendant Console\data.
- Cisco Unified CallManager Attendant Console client application uses the server list to locate the servers that are running CTIManager. The list of CTI services provides scalability. Customer can provision a single machine as the call processing server (CTI server) instead of running the CTI service on the same machine as the Cisco CallManager service and the Cisco CallManager Attendant Console Server service.
- The Cisco Unified CallManager Attendant Console server inspects the Cisco Unified CallManager database and uses the list of Cisco Unified CallManager servers as the list of servers where the Cisco CallManager Attendant Console Server service should be active.

If a Cisco CallManager service fails, the following events occur:

- The attendant console that is attached to the failed server uses the list in the GlobalSettings.xml file to locate and connect to another Cisco Unified CallManager server.
- The Cisco CallManager Attendant Console Server service that is running on the Cisco Unified CallManager server takes over servicing of the route points that are associated with the failed Cisco Unified CallManager.
- When the failed Cisco Unified CallManager comes back up, its Cisco CallManager Attendant Console Server resumes servicing its route points and attendant consoles. The attendant resumes service with the recovered Cisco Unified CallManager after the attendant closes and reopens the console.

**Note**

Automated recovery exists. If a Cisco CallManager Attendant Console Server service fails, another Cisco CallManager Attendant Console Server service takes over.

To ensure redundancy for the Cisco Unified CallManager Attendant Console application, perform one of the following tasks:

- In default configurations where CTIManager and Cisco CallManager Attendant Console Server are running on all nodes in the Cisco Unified CallManager cluster, enter the IP address of one server that is running Cisco CallManager Attendant Console Server in the Attendant Settings dialog box on the attendant PC.
- If Cisco CallManager Attendant Console Server and CTIManager are not running on all nodes in the cluster, enter a comma separated list of the IP addresses of servers in the cluster that have an active CTIManager in the Call Processing Server Host Names or IP Addresses field on the Advanced Tab of the Attendant Settings dialog box on the attendant PC.

**Note**

For more information on accessing the Attendant Settings dialog box, see the [“Configuring Cisco Unified CallManager Attendant Console Settings”](#) section on page 14-37.

Firewall Support for Attendant Console

Cisco Unified CallManager 5.1(1) offers firewall support through Remote Method Indication (RMI).

Attendant console clients and attendant console servers communicate through Java RMI, which is also how attendant console servers communicate with each other. They only differ in that no firewall exists between servers.

The attendant console server uses a custom RMI socket to bind to specific TCP ports for sending the RMI response to the client. You can configure this by using Service Parameter RMI Bind Port.

RMI uses a TCP Callback Port to send callback messages to the attendant console client. You can configure the attendant console Client Callback Port can be configured using Settings Dialog.

**Note**

You must make sure that the RMI ports are open in the firewall.

System Requirements for Cisco Unified CallManager Attendant Console

See the following sections for PC requirements and Cisco Unified IP Phone requirements for using the attendant console:

- [Attendant PC Requirements, page 14-12](#)
- [Cisco Unified IP Phone and Voice-Messaging Requirements for Use with the Attendant Console, page 14-13](#)

Attendant PC Requirements

The following list provides PC requirements for the attendant console:

- Operating system—Windows 2000 and Windows XP
- Network connectivity to the Cisco Unified CallManager

Cisco Unified IP Phone and Voice-Messaging Requirements for Use with the Attendant Console

The attendant console works in conjunction with a Cisco Unified IP Phone. Configure the attendant console to connect the Cisco Unified IP Phone to its registered Cisco Unified CallManager server. To configure the attendant console, make sure that the IP Address or Host Name field in the Attendant Console Settings dialog box specifies the address of the Cisco Unified CallManager server to which the Cisco Unified IP Phone is normally registered.

Cisco Unified IP Phones that are used with the attendant console must meet the following guidelines:

- Use the attendant console with any SCCP Cisco Unified IP Phone Models 7905G, 7911G, 7912G, 7912G-A, 7940G, 7941G, 7941G-GE, 7960G, 7961G, 7961G-GE, 7970G and 7970G-GE. You cannot use SIP phones as attendant phones, but attendants can receive and handle calls from SIP phones.
- Make sure that the Cisco Unified IP Phone is added as a device in Cisco Unified CallManager before it is used with the attendant console.
- Make sure that you check the Allow Control of Device from CTI checkbox on the Phone Configuration window (**Device > Phone**) for each attendant phone. The system enables this field by default. If this checkbox is not checked for the attendant phone, call control does not come up for the attendant console.
- Make sure that you associate the attendant devices with the attendant console device authorization user that you configured in the Application User Configuration window in Cisco Unified CallManager Administration.
- Make sure that you configure voice messaging for each directory number the attendant can access. If you do not, the attendant cannot forward calls to voice-messaging system.
- Do not use a shared-line appearance for pilot points. Make sure that directory numbers for pilot points do not appear on any other device in the system. Attendant phones can share lines with other attendants or non-attendants.
- Disable call forwarding for lines and directory numbers on Cisco Unified IP Phones that are used as attendant consoles.
- If an attendant console user will be logging in to the attendant console at more than one phone, ensure that each phone is set up according to these guidelines and that each phone is registered with its own attendant console.
- Based on the line settings on Directory Number Configuration window, Cisco Unified CallManager Attendant Console can support multiple calls on a line. When no more outgoing calls can be made on a line, Cisco Unified CallManager Attendant Console displays a warning message when the attendant attempts to make a call.

Interactions and Restrictions

The following sections describe the interactions and restrictions for Cisco Unified CallManager Attendant Console:

- [Interactions, page 14-14](#)
- [Restrictions, page 14-15](#)

Interactions

The following sections describe how Cisco Unified CallManager Attendant Console interacts with Cisco Unified CallManager applications:

- [Cisco Extension Mobility, page 14-14](#)
- [Music On Hold, page 14-14](#)
- [Call Park, page 14-14](#)
- [CTI, page 14-14](#)

Cisco Extension Mobility

If a user logs in to or logs off the Cisco Unified IP Phone by using Cisco Extension Mobility while logged in to Cisco Unified CallManager Attendant Console, the Cisco Unified IP Phone resets, and the call-control status of the attendant console goes down. Cisco Unified CallManager Attendant Console displays a message that indicates that the attendant needs to log out and log back in if the directory numbers of the phone have changed. The user must log out of the Cisco Unified CallManager Attendant Console. When logging back into the Cisco Unified CallManager Attendant Console, the attendant must specify the current directory number of the phone in the Directory Number of Your Phone field of the Settings dialog box.

For more information on entering a directory number in the Cisco Unified CallManager Attendant Console, see [“Configuring Cisco Unified CallManager Attendant Console Settings” section on page 14-37](#).

Music On Hold

If you have chosen an audio source from the Network Hold Audio Source and the User Hold MOH Audio Source drop-down list boxes in the Device Pool window or on the Pilot Point window, queued callers receive music on hold while in the queue. The selections you make on the Pilot Point Configuration window override those you make on the Device Pool window.

Call Park

You must associate the Attendant Console application user to the Standard CTI Allow Call Park Monitoring group (found on the Cisco Unified CallManager Administration User Group Configuration window). If you do not associate the application user to this group, pilot points do not register, and the call control does not go on the console.

CTI

You must associate the Attendant Console application user to the Standard CTI Enabled users group and the Standard CTI Allow Call Park Monitoring group (found on the Cisco Unified CallManager Administration User Group Configuration window). If you do not associate the application user to these groups, pilot points do not register, and the call control does not go up on the console.

Restrictions

The following restrictions apply to Cisco Unified CallManager Attendant Console:

- You cannot use SIP phones as attendant phones, but attendants can receive and handle calls from SIP phones.
- The attendant console does not show the correct call forward all (CFA) status of certain SIP phones, including Cisco SIP IP Phone models 7940 and 7960.
- Cisco CallManager Attendant Console Server does not route calls to an instance of a shared line on attendant phone if any other instances of the shared line are in use.
- If you use the attendant console in a cluster environment, make sure that all Cisco Unified CallManagers within a cluster have the Cisco CallManager Attendant Console Server service activated and running. You must manually activate the service through Cisco Unified CallManager Serviceability. Attendant console redundancy requires this setup to work properly; however, not all Cisco CallManager Attendant Console Servers are required to have a route point.
- Cisco Unified CallManager Attendant Console does not support a dual monitor setup on the attendant PC.
- Cisco Unified CallManager Attendant Console does not support Barge and cBarge; however, the client interface does display any activity that is related to these features.
- Do not use a shared-line appearance for pilot points and hunt group members. Make sure that directory numbers for pilot points and hunt group members do not appear on any other device in the system.
- Disable call forwarding for lines and directory numbers on Cisco Unified IP Phones that are used as attendant consoles.
- Cisco Unified CallManager Attendant Console recognizes partitions, but has the following problems working with them:
 - If a directory number exists in more than one partition, the attendant console displays the line state of the DN that changed last. This means that line state that appears for a particular individual in the directory may not be correct.
 - If a directory number in the hunt group also exists in another partition, Cisco Unified CallManager Attendant Console may not route calls appropriately. Consider a scenario in which directory number 2000 exists in Partition1 and Partition2, and directory number 2000 (Partition1) exists in a hunt group. If directory number 2000 (Partition2) receives a call, Cisco Unified CallManager Attendant Console considers the line state of directory number 2000 (Partition1) to be busy and does not route calls to that directory number.
- A user cannot activate call back for a Cisco Unified CallManager Attendant Console pilot point number over a QSIG-enabled intercluster trunk or QSIG-enabled trunk. If the user attempts to activate call back to a Cisco Unified CallManager Attendant Console pilot point number over a QSIG-enabled intercluster trunk or QSIG-enabled trunk, the message “Callback Cannot be activated on xxxx” displays on the user phone. The user can activate call back for a Cisco Unified CallManager Attendant Console pilot point if that pilot point exists in the same Cisco Unified CallManager cluster as the user DN.
- Cisco Unified CallManager Attendant Console does not work with the group call pickup feature. The attendant console user interface cannot appropriately handle calls coming from or made to phones belonging to a call pickup group due to JTAPI and CTI limitations.
- Make sure that you do not add attendant console pilot points or hunt group members or any directory numbers on an attendant phone to line groups in Cisco Unified CallManager Administration.

- When two attendant console clients share a line, the attendant console does not always accurately display the attendant who parked a call in the Call Park window. When attendant #1 parks a call, the correct information regarding who parked the call on the PC of attendant #2; however, Cisco Unified CallManager Attendant Console does not display correct information regarding who parked the call on the PC of attendant #1. On the PC of attendant #1, Cisco Unified CallManager Attendant Console displays that attendant #1 parked the call rather than attendant #2.

Installing and Activating Cisco Unified CallManager Attendant Console

1. Use Cisco Unified CallManager Serviceability to activate and start the Cisco CallManager Attendant Console Server service on all servers that are running the Cisco CallManager service and to activate the CTIManager service on one server in the cluster. Refer to the *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)*.
2. Configure Cisco Unified CallManager Attendant Console in Cisco Unified CallManager Administration. See the [“Configuring Cisco Unified CallManager Attendant Console”](#) section on page 14-16.
3. Install and configure the Cisco Unified CallManager Attendant Console plug-in on each attendant PC. For more information, see the [“Installing the Cisco Unified CallManager Attendant Console Plug-in on an Attendant PC”](#) section on page 14-35, the [“Starting Cisco Unified CallManager Attendant Console After Installing Windows XP SP2”](#) section on page 14-36, and the [“Configuring Cisco Unified CallManager Attendant Console Settings”](#) section on page 14-37. After the attendant console is configured, it operates with the specified settings until the administrator changes them.
4. If the attendants require Cisco Attendant Console user windows to display in a language other than English, make sure that you install the Cisco Unified CallManager Locale Installer on every server in the cluster. For more information, refer to the *Cisco Unified Communications Operating System Administration Guide, Release 5.0(4)*.

Configuring Cisco Unified CallManager Attendant Console

For successful configuration of Cisco Unified CallManager Attendant Console, perform the steps in the configuration checklist. The following sections provide configuration information:

- [Configuration Checklist for Cisco Unified CallManager Attendant Console, page 14-17](#)
- [Configuring Cisco Unified CallManager Attendant Console Users, page 14-18](#)
- [Enabling Device Security for Cisco Unified CallManager Attendant Console, page 14-21](#)
- [Enabling the Super Provider Feature for Cisco Unified CallManager Attendant Console, page 14-22](#)
- [Associating Devices with the Attendant Console Authorization User, page 14-28](#)
- [Configuring Hunt Groups, page 14-29](#)
- [Cisco CallManager Attendant Console Server Service Configuration, page 14-32](#)
- [Creating and Uploading the CorporateDirectory.txt File, page 14-33](#)
- [Deleting the CorporateDirectory.txt File, page 14-34](#)
- [Installing the Cisco Unified CallManager Attendant Console Plug-in on an Attendant PC, page 14-35](#)

- [Starting Cisco Unified CallManager Attendant Console After Installing Windows XP SP2, page 14-36](#)
- [Configuring Cisco Unified CallManager Attendant Console Settings, page 14-37](#)
- [Attendant Console Configuration Settings, page 14-37](#)
- [Configuring Held Icon Timers, page 14-39](#)
- [Dependency Records, page 14-40](#)

Configuration Checklist for Cisco Unified CallManager Attendant Console

Perform the steps in [Table 14-1](#) to set up the attendant console.

Table 14-1 Attendant Console Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Add attendant console users.	Configuring Cisco Unified CallManager Attendant Console Users, page 14-18
Step 2	Configure directory numbers for the pilot points.	Configuring a Directory Number, Cisco Unified CallManager Administration Guide, Release 5.0(4)
Step 3	Set up pilot points and hunt groups.	Understanding Pilot Points and Hunt Groups, page 14-2 Enabling the Super Provider Feature for Cisco Unified CallManager Attendant Console, page 14-22 Configuring Hunt Groups, page 14-29
Step 4	Create the attendant console application user and the attendant console device authorization user.	Enabling Device Security for Cisco Unified CallManager Attendant Console, page 14-21
Step 5	Associate attendant phones with the attendant console device user.	Associating Devices with the Attendant Console Authorization User, page 14-28
Step 6	Add the Attendant Console application user to the Standard CTI Enabled group, the Standard CTI Allow Call Park Monitoring group, and the Standard CTI Allow Control of All Devices user group.	Adding Users to a User Group, Cisco Unified CallManager Administration Guide, Release 5.0(4)
Step 7	Verify that the Cisco CallManager Attendant Console Server service activates and runs on all servers that are running the Cisco CallManager service. Verify that the CTIManager service activates and runs on one server in the cluster.	Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4) Understanding the Cisco CallManager Attendant Console Server Service, page 14-10
Step 8	Make sure that each attendant Cisco Unified IP Phone is set up correctly for use with the attendant console.	Cisco Unified IP Phone and Voice-Messaging Requirements for Use with the Attendant Console, page 14-13
Step 9	Make sure that the attendant console PC is set up correctly for use with the attendant console.	Attendant PC Requirements, page 14-12

Table 14-1 Attendant Console Configuration Checklist (continued)

Configuration Steps	Related Procedures and Topics
Step 10 Create dial rules to transform directory numbers into a dialable pattern. Each rule specifies which numbers to transform based on the beginning digits and length of the number. For example, you can create a dial rule that automatically removes the area code and prefix digits from a 10-digit telephone number beginning with 408525 and adds 89 to the beginning of the telephone number to provide access to an outside line. In this case, the number 4085256666 becomes 8956666.	Configuring Dial Rules, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> Dial Rules Overview, <i>Cisco Unified CallManager System Guide, Release 5.0(4)</i>
Step 11 Directory lookup rules transform caller identification numbers into numbers that can be looked up in the directory. 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.	Configuring Directory Lookup Dial Rules, <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> Directory Lookup Dial Rules, <i>Cisco Unified CallManager System Guide, Release 5.0(4)</i>
Step 12 If your centralized user list is located on a directory server that is separate from the Cisco Unified CallManager server, create and upload the CorporateDirectory.txt file.	Creating and Uploading the CorporateDirectory.txt File, page 14-33
Step 13 Install and configure the attendant console on each attendant console user PC. Note After a Cisco Unified CallManager upgrade, you must reinstall the Cisco Unified CallManager Attendant Console Plug-in on the attendant PCs.	Installing the Cisco Unified CallManager Attendant Console Plug-in on an Attendant PC, page 14-35 Starting Cisco Unified CallManager Attendant Console After Installing Windows XP SP2, page 14-36 Configuring Cisco Unified CallManager Attendant Console Settings, page 14-37

Configuring Cisco Unified CallManager Attendant Console Users

This section covers the following procedures:

- [Finding an Attendant Console User, page 14-19](#)
- [Configuring an Attendant Console User, page 14-20](#)
- [Deleting an Attendant Console User, page 14-21](#)
- [Enabling Device Security for Cisco Unified CallManager Attendant Console, page 14-21](#)
- [Enabling the Super Provider Feature for Cisco Unified CallManager Attendant Console, page 14-22](#)
- “Configuring Pilot Points” section on page 14-23

Additional Information

See the “Related Topics” section on page 14-40.

Finding an Attendant Console User

Use the following procedure to find an attendant console user:

**Note**

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

Procedure

Step 1 Choose **Application > Cisco Unified CM Attendant Console > Cisco Unified CM Attendant Console User**.

The Find and List window displays.

Step 2 From the 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 attendant console users that are registered in the database, click **Find** without entering any search text.

A list of attendant console users displays by Name.

**Tip**

To search for directory numbers within the search results, click the **Extend Query** check box, enter your search criteria as described in this procedure, and click **Find**.

Additional Information

See the [“Related Topics” section on page 14-40](#).

Configuring an Attendant Console User

This section describes how to configure an attendant console user. You must add users through the Cisco Unified CallManager Attendant Console User Configuration window in Cisco Unified CallManager Administration before the users can log in to an attendant console.



Note

Be aware that attendant console user IDs and passwords are *not* the same as directory users and passwords that are entered in the End User Configuration window in Cisco Unified CallManager Administration.

Procedure

-
- Step 1** Choose **Application > Cisco Unified CM Attendant Console > Cisco Unified CM Attendant Console User**.
- Step 2** Perform one of the following tasks:
- To add a new attendant console user, click the **Add New** button.
 - To update an existing attendant console user, locate the appropriate user as described in [“Finding an Attendant Console User”](#) section on page 14-19, and click the name of the user you want to update.
- The Cisco Unified CallManager Attendant Console User Configuration window displays.
- Step 3** Enter the appropriate configuration settings as described in [Table 14-2](#).
- Step 4** Click **Save**.
-

Additional Information

See the [“Related Topics”](#) section on page 14-40.

Cisco Unified CallManager Attendant Console User Configuration Settings

[Table 14-2](#) describes Cisco Unified CallManager Attendant Console user configuration settings.

Table 14-2 Attendant Console User Configuration Settings

Field	Description
User ID	Enter the login name for the attendant console user. Enter up to 50 alphanumeric characters.
Password	Enter a password of up to 50 alphanumeric characters.
Confirm	Enter the same password again.

Additional Information

See the [“Related Topics”](#) section on page 14-40.

Deleting an Attendant Console User

This section describes how to view, update, or delete a Cisco attendant console user.

Before You Begin

To find out which hunt groups are using the attendant console user, click the **Dependency Records** link from the Cisco Unified CallManager Attendant Console 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, refer to the “Accessing Dependency Records” section in the *Cisco Unified CallManager Administration Guide*. If you try to delete an attendant console user that is in use, Cisco Unified CallManager displays a message. To delete an attendant console user that is currently in use, you must perform either or both of the following tasks:

- Assign a different attendant console user to any hunt groups that are using the attendant console user that you want to delete. See the “[Deleting Hunt Group Members](#)” section on page 14-32.
- Delete the hunt groups that are using the attendant console user. See the “[Deleting Hunt Group Members](#)” section on page 14-32.

Procedure

-
- Step 1** Locate the user you want to delete by using the procedure in the “[Finding an Attendant Console User](#)” section on page 14-19.
- Step 2** Click the name of the user that you want to delete.
- Step 3** To remove the user, click **Delete**.



Tip

From the Find and List window, you can delete multiple users by checking the check boxes next to the appropriate users and clicking **Delete Selected**. You can delete all users in the window by clicking **Select All**, then clicking **Delete Selected**.

Additional Information

See the “[Related Topics](#)” section on page 14-40.

Enabling Device Security for Cisco Unified CallManager Attendant Console

If you want to enable device security for the Cisco Unified CallManager Attendant Console, you must configure an attendant console application user and attendant console device authentication application user as well as associate the attendant phones with the user attendant console device authentication application user. If you do not configure these users, the attendant console cannot interact with CTIManager, and the attendant cannot receive calls.

Perform the following procedure to configure the Attendant Console application user.

Procedure

-
- Step 1** Choose **User Management > Application User**.
- The Find and List Application Users window displays.

Step 2 Click **Add New**.

The Application User Configuration window displays.

Step 3 To create the attendant console application user, enter a user ID such as **ac** in the User ID field.



Note

Make sure that the user ID that you use for the attendant console application user is the same as the value in the JTAPI username field in the Service Parameters Configuration window for the Cisco CallManager Attendant Console Server service. For information on accessing the Cisco Unified CallManager Attendant Console service parameters, see the [“Cisco CallManager Attendant Console Server Service Configuration”](#) section on page 14-32.

Step 4 In the Password field, enter a password such as **12345**.

Step 5 In the Confirm Password field, re-enter the password.

Step 6 Click **Save**.

Step 7 Click **Add New**.

Step 8 To create the device authentication user, enter a user ID such as **ac2** in the User ID field.



Note

Make sure that the user ID that you use for the device authentication user is the same as the value in the ACDeviceAuthentication field in the Service Parameters Configuration window for the Cisco CallManager Attendant Console Server service. For information on accessing the Cisco Unified CallManager Attendant Console service parameters, see the [“Cisco CallManager Attendant Console Server Service Configuration”](#) section on page 14-32.

Step 9 In the Password field, enter a password such as **12345**.

Step 10 In the Confirm Password field, re-enter password.

Step 11 Click **Save**.

.Additional Information

See the [“Related Topics”](#) section on page 14-40.

Enabling the Super Provider Feature for Cisco Unified CallManager Attendant Console

You can enable Cisco Unified CallManager Attendant Console devices without associating each of the them with the Cisco Unified CallManager Attendant Console application user by enabling the super provider feature. To do this, add the Cisco Unified CallManager Attendant Console application user to the Standard CTI Allow Control of All Devices user group. After you enable the super provider feature, you do not have to associate pilot points and attendant phones to the Cisco Unified CallManager Attendant Console user.

During an upgrade from Cisco Unified CallManager Release 4.X, the system automatically converts the attendant console application user to a superprovider user and disassociates the devices previously associated to the application user.

Configuring Pilot Points

Before the Cisco CallManager Attendant Console Server service can route calls, you must configure pilot points and hunt groups through Cisco Unified CallManager Administration.

This section contains the following topics:

- [Finding a Pilot Point, page 14-23](#)
- [Configuring a Pilot Point, page 14-24](#)
- [Deleting a Pilot Point, page 14-27](#)
- [Resetting a Pilot Point, page 14-28](#)
- [Pilot Point Configuration Settings, page 14-25](#)

Additional Information

See the “[Related Topics](#)” section on [page 14-40](#).

Finding a Pilot Point

This section describes how to find a pilot point.



Note

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

Procedure

-
- Step 1** Choose **Application > Cisco Unified CM Attendant Console > Pilot Point**.
- The Find and List window displays.
- Step 2** From the drop-down list box, choose one of the following criteria:
- Pilot Point
 - Calling Search Space
 - Device Pool
 - Pilot Number
 - Partition
- 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 pilot points that are registered in the database, click **Find** without entering any search text.

A list of pilot points displays.



Tip

To search for a pilot point within the search results, click the **Extend Query** check box, enter your search criteria as described in this procedure, and click **Find**.

- Step 4** To view a specific pilot point, click the pilot point name.
- Step 5** To delete or reset multiple pilot points from the Find and List Pilot Points window, check the check boxes next to the appropriate pilot points. You can choose all the phones in the window by checking the **Select All** button. Then, do one of the following:
- To delete the pilot points, click **Delete Selected**. When the delete confirmation dialog box displays, click **OK**.
 - To reset the pilot points, click **Reset Selected**. When the Device Reset window displays, click **Restart**.

Additional Information

See the [“Related Topics”](#) section on page 14-40.

Configuring a Pilot Point

This section describes how to configure a pilot point and how to associate the directory number with that pilot point.

Before You Begin

Configure directory numbers to associate with the pilot points.

For more information on configuring directory numbers, see the “Configuring a Directory Number” section in the *Cisco Unified CallManager Administration Guide*.

Procedure

- Step 1** Choose **Application > Cisco Unified CM Attendant Console > Pilot Point**.
The Find and List Pilot Points window displays.
- Step 2** Perform one of the followings tasks:
- To copy an pilot point, locate the appropriate phone as described in [“Finding a Pilot Point”](#) section on page 14-23, and click the **Copy** button.
 - To add a new pilot point, click the **Add New** button.
 - To update an existing phone, locate the appropriate phone as described in [“Finding a Pilot Point”](#) section on page 14-23.
- Step 3** Enter the appropriate settings as described in [Table 14-3](#).
- Step 4** Click **Save**.
- Step 5** To associate a directory number for the pilot point, click the **Line [1]** link.
The Directory Number Configuration window displays.
- Step 6** Enter the directory number that you want to use for the pilot point from the Directory Number field and click **Save**.

**Note**

After the pilot point is created, you must configure a hunt group to specify which attendants receive the calls that come in to the pilot point. For more information, see the [“Configuring Hunt Group Members”](#) section on page 14-29.

Additional Information

See the [“Related Topics”](#) section on page 14-40.

Pilot Point Configuration Settings

Table 14-3 describes pilot point configuration settings.

Table 14-3 Pilot Point Configuration Settings

Field	Description
Pilot Name	Enter up to 15 alphanumeric characters, including spaces, to specify a descriptive name for the pilot point.
Description	Enter a description of the pilot point. This description can contain up to 50 characters.
Device Pool	The device pool comprises a group of Cisco Unified CallManagers in prioritized order. The first Cisco Unified CallManager in the list represents the primary Cisco Unified CallManager for the pilot point.
Calling Search Space	To designate the partitions that the pilot point searches when it attempts to route a call, choose a calling search space from the drop-down list. 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 Find button displays next to the drop-down list box. Click the Find 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 in the Max List Box Items field.

Table 14-3 Pilot Point Configuration Settings (continued)

Field	Description
Route Calls To	Choose the method by which Cisco Unified CallManager Attendant Console routes calls to attendants. The available methods include • First Available Hunt Group Member—Routes incoming calls to the first available member of a hunt group. • Longest Idle Hunt Group Member—Routes incoming calls to the route group member that has been idle for the longest time. If the voice-messaging number is the longest idle member of the group, Cisco Unified CallManager Attendant Console routes the call to voice-messaging system without first checking the other members of the group. • Circular Hunting—Cisco Unified CallManager Attendant Console maintains a record of the last hunt group member to receive a call. When a new call arrives, Cisco Unified CallManager Attendant Console routes the call to the next hunt group member in the hunt group. • Broadcast Hunting—When a call arrives at the pilot point, Cisco Unified CallManager Attendant Console answers the call, places the call on hold, adds the call to the queue, and displays the call in the Broadcast Calls window on attendant PCs. While on hold, the caller receives music on hold, if it is configured. Any attendant can answer the call from the Broadcast Calls window.
Location	This field specifies a selection of locations that are defined by using System > Location. When a location is defined, a location name, audio and video bandwidths get specified.
Media Resource Group	Choose the appropriate Media Resource Group List. A Media Resource Group List specifies a prioritized list of media resource groups. Cisco Unified CallManager Attendant Console 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 the media resource group list. Note For more information on media resource group lists, see “Configuring a Media Resource Group List” in the <i>Cisco Unified CallManager Administration Guide</i>.
Network Hold MOH Audio Source	Choose the audio source that Cisco Unified CallManager Attendant Console uses for network hold, including transfer hold, conference hold, and call park hold.
User Hold MOH Audio Source	Choose the audio source that Cisco Unified CallManager Attendant Console uses when the attendant places a caller on hold.
Queuing Enable	If you want Cisco Unified CallManager Attendant Console to queue calls when all attendants in a hunt group are busy, check the Queuing Enable check box. To complete the call-queuing configuration, enter values in the Queue Size and Queue Hold Time (in Seconds) fields.

Table 14-3 Pilot Point Configuration Settings (continued)

Field	Description
Queue Size	This field specifies the number of calls that are allowed in the queue. If the queue is full, Cisco Unified CallManager Attendant Console routes calls to the “always route” member that is specified on the Hunt Group Configuration window. If you do not specify an always route member, Cisco Unified CallManager Attendant Console drops the call when the queue size limit is reached. The range is 0 to 255. The default specifies 32.
Queue Hold Time (in Seconds)	This field specifies the maximum time (in seconds) that Cisco Unified CallManager Attendant Console keeps a call in the queue. If a call remains on hold for the number of seconds that are entered in this field and you configured an “always route” hunt group member on the Hunt Group Configuration window, Cisco Unified CallManager Attendant Console sends the call to the always route member that is specified on the Hunt Group Configuration window. If you do not configure an always route member, the call remains in the queue until an attendant becomes available. Enter 0 in this field to keep calls in the queue until an attendant becomes available. The range is 0 to 3600 seconds. The default specifies 0.

Additional Information

See the [“Related Topics” section on page 14-40](#).

Deleting a Pilot Point

This section describes how to delete a pilot point.

Before You Begin

To find out which virtual directory numbers are using the pilot point, click the **Dependency Records** link from the Pilot Point 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 in the *Cisco Unified CallManager Administration Guide*. If you try to delete a pilot point that is in use, Cisco Unified CallManager displays a message. To delete a pilot point that is currently in use, you must delete the virtual directory numbers that are using the pilot point.

**Note**

You do not have to restart the Cisco CallManager Attendant Console Server service or the Cisco CallManager service after you delete a pilot point for the deletion to take effect.

Procedure

- Step 1** Locate the pilot point by using the procedure in the [“Finding a Pilot Point” section on page 14-23](#).
- Step 2** Click the name of the pilot point that you want to delete. The Pilot Point Configuration window displays with information for the chosen pilot point.

Step 3 To remove the pilot point, click the **Delete** button.

Approximately 10 minutes after you delete a pilot point, Cisco Unified CallManager Attendant Console stops directing calls to any hunt group members that are associated with that pilot point.



Tip

From the Find and List window, you can delete multiple pilot points by checking the check boxes next to the appropriate pilot points and clicking **Delete Selected**. You can delete all pilot points in the window by clicking **Select All**, then clicking **Delete Selected**.

Additional Information

See the “[Related Topics](#)” section on page 14-40.

Resetting a Pilot Point

You must reset the pilot point after you update pilot point configuration settings. When you reset the pilot point, the Cisco CallManager service continues to run, and call processing continues to occur. Perform the following procedure to reset the pilot point:

Procedure

-
- Step 1** Locate the pilot point that you want to reset by using the procedure in the “[Finding a Pilot Point](#)” section on page 14-23.
- Step 2** Click the name of the pilot point that you want to reset.
- Step 3** Click **Reset**.
- The Reset window displays.
- Step 4** Click one of the following buttons:
- **Restart**—Restarts the selected device for the pilot point without shutting the device down (reregisters the phones with Cisco Unified CallManager).
 - **Reset**—Shuts down the selected device for the pilot point and brings it back up (performs a complete shutdown and reinitialization of the phone).
 - **Close**—Returns you to the previous window without restarting or resetting the selected device.
-

Additional Information

See the “[Related Topics](#)” section on page 14-40.

Associating Devices with the Attendant Console Authorization User

Before the attendant uses the attendant console, you must associate the attendant console phones to the attendant console device authorization user that you created on the Application User Configuration window. Perform the following procedure:

Procedure

- Choose **User Management > Application User**, and perform a search for the device authorization user that you set up in the [“Enabling Device Security for Cisco Unified CallManager Attendant Console” section on page 14-21](#). For more information on performing a user search, see the “Finding an End User” in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

Step 1

The device authorization user information appears in the Application User Configuration window.

Step 2

Choose the attendant phones from the Available Devices list in the Device Associations box that you want to associate with the device authorization user and click the down arrow to move the devices to the Controlled Devices box. To choose multiple devices, Ctrl+click the devices. To locate specific devices, click the **Find More Phones** button, locate the devices as described in [“Finding a Pilot Point” section on page 14-23](#), check the check boxes next to the pilot points that you want to associate to the ac user, and click **Add Selected**.

Step 3

Click **Save**.

Additional Information

See the [“Related Topics” section on page 14-40](#).

Configuring Hunt Groups

After you configure the pilot point, you must configure the hunt group. A hunt group comprises an ordered list of destinations (either directory numbers or attendant console user/line numbers) to which Cisco Unified CallManager Attendant Console directs incoming calls.

This section covers the following procedures:

- [Configuring Hunt Group Members, page 14-29](#)
- [Hunt Group Configuration Settings, page 14-30](#)
- [Deleting Hunt Group Members, page 14-32](#)

Additional Information

See the [“Related Topics” section on page 14-40](#).

Configuring Hunt Group Members

This section describes how to add and update hunt group members.

Before You Begin

Configure the pilot point for which you want to add hunt group members, including associating the directory number to the pilot point, as described in the [“Enabling the Super Provider Feature for Cisco Unified CallManager Attendant Console” section on page 14-22](#).

Procedure

Step 1

Find the pilot point for which you want to configure hunt group members as described in the [“Finding a Pilot Point” section on page 14-23](#).

Step 2 Do one of the following:

- To add a hunt group member, click the **Add Member** button in the Hunt Group Member Information area.
- To edit an existing hunt group member, choose the hunt group member and click the **Edit Member** button in the Hunt Group Member Information area.

The Hunt Group Configuration window displays.

Step 3 Enter the appropriate configuration settings for the new hunt group member as described in [Table 14-4](#).

Step 4 Click **Save**.

Step 5 Do one of the following

- To add a new hunt group member to the pilot point, click **Add New** and repeat [Step 3](#) and [Step 4](#).
- To create another hunt group member by copying the hunt group member that is displayed in the Hunt Group Configuration window, click **Copy** and repeat [Step 3](#) and [Step 4](#).
- To delete the hunt group member that is displayed, click **Delete**.
- To close the Hunt Group Configuration window and return to the Pilot Point Configuration window, click **Close**.

Step 6 To reorder the hunt group list, choose the member that you want to reorder from the list. Click the up and down arrows to move that member to a new position in the list.

If you are configuring a linked hunt group, make sure that the final member of each hunt group is the pilot point for the next hunt group.



Caution

Cisco strongly recommends that you do not link the last hunt group back to the first hunt group.

For an example of a linked hunt group, see the “[Understanding Linked Hunt Groups](#)” section on [page 14-5](#).

Additional Information

See the “[Related Topics](#)” section on [page 14-40](#).

Hunt Group Configuration Settings

[Table 14-4](#) describes hunt group configuration settings.

Table 14-4 *Hunt Group Configuration Settings*

Field	Description
Pilot Point	Displays the name of the pilot point for which you are configuring hunt group members.
Pilot Number (DirN)	Displays the directory number that is associated with the pilot point for which you are configuring hunt group members.

Table 14-4 **Hunt Group Configuration Settings (continued)**

Field	Description
Hunt Group Member	This read-only field reflects the information that you choose from the Hunt Group Configuration window whether you enter the device directory number or the attendant console user name and line number; for example: • Call directory number 35201 (directory number example) • Direct Call to Mary Brown, Line 1 (user and line number example)
Member Option	Choose Device Member or User Member. If you choose the Device Member radio button, complete the fields in the Device Member Information section. If you choose the User Member, complete the User Name and Line Number fields in the User Member Information section. Note If you specify an attendant console user and line number, Cisco Unified CallManager Attendant Console first checks whether the attendant console user is logged in to an attendant console and online before attempting to route the call. When you specify a user and line number, the user can log in to and receive calls on any Cisco Unified IP Phone in the cluster that the attendant console controls.
Directory Number	Choose the directory number that you want to include in the hunt group. This field is only available if you chose the Device Member radio button from the Member Option field.  Caution If you are configuring a linked hunt group, Cisco strongly recommends that you do not include any pilot point numbers in the hunt group except as the final member. Including other pilot point numbers in the hunt group may cause a continuous route loop.
Always Route Member	If you want Cisco Unified CallManager Attendant Console to always route calls to this hunt group member, whether it is busy or not, check this check box. If this check box is checked, Cisco Unified CallManager Attendant Console does not check whether the line is available before routing the call. To manage overflow conditions, check this check box for voice-messaging or auto-attendant numbers that handle multiple, simultaneous calls. For linked hunt groups, only check the Always Route Member check box when you are configuring the final member of each hunt group.
User Name	From the drop-down list, choose the attendant console user that will serve as a hunt group member. This field is only available if you chose the User Member radio button from the Member Option field. Only attendant console users that are added in the Cisco Unified CallManager Attendant Console User Configuration window appear in this list.

Table 14-4 *Hunt Group Configuration Settings (continued)*

Field	Description
Line Number	From the drop-down list, choose the appropriate line numbers for the hunt group. This field is only available if you chose the User Member radio button from the Member Option field. Note You can add the same user to the same line only once within a single hunt group. For example, you cannot add Mary Brown, Line 1, more than once in the hunt group.

Additional Information

See the [“Related Topics”](#) section on page 14-40.

Deleting Hunt Group Members

This section describes how to delete hunt group members.

Procedure

-
- Step 1** Choose **Application > Cisco Unified CM Attendant Console > Pilot Point**.
The Pilot Point Configuration window displays.
- Step 2** In the Hunt Group member Information group box, click the name of the member that you want to delete and click **Delete Member**.
The delete confirmation dialog box displays.
- Step 3** To remove the hunt group member, click **OK**. To cancel the deletion, click **Cancel**.
-

Additional Information

See the [“Related Topics”](#) section on page 14-40.

Cisco CallManager Attendant Console Server Service Configuration

From the Service Parameters Configuration window, you can set service parameters for the Cisco CallManager Attendant Console Server service. You obtain information about the parameters by clicking the ? button help icon in the upper, right corner of the window.

**Caution**

Do not change any service parameters without permission of a Cisco Technical Assistance Center engineer. Doing so may cause system failure.

Perform the following steps to update Cisco CallManager Attendant Console Server service parameters.

Procedure

Step 1 Choose **System > Service Parameters**.

The Service Parameter Configuration window displays.

Step 2 From the Server drop-down list box, choose a server.

Step 3 From the Service drop-down list box, choose the Cisco CallManager Attendant Console Server service.



Note You must activate the Cisco CallManager Attendant Console Server service on a server before the server displays in the Cisco CallManager Attendant Console Servers list. For more information on activating a service, refer to the *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)*.

The window refreshes and displays all configured service parameters for the Cisco CallManager Attendant Console Server service.

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 ? button in the upper, right corner of the window. To view the list with a particular parameter at the top, click that parameter in the Cisco CallManager Attendant Console Server Configuration window.

Step 5 Click **Update**.

The window refreshes, and Cisco Unified CallManager updates the service parameter with your changes.

Additional Information

See the [“Related Topics” section on page 14-40](#).

Creating and Uploading the CorporateDirectory.txt File

You can create and upload a CorporateDirectory.txt file if your centralized user list is located on a directory server that is separate from the Cisco Unified CallManager server. To do this, perform the following procedure:

Procedure

Step 1 On your PC, create a corporate directory file named CorporateDirectory.txt that contains comma separated entries for each user in the format Last Name, First Name, Telephone Number, Department. Create one line for each user in the directory. You can include empty values for fields. The system ignores blank lines and lines starting with pound (#) or semi-colons (;). The following represents a sample directory file:

```
Doe, Jane, 67890, Engineering
Doe, John, 12345, Sales
Doe, Rodney, 12346, Marketing
Doe, Brian, 12347, Customer Support
```

```
Smith,,,Marketing
Clark,,,

```



Note The CorporateDirectory.txt filename is case-sensitive.

- Step 2** In Cisco Unified CallManager Administration, choose **Application > Cisco Unified CM Attendant Console > Cisco Unified CM Attendant Console User File Upload**.

The Attendant Console User File Upload window displays.



Tip To view a sample directory file, choose the **View Sample CorporateDirectory.txt File** link. Then, click the browser Back button to return to the Attendant Console User File Upload window. If you have previously uploaded a corporate directory file, you can view that file by clicking the **View Current CorporateDirectory.txt File** link.

- Step 3** Choose **Upload File**.

The Upload File window displays.

- Step 4** Browse to the CorporateDirectory.txt file and click **Upload**.

When Cisco Unified CallManager Administration completes the file upload, a confirmation window displays.



Note Although Cisco Unified CallManager can import any file that you specify, the system can only use data from files that are named CorporateDirectory.txt.

- Step 5** Click **Close**.



Note To update the corporate directory list, update the CorporateDirectory.txt file and upload the file again. Cisco Unified CallManager Administration overwrites the previous file.

Additional Information

See the [“Related Topics” section on page 14-40](#).

Deleting the CorporateDirectory.txt File

If you want to use the user list generated by the Cisco Unified CallManager Attendant Console service rather than a user list that you imported from a separate directory server, you must delete the CorporateDirectory.txt file that you imported. The Cisco Unified CallManager Attendant Console service will generate a new AutoGenerated.txt file when the Cisco Unified CallManager Attendant Console service starts and when the directory sync period expires if the Directory Sync Period service parameter does not equal zero.

To delete the CorporateDirectory.txt file, use the following procedure:

Procedure

-
- Step 1** In Cisco Unified CallManager Administration, choose **Application > Cisco Unified CM Attendant Console > Cisco Unified CM Attendant Console User File Upload**.
- The Attendant Console User File Upload window displays.
- Step 2** Click the **Delete** button that appears next to the CorporateDirectory.txt link.
- Step 3** To delete the CorporateDirectory.txt file, click **OK**. To continue without deleting the file, click **Cancel**.



Note The Cisco Unified CallManager Attendant Console service will generate a new AutoGenerated.txt file when the Cisco Unified CallManager Attendant Console service starts and when the directory sync period expires if the Directory Sync Period service parameter does not equal zero.

Additional Information

See the [“Related Topics” section on page 14-40](#).

Installing the Cisco Unified CallManager Attendant Console Plug-in on an Attendant PC

You access the Cisco Unified CallManager Attendant Console plug-in from the Cisco Unified CallManager Application Plugin Installation window. This section describes how to install the attendant console on a user PC.

Before You Begin

Add the attendant console user and the phone that you want to associate with the attendant console to the Cisco Unified CallManager database. For more information on adding users, see the [“Configuring an Attendant Console User” section on page 14-20](#). For more information on adding phones, “Configuring Cisco Unified IP Phones” section in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

Make sure that you have administrative privileges on the attendant PC when installing Cisco Unified CallManager Attendant Console.

Procedure

-
- Step 1** From each Cisco Unified CallManager Attendant Console PC, browse into a server that is running Cisco Unified CallManager Administration and log in with administrative privileges.



Tip To browse into the server, enter `https://<CM-server-name>/ccmadmin/showHome.do`, where <CM-server-name> equals the name of the server, in the Address bar in the web browser.

- Step 2** From Cisco Unified CallManager Administration, choose **Application > Plugins**.

- Step 3** Click the icon for the Cisco Unified CallManager Attendant Console.
The Cisco Unified CallManager Attendant Console installation wizard runs.
- Step 4** To acknowledge the installation, click **Yes**.
- Step 5** In the initial installation wizard window, click **Next**.
- Step 6** To install the attendant console in the default location, click **Next**.



Note If you do not install the attendant console in the default location, it is possible that you will not be able to launch the Cisco Unified CallManager Attendant Console.

- Step 7** In the Ready to Install window, click **Next**.
- Step 8** After the installation program finishes installing files, choose whether you want to restart the computer now or later; then, click **Finish**.
- Step 9** If prompted, restart the computer.
If you installed Windows XP SP2 on the client PC, see the [“Starting Cisco Unified CallManager Attendant Console After Installing Windows XP SP2” section on page 14-36](#) for information on unblocking the firewall, so the attendant can use the attendant console.
- Step 10** If the attendant does not have administrative privileges on the PC, grant read, write, and execute permissions on the folder where you installed Cisco Unified CallManager Attendant Console. By default, you install the Cisco Unified CallManager Attendant Console in C:\Program Files\Cisco\CallManager Attendant Console. For more information on setting folder permissions, refer to your operating system documentation.
- Step 11** Configure or update any attendant console settings that you did not configure during the installation process. See the [“Configuring Cisco Unified CallManager Attendant Console Settings” section on page 14-37](#).



Tip If you change IP addresses of the Cisco Unified CallManager servers or the device pool of the attendant phone changes after you install the attendant console plug-in, the attendants must close and open Cisco Unified CallManager Attendant Console, so the application can download the list of servers in the Cisco Unified CallManager group.

Additional Information

See the [“Related Topics” section on page 14-40](#).

Starting Cisco Unified CallManager Attendant Console After Installing Windows XP SP2

When you start Cisco Unified CallManager Attendant Console for the first time after you install Windows XP SP2, a dialog box displays that indicates that Windows Firewall has blocked some features of the ACClient application. To create an exception in the Windows Firewall, so you can continue using Cisco Unified CallManager Attendant Console, click **Unblock**. The operating system configures the exception automatically.

After you unblock the firewall, configure or update any attendant console settings that you did not configure during the installation process. See the “[Configuring Cisco Unified CallManager Attendant Console Settings](#)” section on page 14-37.

Additional Information

See the “[Related Topics](#)” section on page 14-40.

Configuring Cisco Unified CallManager Attendant Console Settings

Configure each attendant console to meet the following criteria:

- Provide the attendant console username and password.
- Connect to the correct Cisco CallManager Attendant Console server and directory number for the Cisco Unified IP Phone that the attendant uses with the attendant console.

After you install the attendant console, you must configure the attendant console before a user can log in to the console. Use the procedure in this section to configure settings that are not specified during installation, to view current settings, or to update the attendant console configuration.

After it is configured, the attendant console operates with the specified settings until the administrator changes them.



Note

If you change the IP addresses of the nodes in the cluster, you may also need to change the IP address in the Attendant Server Host Name or IP Address field in the Attendant Console Settings dialog box.

Procedure

-
Step 1	On the PC where the attendant console is installed, choose Start > Programs > Cisco Unified CallManager > Cisco Unified CallManager Attendant Console or click the Cisco Unified CallManager Attendant Console icon on the desktop; then, click Yes to launch the attendant console.
Step 2	Click Settings .
Step 3	Enter the appropriate configuration settings, as described in Table 14-5 .
Step 4	Click Save . You have now configured the settings for the attendant console, and the settings can now be used for call-distribution activities.
-

Additional Information

See the “[Related Topics](#)” section on page 14-40.

Attendant Console Configuration Settings

[Table 14-5](#) describes Cisco Unified CallManager Attendant Console configuration settings.

Table 14-5 Settings Dialog Box

Field/Check Box	Notes
Basic Tab (Cisco requires that you enter the information in the appropriate fields.)	
Attendant Server Host Name or IP Address	Enter the appropriate information in the field.
Directory Number of Your Phone	Confirm or enter the directory number of the Cisco Unified IP Phone that the attendant uses with the attendant console. If you enter a directory number that appears on more than one device, the Device Selector dialog box displays when you click Save. Choose the device that you want to use with the attendant console from the drop-down list box and click OK.
Attendant Console Client CallBack Port	If you are using a firewall, specify the port that the firewall should use to send callback messages to the attendant console client. Valid port numbers include 0 and port numbers equal to or greater than 1023.
Advanced Tab (You can enter information in these optional fields to change the default settings.)	
Path of Local Directory File	If you want the console to access a local user list rather than a centralized user list from Cisco Unified CallManager Administration, enter the path to the user list file on the attendant PC or network share that contains the directory information.
Directory Reload Interval (in seconds)	Enter the time (in seconds) that the Cisco Unified CallManager Attendant Console server waits before reloading the user list that displays in the Directory window of the Cisco Unified CallManager Attendant Console.
Call Processing Server Host Name or IP Address	Enter the call processing server host name or IP address if it differs from the attendant server that you specified on the Basic tab.
Local Host IP Address (for line state)	Enter the IP address that your client uses to receive line state updates. Note If the attendant PC has two Network Interface Cards (NICs), you can specify the IP address that will receive line state updates.
Enable Trace	Check the check box to ensure that you can troubleshoot issues that are associated with the attendant console.

Table 14-5 Settings Dialog Box (continued)

Field/Check Box	Notes
Enable Audible Alerts	To enable audible alerts that indicate when the attendant receives calls (incoming and broadcast), drops calls, parks calls, and places calls on hold as well as that indicate how long calls have been on hold, check the Enable Audible Alerts check box. The audible alerts sound once per call event. The “audio” subdirectory of the Cisco Unified CallManager Attendant Console application contains the audible alert files. By default, the system specifies the directory location, C:\Program Files\Cisco\CallManager Attendant Console\audio.
Show Accessibility Messages	You can enable accessibility messages so that dialog boxes display information about the status of the attendant console, such as when call control goes up or down. For information on accessing the Attendant Settings dialog box, see http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/attndnt/call_att/141/english/ac_1_eng.htm#wp4911.
Hold Call When Dial Pad is Active	If you want the attendant console to place a call on hold while the attendant uses the Dial Pad window, check this check box.

Additional Information

See the “Related Topics” section on page 14-40.

Configuring Held Icon Timers

The color of the held icons on the attendant console indicates how long a call has been on hold. The WaitTimeMedium parameter indicates the time before the held icon turns yellow. The WaitTimeLong parameter indicates the time before the held icon turns red. By default, the held icon turns yellow when a call remains on hold for 60 seconds and turns red when the call remains on hold for 120 seconds. To configure the duration after which the held icons change color, perform the following procedure.

**Note**

Cisco recommends that you do not change the default values of the held icon timers.

Procedure

- Step 1** Open the GlobalUI.properties files that are located on the attendant PC in the ..\Program Files\Cisco\CallManager Attendant Console\etc directory.
- Step 2** To change the time before the held icon turns yellow, edit the WaitTimeMedium parameter.
- Step 3** To change the time before the held icon turns red, edit the WaitTimeLong parameter.
- Step 4** Save and close the GlobalUI.properties file.

Additional Information

See the [“Related Topics”](#) section on page 14-40.

Dependency Records

To find specific directory numbers, refer to the “Dependency Records Buttons” section in the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

Related Topics

- End User Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Dependency Records, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Application Users and End Users, *Cisco Unified CallManager System Guide, Release 5.0(4)*

Attendant Console

- [Configuration Checklist for Cisco Unified CallManager Attendant Console, page 14-17](#)
- [Introducing Cisco Unified CallManager Attendant Console, page 14-1](#)
- [System Requirements for Cisco Unified CallManager Attendant Console, page 14-12](#)
- [Interactions and Restrictions, page 14-13](#)
- [Understanding Call Queuing, page 14-9](#)
- [Configuring Cisco Unified CallManager Attendant Console, page 14-16](#)
- [Related Topics, page 14-40](#)

Attendant Console Server

- [Understanding the Cisco CallManager Attendant Console Server Service, page 14-10](#)
- [Cisco Unified CallManager Attendant Console Redundancy, page 14-11](#)
- [Cisco CallManager Attendant Console Server Service Configuration, page 14-32](#)

Attendant Console User

- [Understanding Cisco Unified CallManager Attendant Console Users, page 14-2](#)
- [Finding an Attendant Console User, page 14-19](#)
- [Configuring an Attendant Console User, page 14-20](#)
- [Cisco Unified CallManager Attendant Console User Configuration Settings, page 14-20](#)
- [Enabling Device Security for Cisco Unified CallManager Attendant Console, page 14-21](#)

Hunt Groups

- [Understanding Pilot Points and Hunt Groups, page 14-2](#)
- [Understanding Linked Hunt Groups, page 14-5](#)
- [Understanding Circular Hunt Groups, page 14-6](#)
- [Understanding Broadcast Hunting, page 14-8](#)
- [Configuring Hunt Groups, page 14-29](#)

- [Configuring Hunt Group Members, page 14-29](#)
- [Deleting Hunt Group Members, page 14-32](#)
- [Hunt Group Configuration Settings, page 14-30](#)

Media Resources

- Media Resource Management, *Cisco Unified CallManager System Guide, Release 5.0(4)*

Pilot Points

- [Understanding Pilot Points and Hunt Groups, page 14-2](#)
- [Finding a Pilot Point, page 14-23](#)
- [Configuring a Pilot Point, page 14-24](#)
- [Deleting a Pilot Point, page 14-27](#)
- [Pilot Point Configuration Settings, page 14-25](#)
- [Resetting a Pilot Point, page 14-28](#)
- [Associating Devices with the Attendant Console Authorization User, page 14-28](#)

Dial Rules

- Application Dial Rules Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- Directory Lookup Dial Rules Configuration, *Cisco Unified CallManager Administration Guide, Release 5.0(4)*

Directory Lists

- [Understanding the Cisco Unified CallManager Attendant Console Directory, page 14-9](#)
- [Creating and Uploading the CorporateDirectory.txt File, page 14-33](#)
- [Deleting the CorporateDirectory.txt File, page 14-34](#)

Attendant Console Plug-in

- [Installing the Cisco Unified CallManager Attendant Console Plug-in on an Attendant PC, page 14-35](#)
- [Starting Cisco Unified CallManager Attendant Console After Installing Windows XP SP2, page 14-36](#)
- [Configuring Cisco Unified CallManager Attendant Console Settings, page 14-37](#)
- [Attendant Console Configuration Settings, page 14-37](#)
- [Configuring Held Icon Timers, page 14-39](#)

Additional Documentation

- *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)*
- *Cisco Unified CallManager Serviceability System Guide, Release 5.0(4)*
- *Cisco Unified CallManager Attendant Console User Guide*



PART 5

Cisco Unified CallManager Serviceability Administration Guide





Managing Services

This chapter contains information on the following topics:

- [Activating and Deactivating Feature Services, page 15-1](#)
- [Starting, Stopping, Restarting, and Refreshing Status of Services in Control Center, page 15-4](#)
- [Using a Command Line Interface to Start and Stop Services, page 15-6](#)

Activating and Deactivating Feature Services

You activate and deactivate services in the Service Activation window in Cisco Unified CallManager Serviceability. Services that display in Service Activation window do not start until you activate them.

Cisco Unified CallManager allows you to activate and deactivate features services only. You may activate or deactivate as many services as you want at the same time. Some feature services depend on other services, and the dependent services get activated before the feature service activates.



Tip

Before you activate services in the Service Activation window, review [Table 15-1](#).

Perform the following procedure to activate or deactivate Cisco Unified CallManager services in Cisco Unified CallManager Serviceability.

Procedure

Step 1 Choose **Tools > Service Activation**.

The Service Activation window displays.

Step 2 From the Server drop-down list box, choose the server.

The window displays the service names for the server that you chose and the activation status of the services.

Step 3 Perform one of the following tasks:

- To activate services for a single server configuration, click the **Set Default** button or activate the services that you want to use.
You can choose all services that are required to run on a single server by clicking the Set Default button. This action not only chooses all required services but also checks for service dependencies.
- For a multiserver configuration, review [Table 15-1](#) for service activation recommendations; then, check the check boxes next to the services that you want to activate.

Table 15-1 Service Activation Recommendation

Service/Servlet	Activation Recommendations
CM Services	
Cisco CallManager	This service supports Cisco Unified CallManager. In the Control Center—Network Services, ensure that the Cisco RIS Data Collector service and Database Layer Monitor service are running on the server. Tip Before you activate this service, verify that the Cisco Unified CallManager displays in the Cisco Unified CallManager Find/List window in Cisco Unified CallManager Administration. If the server does not display, add the Cisco Unified CallManager before you activate this service. For information on how to add the Cisco Unified CallManager, refer to the <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>.
Cisco TFTP	If you have more than one server in the cluster, activate this service on one server that is dedicated specifically for the Cisco TFTP service. Configure Option 150 if you activate this service on more than one server in the cluster.
Cisco Messaging Interface	Activate on only one server in the cluster. Do not activate this service if you plan to use Cisco Unity voice-messaging system.
Cisco IP Voice Media Streaming App	If you have more than one server in the cluster, activate on one or two servers per cluster. You may activate on a server that is dedicated specifically for music on hold. This service requires that you activate Cisco TFTP on one server in the cluster. Do not activate this service on the first node or on any servers that run the Cisco CallManager service.
Cisco CTIManager	Activate on each server to which JTAPI/TAPI applications will connect. CTIManager activation requires the Cisco CallManager services also to be activated on the server. See the “ Cisco CallManager ” service in the “ Service Management ” section on page 19-1 for more information on CTIManager and Cisco CallManager services interaction.
Cisco CallManager Attendant Console Server	If you are planning to use Cisco Unified CallManager Attendant Console, activate on every server in the cluster that runs the Cisco CallManager service.
Cisco Extension Mobility	Activate on each server that the Cisco Extension Mobility application accesses.
Cisco Extended Functions	Activate this service, which supports the Quality Report Tool (QRT), on one or more servers that run the Cisco RIS Data Collector. Make sure that you activate the Cisco CTIManager service on a server in the cluster.

Table 15-1 Service Activation Recommendation (continued)

Service/Servlet	Activation Recommendations
Cisco IP Phone Services	Activate this service only on one server (any server) in the cluster.
Cisco Dialed Number Analyzer	If you are planning to use Cisco Unified CallManager Dialed Number Analyzer, activate this service. This service may consume a lot of resources, so only activate this service on the node with the least amount of call-processing activity or during off-peak hours.
Cisco Extension Mobility Application	The application automatically activates when Cisco Extension Mobility is activated.
Cisco DHCP Monitor Service	When the DHCP Monitor service is enabled, it detects changes in the database that affect IP addresses for the IP phones, modifies the /etc/dhcpd.conf file, and stops and restarts the DHCPD daemon with the updated configuration file. Activate this service on the server that has DHCP enabled.
CTI Services	
Cisco IP Manager Assistant	If you are planning to use Cisco Unified CallManager Assistant, activate this service on any two servers (Primary and Backup) in the cluster. Ensure that Cisco CTI Manager service is activated in the cluster. Refer to <i>Cisco Unified CallManager Features and Services Guide, Release 5.0(4)</i> , for other recommendations.
Cisco WebDialer Web Service	Activate on one server per cluster.
CDR Services	
Cisco SOAP-CDRonDemand Service	You can activate the Cisco SOAP-CDRonDemand Service only on the first node, and it requires that the Cisco CDR Repository Manager and Cisco CDR Agent services are running on the same server.
Cisco CAR Scheduler	You can activate the Cisco CAR Scheduler service only on the first node, and it requires that the Cisco CAR Web Service is activated and running on the server. It also requires that the Cisco CDR Repository and Cisco CDR Agent services are running on the same server.
Cisco CAR Web Service	You can activate the Cisco CAR Web Service only on the first node, and it requires that the Cisco CAR Scheduler service is activated and running on the server and that the Cisco CallManager CDR Repository Manager also is running on the same server.
Database and Admin Services	
Cisco AXL Web Service	Activate on the first node only. Failing to activate this service causes the inability to update Cisco Unified CallManager from client-based applications that use AXL.
Cisco Bulk Provisioning Service	You can activate the Cisco Bulk Provisioning Service only on the first node. If you use the Bulk Administration Tool (BAT) to administer phones and users, you must activate this service.
Cisco TAPS Service	Before you can use the Cisco Unified CallManager Auto-Register Phone Tool, you must activate this service on the first node. When you create dummy MAC addresses for the Cisco Unified CallManager Auto-Register Phone Tool, ensure that the Cisco Bulk Provisioning Service is activated on the same node.

Table 15-1 *Service Activation Recommendation (continued)*

Service/Servlet	Activation Recommendations
Performance and Monitoring Services	
Cisco Serviceability Reporter	Activate on only the first node. Note The service only generates reports on the first node even if you activate the service on other nodes.
Cisco CCM SNMP Service	If you use SNMP, activate this service on all servers in the cluster.
Security Services	
Cisco CTL Provider	Activate on all servers in the cluster.
Cisco Certificate Authority Proxy Function (CAPF)	Activate on only the first node.
Directory Services	
Cisco DirSync	Activate only on the first node.

Step 4 After you finish making the appropriate changes, click **Update**.

**Tip**

To deactivate services that you activated, uncheck the check boxes next to the services that you want to deactivate; click **Update**.

Additional Information

See the [Related Topics](#), page 15-6.

Starting, Stopping, Restarting, and Refreshing Status of Services in Control Center

Control Center in Cisco Unified CallManager Serviceability allows you to view status, refresh the status, and to start, stop, and restart Cisco Unified CallManager services for a particular server in a cluster. Starting, stopping, or restarting a Cisco CallManager service causes all Cisco Unified IP Phones and gateways that are currently registered to that Cisco CallManager service to fail over to their secondary Cisco CallManager service. Devices and phones need to restart only if they cannot register with another Cisco CallManager service. Starting, stopping, or restarting a Cisco CallManager service causes other installed applications (such as Conference Bridge or Cisco Messaging Interface) that are homed to that Cisco Unified CallManager to start and stop as well.

**Note**

If you are upgrading Cisco Unified CallManager, those services that were already started on your system will start after the upgrade.

**Caution**

Stopping a Cisco CallManager service also stops call processing for all devices that the service controls. When a Cisco CallManager service is stopped, calls from an IP phone to another IP phone will stay up; calls in progress from an IP phone to a Media Gateway Control Protocol (MGCP) gateway will also stay up, and other types of calls will get dropped.

Perform the following procedure to start, stop, restart, or view the status of services for a particular server in a cluster. You can start, stop, or refresh only one service at a time.

Procedure

Step 1 Depending on the service type that you want to start/stop/restart/refresh, perform one of the following tasks:

- Choose **Tools > Control Center—Feature Services**.

**Tip**

You can only start/stop/restart feature services that are activated. To activate a service, see the [“Activating and Deactivating Feature Services” section on page 15-1](#).

- Choose **Tools > Control Center—Network Services**.

Step 2 From the Server drop-down list box, choose the server.

The window displays the service names for the server that you chose, the service type, and service status. The window also displays the status of the services (Started, Running or Stopped)

Step 3 Perform one of the following tasks:

- Click the radio button next to the service that you want to start and click the **Start** button.
The Status changes to reflect the updated status.
- Click the radio button next to the service that you want to restart and click the **Restart** button.
A message indicates that restarting may take a while. Click **OK**.
- Click the radio button next to the service that you want to stop and click the **Stop** button.
The Status changes to reflect the updated status.
- To get the latest status of the services, click the **Refresh** button.
- To go to the Service Activation window or to the other Control Center window, choose an option from the Related Links drop-down list box and click **Go**.

Additional Information

See the [Related Topics, page 15-6](#).

Using a Command Line Interface to Start and Stop Services

You can start and stop the following services by issuing a command in the command line interface (CLI):

- System NTP
- System SSH
- Service Manager
- A Cisco DB
- Cisco Tomcat
- Cisco Database Layer Monitor
- Cisco Unified CallManager Serviceability

To start a service, enter **utils service start <service name>**, where service name equals the entire name of the service.

To stop a service, enter **utils service stop <service name>**, where service name equals the entire name of the service.

**Tip**

You must start and stop all other services from Control Center in Cisco Unified CallManager Serviceability.

Additional Information

See the [Related Topics](#), page 15-6.

Related Topics

- [Starting, Stopping, Restarting, and Refreshing Status of Services in Control Center](#), page 15-4
- [Activating and Deactivating Feature Services](#), page 15-1
- [Service Management](#), *Cisco Unified CallManager New and Changed Information Guide*, Release 5.1(1)



Alarm Configuration

Cisco Unified CallManager Serviceability Alarms assist system administrators and support personnel in troubleshooting Cisco Unified CallManager problems by enabling administrators to configure alarms and events and by providing alarm message definitions. An administrator configures alarms and trace parameters and provides the information to a Cisco TAC engineer.

Administrators use alarms to provide runtime status and state of the system and to take corrective action for problem resolution; for example, to determine whether phones are registered and working. Alarms contain information such as explanation and recommended action. Alarm information includes application name, machine name, and cluster name to help you perform troubleshooting for problems that are not on your local Cisco Unified CallManager.

You can configure alarms for Cisco Unified CallManager servers that are in a cluster and services for each server, such as Cisco Unified CallManager, Cisco TFTP, and Cisco CTIManager. You configure the alarm interface to send alarm information to multiple destinations, and each destination can have its own alarm event level (from debug to emergency). Then, you use the real-time monitoring tool to collect and view the alarms.

When a service issues an alarm, the alarm interface sends the alarm to the chosen monitors (for example, SDI trace, Cisco RIS Data Collector). The monitor forwards the alarm or writes it to its final destination (such as a log file).

This chapter contains the following topics:

- [Configuring or Updating an Alarm for a Service, page 16-1](#)
- [Alarm Destination Settings, page 16-3](#)
- [Alarm Event Level Settings, page 16-4](#)

Configuring or Updating an Alarm for a Service

This section describes how to configure an alarm for any Cisco Unified CallManager service.



Note

Cisco recommends that you do not change SNMP Trap and Catalog configurations.

Refer to your online OS documentation for more information on how to use your standard registry editor.

Procedure

Step 1 Choose **Alarm > Configuration**.

The Alarm Configuration window displays.

Step 2 From the Server drop-down box, choose the server for which you want to configure the alarm.

Step 3 From the Service drop-down box, choose the service for which you want to configure the alarm.



Note The drop-down list box displays all services (active and inactive).

In the Alarm Configuration window, a list of alarm monitors with the event levels displays for the chosen service displays.

Step 4 Check the check box or boxes for the desired alarm destination as described in [Table 16-1](#).

Step 5 In the Alarm Event Level selection box, click the Down arrow.

A list with event levels displays.

Step 6 Click the desired alarm event level as described in [Table 16-2](#).

Step 7 To apply the current settings for selected services to all nodes in a cluster, check the **Apply to all Nodes** check box.

Step 8 To save your configuration, click the **Update** button.



Note To set the default, click the **Set Default** button; then, click **Update**.

Additional Information

See the [Related Topics, page 16-4](#).

Alarm Destination Settings

Table 16-1 describes the alarm destination settings.

Table 16-1 Alarm Destinations

Name	Destination description
Enable Alarm for Local Syslogs	SysLog viewer. The program logs Cisco Unified CallManager errors in the Application Logs within SysLog Viewer and provides a description of the alarm and a recommended action. You can access the SysLog Viewer from the Serviceability Real-Time Monitoring Tool. For information on viewing logs with the SysLog Viewer, see the “Using SysLog Viewer in RTMT” section in the <i>Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)</i>.
Enable Alarm for Remote Syslogs	Syslog file. Check this check box to enable the Syslog messages to be stored on a Syslog server and to specify the Syslog server name. If this destination is enabled and no server name is specified, Cisco Unified CallManager does not send the Syslog messages. Note In the Server field, enter the name or IP address of the remote Syslog server that you want to use to accept Syslog messages. Do not specify a Cisco Unified CallManager node as the destination because the Cisco Unified CallManager node does not accept Syslog messages from another server. For example, if you want to send the alarms to CiscoWorks 2000, specify the CiscoWorks 2000 server name.
Enable Alarm for SDI Trace	The SDI trace library. To log alarms in the SDI trace log file, check this check box and check the Trace On check box in Trace Configuration window for the chosen service. For more information on using the Trace Configuration window, see the “Configuring Trace Parameters” section in the <i>Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)</i>.
Enable Alarm for SDL Trace	The SDL trace library. This destination applies only to Cisco CallManager and CTIManager services. Configure this alarm destination by using Trace SDL configuration.

Additional Information

See the [Related Topics, page 16-4](#).

Alarm Event Level Settings

Table 16-2 describes the alarm event level settings.

Table 16-2 **Alarm Event Levels**

Name	Description
Emergency	This level designates system as unusable.
Alert	This level indicates that immediate action is needed.
Critical	Cisco Unified CallManager detects a critical condition.
Error	This level signifies an error condition exists.
Warning	This level indicates that a warning condition is detected.
Notice	This level designates a normal but significant condition.
Informational	This level designates information messages only.
Debug	This level designates detailed event information that Cisco TAC engineers use for debugging.

Additional Information

See the [Related Topics](#), page 16-4.

Related Topics

- [Configuring or Updating an Alarm for a Service](#), page 16-1
- [Alarm Destination Settings](#), page 16-3
- [Alarm Event Level Settings](#), page 16-4
- [Alarms](#), *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*



Troubleshooting Trace Setting Configuration

The Troubleshooting Trace Settings window allows you to choose the services in Cisco Unified CallManager for which you want to set predetermined troubleshooting trace settings. This chapter contains information on how to set and reset troubleshooting trace settings for specific services.



Note Leaving Troubleshooting trace enabled for a long time increases the size of the trace files and may impact the performance of the services.

Procedure

- Step 1** From Cisco Unified CallManager Serviceability, choose **Trace > Troubleshooting Trace Settings**.
- Step 2** From the Server drop-down list box, choose the server where you want to troubleshoot trace settings; then, click **Go**.
- Step 3** Perform one of the following tasks:
- To check specific services for the node that you chose in the Server drop-down list box, check the service(s) check box(es) in the Services pane; for example, the CM Services, CTI Services, or Database and Admin Services panes (and so on).

This task affects only the node that you chose in the Server drop-down list box.
 - Check one of the following check boxes:
 - **Check All Services**—Automatically checks all check boxes for the services on the current node that you chose in the Server drop-down list box.
 - **Check Selected Services on All Nodes**—Allows you to check specific service check boxes in the Troubleshooting Trace Setting window. This setting applies for all nodes in the cluster where the service is activated.
 - **Check All Services on All Nodes** —Automatically checks all check boxes for all services for all nodes in the cluster. When you check this check box, the Check All Services and Check Selected Services on All Nodes check boxes automatically get checked.



Note The services that are not activated on a Cisco Unified CallManager node display as N/A.

- Step 4** Click the **Save** button.

Step 5 After you configure troubleshooting trace for one or more services, the following Reset Troubleshooting Traces buttons appear enabled. If you want to restore the original trace settings, click one of the following buttons:

- **Reset Troubleshooting Traces**—Restores the original trace settings for the services on the node that you chose in the Server drop-down list box; also displays as an icon that you can click.
- **Reset Troubleshooting Traces On All Nodes**—Restores the original trace settings for the services on all nodes in the cluster.

After you click the reset button, the window refreshes, and the service check boxes display as unchecked.

Additional Information

See the [Related Topics](#), page 17-2.

Related Topics

- [Trace](#), *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*



Real-Time Monitoring Configuration

This chapter contains the following information for configuring the Cisco Unified CallManager Real-Time Monitoring Tool (RTMT).

- [Installing the Real-Time Monitoring Tool \(RTMT\), page 18-1](#)
- [Uninstalling RTMT, page 18-2](#)
- [Using RTMT, page 18-3](#)
- [Configuring E-mail Notification, page 18-4](#)
- [Working with Configuration Profiles, page 18-5](#)
- [Working with Predefined Objects, page 18-7](#)
- [Working with Devices, page 18-10](#)
- [Working with CTI Applications, Devices, and Lines, page 18-13](#)
- [Where to Find More Information, page 18-18](#)



Tip

For information on alert, performance monitoring, trace collection, and syslog viewer configuration, see the [“Where to Find More Information”](#) section on page 18-18.

Installing the Real-Time Monitoring Tool (RTMT)

You can install RTMT, which works for resolutions 800*600 and above, on a Windows 98, Windows XP, Windows 2000, or Red Hat Linux with KDE and/or Gnome client.



Tip

Ensure that the RTMT version that you install is compatible with the Cisco Unified CallManager version that runs in your cluster; for example, the RTMT version that supports Cisco Unified CallManager 4.X does not support Cisco Unified CallManager 5.X, but the RTMT version that supports Cisco Unified CallManager 5.0 supports Cisco Unified CallManager 5.1.

To monitor Cisco Unified CallManager 4.X and 5.X clusters simultaneously, you must install multiple versions of RTMT (one version per Cisco Unified CallManager release). If you install multiple versions of the plug-in, you can install the versions on the same client as long as the versions exist in different folders. If the installation detects another version in the folder, a message displays. To continue the installation, install the version in a different folder.

To install the tool, perform the following procedure:

Procedure

-
- Step 1** From Cisco Unified CallManager Administration, choose **Application > Plugins**.
 - Step 2** Click the **Find** button.
 - Step 3** To install the RTMT tool on a client that is running the Microsoft Windows operating system, click the **Download** link for the Cisco Unified CallManager Real-Time Monitoring Tool-Windows. To install the RTMT tool on a client that is running the Linux operating system, click the **Download** link for the Cisco Unified CallManager Real-Time Monitoring Tool-Linux.
 - Step 4** Download the executable to the preferred location on your client.
 - Step 5** To install the Windows version, double-click the RTMT icon that displays on the desktop or locate the directory where you downloaded the file and run the RTMT installation file.
The extraction process begins.
 - Step 6** To install the Linux version, ensure that the file has execute privileges; for example, enter the following command, which is case sensitive: **chmod +x CcmServRtmtPlugin.bin**
 - Step 7** After the RTMT welcome window displays, click **Next**.
 - Step 8** To accept the license agreement, click **I accept the terms of the license agreement**; then, click **Next**.
 - Step 9** Choose the location where you want to install RTMT. If you do not want to use the default location, click **Browse** and navigate to a different location. Click **Next**.
 - Step 10** To begin the installation, click **Next**.
The Setup Status window displays. Do not click Cancel.
 - Step 11** To complete the installation, click **Finish**.
-

Additional Information

See the [Related Topics, page 18-18](#).

Uninstalling RTMT



Tip

When you use the tool (RTMT), it saves user preferences and downloaded module jar files (the cache) locally on the client machine. The system saves the cache in the Cisco Unified CallManager database. When you uninstall RTMT, you choose whether to delete or save the cache.

On a Windows client, you uninstall RTMT through **Add/Remove Programs** under the Control Panel. (Choose **Start > Settings > Control Panel > Add/Remove Programs**.)

To uninstall RTMT on a Red Hat Linux with KDE and/or Gnome client, choose **Start > Accessories > Uninstall Real-time Monitoring tool** from the task bar.

Additional Information

See the [Related Topics, page 18-18](#).

Using RTMT

Before You Begin

Before you can use RTMT, you must activate the Cisco AMC Service on each node in the cluster. From Cisco Unified CallManager Serviceability, choose **Tools > Service Activation** and check the **Cisco AMC Service** check box. Click **Update**.

Procedure

-
- Step 1** After you install the plug-in, perform one of the following tasks:
- From your Windows desktop, double-click the **Cisco Unified CallManager Real-Time Monitoring Tool** icon.
 - Choose **Start > Programs > Cisco CallManager Serviceability > Real-Time Monitoring Tool > Real-Time Monitoring Tool**.

The Real-Time Monitoring Tool Login window displays.

- Step 2** In the Host IP Address field, enter either the IP address or host name of the first node.
- Step 3** In the User Name field, enter the CCMAdministrator application user username; for example, the default username for this user equals **CCMAdministrator**.
- Step 4** In the Password field, enter the CCMAdministrator application user password that you established for the username.



Note If the authentication fails or if the server is unreachable, the tool prompts you to reenter the server and authentication details, or you can click the Cancel button to exit the application. After the authentication succeeds, RTMT launches the monitoring module from local cache or from a remote node, when the local cache does not contain a monitoring module that matches the backend Cisco Unified CallManager version.

- Step 5** Enter the port that the application will use to listen to the server. The default setting equals 8443.
- Step 6** Check the **Secure Connection** check box.
- Step 7** Click **OK**.
- Step 8** Add the certificate store by clicking **Yes**.
- Step 9** See the following list for tasks that you can perform in RTMT:
- To configure the mail server for e-mail alerts, see the [“Configuring E-mail Notification” section on page 18-4](#).
 - To create configuration profiles, see the [“Adding Configuration Profiles” section on page 18-5](#).
 - To monitor predefined objects, see the [“Working with Predefined Objects” section on page 18-7](#).
 - To work with devices, see the [“Working with Devices” section on page 18-10](#).
 - To work with CTI applications, devices, and lines, see the [“Working with CTI Applications, Devices, and Lines” section on page 18-13](#).
 - To work with Alerts, see “Alert Configuration in RTMT” in the *Cisco CallManager Serviceability Administration Guide, Release 5.0(4)*.
 - To work with performance monitoring objects, see the “Configuring and Using Performance Monitoring” section in the *Cisco CallManager Serviceability Administration Guide, Release 5.0(4)*.

- To collect and view traces, see the “Trace Collection and Log Central in RTMT” in the *Cisco CallManager Serviceability Administration Guide, Release 5.0(4)*.
- To use SysLog Viewer, see the “Using SysLog Viewer in RTMT” in the *Cisco CallManager Serviceability Administration Guide, Release 5.0(4)*.
- To configure the trace setting for RTMT, choose **Edit > Trace Setting**. Click the radio button that applies.
- To hide the Quick Launch Channel, which is the pane that displays on the left side of the window, choose **Edit > Hide Quick Launch Channel**.

To display the Quick Launch Channel after it is hidden, choose **Edit > Hide Quick Launch Channel**.

- To close a monitoring window, choose **Window > Close**. To close all monitoring windows that display, choose **Window > Close All Windows**.
- To access Cisco Unified CallManager Administration or Cisco Unified CallManager Serviceability from the RTMT window, choose **Application > CCMAdmin webpage** (or **CCM Serviceability webpage**).
- To access the Serviceability Report Archive option from RTMT, choose **System > Report Archive**. If the Security Alert window displays, click **Yes**. Enter the administrative user name and password for the server; then, click **OK**.
- To determine the RTMT version that is installed, choose **Help > About**. The version information displays in the window. After you view the information, click **OK**.
- To access documentation for RTMT, choose **Help > Help Topics** (or **For this Window**). For additional information on RTMT or Cisco Unified CallManager Serviceability, refer to the *Cisco Unified CallManager Serviceability System Guide, Release 5.0(4)*, and the *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)*.
- To monitor JVM information, click **System > JVM Information**. The JAVA heap memory usage displays in the window. Click **OK**.
- To log out of RTMT, choose **System > Log Off**. Performing this task logs off the current user, and the Real-Time Monitoring Tool Login window displays.
- To exit the application, choose **System > Exit**. Performing this task closes the application.

Additional Information

See the [Related Topics, page 18-18](#).

Configuring E-mail Notification

To configure e-mail notification, perform the following procedure:

Procedure

- Step 1** In the Mail Server field, enter the e-mail recipient information.
- Step 2** In the Port field, enter the port number of the mail server.

Step 3 Click **OK**.

Additional Information

See the [Related Topics, page 18-18](#).

Working with Configuration Profiles

This section provides information on the following topics:

- [Using the Default Configuration Profile, page 18-5](#)
- [Adding Configuration Profiles, page 18-5](#)
- [Restoring Profiles, page 18-6](#)
- [Deleting Configuration Profiles, page 18-6](#)

Using the Default Configuration Profile

When you initially load RTMT, the system includes a default profile that is called CM-Default. The first time that you use RTMT, it will use the CM-Default profile and display the summary page in the monitor pane. CM-Default monitors all registered phones dynamically in all the Cisco Unified CallManager nodes. If your cluster includes five Cisco Unified CallManager-configured nodes, CM-Default displays all registered phones for each node in a Cisco Unified CallManager cluster, as well as calls in progress and active gateway ports and channels.

See the “[Adding Configuration Profiles](#)” section on [page 18-5](#) for information on how to create your own configuration profile.

Additional Information

See the [Related Topics, page 18-18](#).

Adding Configuration Profiles

After you open multiple monitoring windows in RTMT (such as CPU & Memory, SDL Queue, and performance counters), you can create your own configuration profiles, so you can restore these monitoring windows in a single step rather than opening each window again. You can switch between different profiles during the same RTMT session or use the configuration profile in subsequent RTMT sessions.

The following procedure describes how to create a profile.

Procedure

Step 1 Choose **System > Profile**.

The Preferences dialog box displays.

Step 2 Click **Save**.

The Save Current Configuration dialog box displays.

- Step 3** In the Configuration name field, enter a name for this particular configuration profile.
- Step 4** In the Configuration description field, enter a description of this particular configuration profile.



Note You can enter whatever you want for the configuration profile name and description.

The system creates the new configuration profile.

Additional Information

See the [Related Topics, page 18-18](#).

Restoring Profiles

Perform the following procedure to restore a profile that you configured:

Procedure

- Step 1** Choose **System > Profile**.
The Preferences dialog box displays.
- Step 2** Click the profile that you want to restore.
- Step 3** Click **Restore**.
All windows with precanned settings and/or performance monitoring counters for the restored configuration open.

Additional Information

See the [Related Topics, page 18-18](#).

Deleting Configuration Profiles

Perform the following procedure to delete a profile that you configured:

Procedure

- Step 1** Choose **System > Profile**.
The Preferences dialog box displays.
- Step 2** Click the profile that you want to delete.
- Step 3** Click **Delete**.
- Step 4** Click **Close**.

Additional Information

See the [Related Topics](#), page 18-18.

Working with Predefined Objects

The tool (RTMT) provides a set of default monitoring objects that monitor the health of the system. Default objects include performance counters or critical event status for services that are supported with Cisco Unified CallManager.

This section provides information on the following topics:

- [Viewing/Monitoring a Predefined Object](#), page 18-7
- [Working with Devices](#), page 18-10
- [Working with CTI Applications, Devices, and Lines](#), page 18-13

Viewing/Monitoring a Predefined Object

The monitoring pane for a category, that is, a predefined object, displays the activities of predefined monitoring objects. The following procedure describes how to view information for a category.

Procedure

- Step 1** To view or monitor a category, perform one of the following tasks:
- In the Quick Launch Channel, click the **View** tab. Then, click a category; for example, Summary, Server, Call Process, and so on. If an icon displays for the category, click the icon to display the information that you want to monitor.
 - Depending on which category you want to display, choose one of the following options from [Table 18-1](#):

Table 18-1 **Menu Path for Categories**

Category	Menu Path	Data that Displays
Summary	Monitor > Summary	Displays memory usage, CPU usage, registered phones, calls in progress, and active gateway ports and channels
Server	Monitor > Server > CPU Usage and Memory (or Process, Disk Usage, or Critical Services)	• CPU Usage and Memory—Displays memory and CPU usage • Process—Displays the process name, process ID (PID) and percentage of CPU and memory that is used by the process, the resident and shared memory, and the Nice (level) • Disk Usage—Displays the percentage of disk usage per the largest partition in each host • Critical Services—Displays the services for a specific server

Table 18-1 *Menu Path for Categories (continued)*

Category	Menu Path	Data that Displays
Call Process	Monitor > Call Process > Call Activity (or Gateway Activity, Trunk Activity, SDL Queue, or SIP Activity)	• Call Activity—Displays the call activity for each Cisco Unified CallManager server in the cluster, including calls completed, calls attempted, and calls in progress • Gateway Activity—Displays gateway activity for the Cisco Unified CallManager cluster, including active ports, ports in service, and calls completed • Trunk Activity—Displays the trunk activity for the Cisco Unified CallManager cluster, including calls in progress and calls completed • SDL Queue—Displays SDL queue information, including number of signals in queue and number of processed signals. • SIP Activity—Displays SIP activity for each Cisco Unified CallManager server in the cluster, including summary requests, summary responses, summary of failure responses in, summary of failure responses out, retry requests out, and retry responses out
Service	Monitor > Service > Cisco TFTP (or Heartbeat or Database Summary)	• Cisco TFTP—Displays Cisco TFTP status for each Cisco Unified CallManager server in the cluster, including total TFTP requests, total TFTP requests found, and total TFTP requests aborted • Heartbeat—Displays heartbeat information for the Cisco Unified CallManager, Cisco TFTP, and the Cisco CallManager Attendant Console service • Database Summary—Displays summary information for the database on the Cisco Unified CallManager server, including change notification requests that are queued in the database, change notification requests that are queued in memory, total number of clients connected, and the number of device resets that are in the queue

Table 18-1 Menu Path for Categories (continued)

Category	Menu Path	Data that Displays
Device	Monitor > Device Summary (or Phone Summary)	Device Summary displays information for each Cisco Unified CallManager server in the cluster, including the number of registered phone devices, registered gateway devices, and registered media resource devices. Device Search displays cluster name and device types in tree hierarchy and allows you to query for information on phones and devices. Phone Summary displays information for each Cisco Unified CallManager server in the cluster, including the number of registered phones, registered SIP phones, registered SCCP phones, partially registered phones, and the number of failed registration attempts. Tip Instead of choosing Monitor > Device Summary or Monitor > Phone Summary, you can choose Device > Open Device Search to display the cluster name and device or phone types in the tree hierarchy. Tip To monitor devices, you must perform additional configuration steps, as described in the “Finding Specific Devices to Monitor” section on page 18-10.
CTI Manager	Monitor > CTI Manager	Displays cluster name and CTI types (application, device, and line) in tree hierarchy To monitor specific CTI types, you must perform additional configuration steps, as described in the following sections: • Finding CTI Applications to Monitor, page 18-14 • Finding CTI Devices to Monitor, page 18-14 • Finding CTI Lines to Monitor, page 18-15 You cannot choose CTI Manager by using the menu bar. To monitor the number of open devices, lines, and CTI connections in a single window for each Cisco Unified CallManager server in the cluster, see the “Working with Devices” section on page 18-10.
Performance	Performance > Open Performance	Displays perfmon counters. For more information on using perfmon counters, see the “Configuring and Using Performance Monitoring” in the <i>Cisco CallManager Serviceability Administration Guide, Release 5.0(4)</i>.

- Step 2** Some categories allow you to choose a specific server or device type to monitor. To choose a specific server or device type to monitor, perform one of the following tasks in the panes that are listed:
- CPU and Memory Usage pane—To monitor CPU and memory usage for specific server, choose the server from the Host drop-down list box.
 - Disk Usage pane—To monitor disk usage for a specific server, choose the server from the Disk Usage at Host drop-down list box.
 - Critical Services pane—To monitor critical services for a specific server, choose the server from the Critical Services at Host drop-down list box.

- Gateway Activity pane—To monitor the gateway activity for a specific gateway type, choose the gateway type from the Gateway Type drop-down list box.
- Trunk Activity pane—To monitor the trunk activity for a specific trunk type, choose the trunk type from the Trunk Type drop-down list box.
- SDL Queue pane—To monitor the SDL queue information for a specific SDL queue type, choose the type from the SDL Queue Type drop-down list box.

**Tip**

To zoom in on the monitor of a predefined object, click and drag the left mouse button over the area of the chart in which you are interested. Release the left mouse button when you have the selected area. RTMT updates the monitored view. To zoom out and reset the monitor to the initial default view, press the “R” key.

Additional Information

See the [Related Topics, page 18-18](#).

Working with Devices

This section contains information on the following topics:

- [Finding Specific Devices to Monitor, page 18-10](#)
- [Viewing Phone Information, page 18-12](#)
- [Viewing Device Properties, page 18-12](#)
- [Configuring Polling Rate for Devices and Performance Monitoring Counters, page 18-13](#)

Finding Specific Devices to Monitor

By performing the following procedure, you can monitor data for the following device types:

- Phones
- Gateway Devices
- H.323 Devices
- CTI Devices
- Voice Mail Devices
- Media Resources
- Hunt List
- SIP Trunk

Procedure

Step 1 Perform one of the following tasks:

- Choose **Search > Device >** <device type; for example, **Phone, Gateway, Hunt List**, and so on>. A device selection window displays where you enter the search criteria. Go to [Step 4](#).

- In the quick launch channel, click **Device**; then, click the **Device Search** icon.
- Choose **Device > Open Device Search**.

The Device Search window displays the cluster names and tree hierarchy that lists all device types that you can monitor.



Tip After you display the Device Search or CTI Search panes, you can right-click a device type and choose **CCMAdmin** to go to Cisco Unified CallManager Administration.

Step 2 To find all devices in the cluster or to view a complete list of device models from which you can choose, right-click the cluster name and choose **Monitor**.

Step 3 To monitor a specific device type, right-click or double-click the device type from the tree hierarchy.



Tip If you right-click the device type, you must choose **Monitor** for the device selection window to display.

Step 4 In the Select device with status window, click the radio button that applies.

Step 5 In the drop-down list box next to the radio button that you clicked, choose **Any CallManager** or a specific Cisco Unified CallManager server for which you want the device information to display.



Tip In the remaining steps, you can choose the **< Back**, **Next >**, **Finish**, or **Cancel** buttons.

Step 6 Click the **Next >** button.

Step 7 In the Search by device model pane, click the radio button that applies.



Tip If you chose **Device Model**, choose the device type for which you want the device information to display.

Step 8 Click **Next**.

Step 9 In the Search with name pane, click one of the following radio buttons and enter the appropriate information in the corresponding fields, if required.

Step 10 Click **Next**.

Step 11 In the Monitor following attributes pane, check one or all of the search attributes.

Step 12 Click **Finish**.

Additional Information

See the [Related Topics](#), page 18-18.

Viewing Phone Information

You can view information about phones that display in the RTMT device monitoring pane. This section describes how to view phone information.

Procedure

-
- Step 1** To display the phone in the RTMT device monitoring pane, see the [“Finding Specific Devices to Monitor” section on page 18-10](#).
- Step 2** Perform one of the following tasks:
- Right-click the phone for which you want information to display and choose **Open**.
 - Click the phone and choose **Device > Open**.
- Step 3** In the Select Device with Status pane, click the radio button that applies.
- Step 4** In the drop-down list box next to the radio button that you clicked, choose **Any CallManager** or a specific Cisco Unified CallManager server for which you want the device information to display.
- Step 5** In the Search By Device Model pane, choose the phone protocol that you want to display.
- Step 6** Click the **Any Model** or **Device Model** radio button. If you click the Device Model radio button, choose a particular phone model that you want to display.
- Step 7** Click **Next**.
- Step 8** In the Search With Name pane, click the radio button that applies and enter the appropriate information in the corresponding fields.
- Step 9** In the Monitor following attributes pane, check one or all of the search attributes.
- Step 10** Click **Finish**.
- The Device Information window displays. For more information on the device, choose any field that displays in the left pane of the window.
-

Additional Information

See the [Related Topics, page 18-18](#).

Viewing Device Properties

You can view the properties of devices that display in the RTMT device monitoring pane. This section describes how to view device properties.

Procedure

-
- Step 1** Display the device in the RTMT device monitoring pane. See the [“Finding Specific Devices to Monitor” section on page 18-10](#).
- Step 2** Perform one of the following tasks:
- Right-click the device for which you want property information and choose **Properties**.
 - Click the device for which you want property information and choose **Device > Properties**.
- Step 3** To display the device description information, click the **Description** tab.

Step 4 To display other device information, click the **Other Info** tab.

Additional Information

See the [Related Topics, page 18-18](#).

Configuring Polling Rate for Devices and Performance Monitoring Counters

Cisco Unified CallManager polls counters, devices, and gateway ports to gather status information. In the RTMT monitoring pane, you configure the polling intervals for the performance monitoring counters and devices.



Note

High-frequency polling rate may adversely affect Cisco Unified CallManager performance. The minimum polling rate for monitoring a performance counter in chart view equals 5 seconds; the minimum rate for monitoring a performance counter in table view equals 1 second. The default value for both equals 10 seconds.

The default value for devices equals 10 minutes.

Perform the following procedure to update the polling rate:

Procedure

-
- Step 1** Display the device or performance monitoring counter in the RTMT monitoring pane.
- Step 2** Click the device and choose **Edit > Polling Rate**.
- Step 3** In the Polling Interval pane, specify the time that you want to use.
- Step 4** Click **OK**.
-

Additional Information

See the [Related Topics, page 18-18](#).

Working with CTI Applications, Devices, and Lines

This section contains information on the following topics:

- [Viewing CTI Manager Information, page 18-14](#)
- [Finding CTI Applications to Monitor, page 18-14](#)
- [Finding CTI Devices to Monitor, page 18-14](#)
- [Finding CTI Lines to Monitor, page 18-15](#)
- [Viewing Application Information, page 18-16](#)

Viewing CTI Manager Information

To display a chart of open devices, lines, and CTI connections for each Cisco Unified CallManager server in the cluster, click **CTI** in the quick launch channel; then, click the **CTI Manager** icon.

Additional Information

See the [Related Topics, page 18-18](#).

Finding CTI Applications to Monitor

Perform the following procedure to find specific CTI applications to monitor:

Procedure

- Step 1** Perform one of the following tasks:
- Choose **Search > CTI > CTI Applications**; the selection window displays where you can enter the search criteria. Go to [Step 3](#).
 - In the quick launch channel, click **CTI**; then, click the **CTI Search** icon. The CTI search window displays the cluster names and tree hierarchy that lists all CTI types that you can monitor.
- Step 2** From the tree hierarchy, right-click or double-click **Applications**:



Tip If you right-click the option, choose **Monitor**.

- Step 3** From the CTI Manager drop-down list box, choose the CTI Manager that you want to monitor.
- Step 4** From the Applications Status drop-down list box, choose the application status.
- Step 5** Click **Next**.
- Step 6** In the Application Pattern pane, click the radio button that applies.
- Step 7** Enter the information in the field for the radio button that you clicked; for example, if you clicked the IP Subnet radio button, enter the IP address and the subnet mask in the field.
- Step 8** Click **Next**.
- Step 9** In the Monitor following attributes window, check one or all of the check boxes for the attributes that you want to monitor.
- Step 10** Click **Finish**.

The applications monitoring pane displays the information that you chose.

Additional Information

See the [Related Topics, page 18-18](#).

Finding CTI Devices to Monitor

Perform the following procedure to find specific CTI devices to monitor.

Procedure

-
- Step 1** Perform one of the following tasks:
- Choose **Monitor > CTI > CTI Devices**; the selection window where you can enter the search criteria displays. Go to [Step 3](#).
 - In the quick launch channel, click **CTI**; then, click the **CTI Search** icon. The CTI search window displays the cluster names and tree hierarchy that lists all CTI types that you can monitor.
- Step 2** From the tree hierarchy, right-click or double-click **Devices**.
-  **Tip** If you right-click the option, choose **Monitor**.
-
- Step 3** From the CTI Manager drop-down list box, choose the CTI Manager that you want to monitor.
- Step 4** From the Devices Status drop-down list box, choose the device status.
- Step 5** In the Devices pane, click the radio button that applies.
-  **Tip** If you chose **Device Name**, enter the device name in the field.
-
- Step 6** Click **Next**.
- Step 7** In the Application Pattern window, click the radio button that applies.
- Step 8** Enter the information in the field for the radio button that you clicked; for example, if you clicked IP Subnet, enter the IP address and subnet mask in the field.
- Step 9** Click **Next**.
- Step 10** In the Monitor following attributes window, check one or all check boxes for the attributes that you want to monitor.
- Step 11** Click **Finish**.
- The devices monitoring pane displays the information that you chose.
-

Additional Information

See the [Related Topics, page 18-18](#).

Finding CTI Lines to Monitor

Perform the following procedure to find specific CTI lines to monitor.

Procedure

-
- Step 1** Perform one of the following tasks:
- Choose **Monitor > CTI > CTI Lines**; the selection window displays where you can enter the search criteria. Go to [Step 3](#).
 - In the quick launch channel, click **CTI**; then, click the **CTI Search** icon. The CTI search window displays the cluster names and tree hierarchy that lists all CTI types that you can monitor.

Step 2 From the tree hierarchy, right-click or double-click **Lines**.



Tip If you right-click the option, choose **Monitor**.

Step 3 From the CTI Manager & Status drop-down list box, choose the CTI manager that you want to monitor.

Step 4 From the Lines Status drop-down list box, choose the status.

Step 5 In the Devices pane, click the radio button that applies.



Tip If you chose **Device Name**, enter the device name in the field.

Step 6 In the Lines pane, click the radio button that applies:



Note If you chose **Directory Number**, enter the directory number in the field.

Step 7 Click **Next**.

Step 8 In the Application Pattern pane, click the radio buttons apply:

Step 9 Enter the information in the field for the radio button that you clicked; for example, if you clicked IP Subnet, enter the IP address and subnet mask in the field.

Step 10 Click **Next**.

Step 11 In the Monitor following attributes window, check one or all check boxes for the attributes that you want to monitor.

Step 12 Click **Finish**.

The lines monitoring pane displays the information that you chose.

Additional Information

See the [Related Topics](#), page 18-18.

Viewing Application Information

You can view the application information for selected devices such as the Cisco IP Phone, CTI port, and CTI route point. This section describes how to view application information.

Procedure

Step 1 Display the devices in the RTMT monitoring pane, as described in the [“Finding CTI Devices to Monitor” section on page 18-14](#).

Step 2 Perform one of the following tasks:

- Right-click the device for which you want application information; for example, CTI; then, choose **App Info**.
- Click the device for which you want application information and choose **Device > App Info**.

The Application Information window displays the CTI manager node name, application ID, user ID, application IP address, application status, app time stamp, device time stamp, device name, and CTI device open status.

Step 3 To view updated information, click **Refresh**. To close the window, click **OK**.

Additional Information

See the [Related Topics, page 18-18](#).

Working with Categories

Categories allow you to monitor performance monitoring counters and devices. For example, the default category, CallManager, allows you to monitor six performance monitoring counters in graph format. If you want to monitor more counters, you can configure a new category and display the data in table format.

If you perform various searches for devices, for example, for phones, gateways, and so on, you can create a category for each search and save the results in the category.

Adding a Category

To add a category, perform the following procedure:

Procedure

Step 1 Display the Performance Monitoring or Devices tree hierarchy.

Step 2 Choose **Edit > Add New Category**.

Step 3 Enter the name of the category; click **OK**.

The category tab displays at the bottom of the window.

Additional Information

- See the [Related Topics, page 18-18](#).

Renaming a Category

To rename a category, perform the following procedure:

Procedure

Step 1 Perform one of the following tasks:

- Right-click the category tab that you want to rename and choose **Rename Category**.
- Click the category tab that you want to rename and choose **Edit > Rename Category**.

- Step 2** Enter the new name and click **OK**.
The renamed category displays at the bottom of the window.
-

Additional Information

- See the [Related Topics](#), page 18-18.

Deleting a Category

To delete a category, perform one of the following tasks:

- Right-click the category tab that you want to delete and choose **Remove Category**.
- Click the category tab that you want to delete and choose **Edit > Remove Category**.

Additional Information

See the [Related Topics](#), page 18-18.

Where to Find More Information

- Alert Configuration in RTMT, *Cisco CallManager Serviceability Administration Guide, Release 5.0(4)*
- Configuring and Using Performance Monitoring, *Cisco CallManager Serviceability Administration Guide, Release 5.0(4)*
- Trace Collection and Log Central in RTMT, *Cisco CallManager Serviceability Administration Guide, Release 5.0(4)*
- [Real-Time Monitoring Tool](#), *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*
- Alerts, *Cisco Unified CallManager Serviceability System Guide, Release 5.0(4)*
- [Performance Objects and Counters](#), *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*

Additional Information

See the [Related Topics](#), page 18-18.

Related Topics

- [Adding a Category](#), page 18-17
- [Renaming a Category](#), page 18-17
- [Deleting a Category](#), page 18-18
- [Viewing CTI Manager Information](#), page 18-14
- [Finding CTI Applications to Monitor](#), page 18-14
- [Finding CTI Devices to Monitor](#), page 18-14

- [Finding CTI Lines to Monitor, page 18-15](#)
- [Configuring and Using Performance Monitoring, *Cisco CallManager Serviceability Administration Guide, Release 5.0\(4\)*](#)
- [Working with Devices, page 18-10](#)
- [Viewing Device Properties, page 18-12](#)
- [Finding Specific Devices to Monitor, page 18-10](#)
- [Viewing Phone Information, page 18-12](#)
- [Configuring Polling Rate for Devices and Performance Monitoring Counters, page 18-13](#)
- [Using the Default Configuration Profile, page 18-5](#)
- [Restoring Profiles, page 18-6](#)
- [Using the Default Configuration Profile, page 18-5](#)
- [Deleting Configuration Profiles, page 18-6](#)
- [Adding Configuration Profiles, page 18-5](#)
- [Working with Configuration Profiles, page 18-5](#)
- [Working with Predefined Objects, page 18-7](#)
- [Alert Configuration in RTMT, *Cisco CallManager Serviceability Administration Guide, Release 5.0\(4\)*](#)
- [Using SysLog Viewer in RTMT, *Cisco CallManager Serviceability Administration Guide, Release 5.0\(4\)*](#)
- [Installing the Real-Time Monitoring Tool \(RTMT\), page 18-1](#)
- [Uninstalling RTMT, page 18-2](#)
- [Using RTMT, page 18-3](#)



PART 6

Cisco Unified CallManager Serviceability System Guide





Service Management

Cisco Unified CallManager Serviceability service management includes working with feature and network services and servlets, which are associated with the Tomcat Java Webserver. Feature services allow you to use Cisco Unified CallManager-related features, while network services are required for your system to function.

If something is wrong with a service or servlet, an alarm gets written to an alarm monitor. After viewing the alarm information, you can run a trace on the service. Be aware that services and servlets display different trace levels in the Trace Configuration window.

This chapter, which provides a description of services/servlets, Service Activation, and Control Center, contains information on the following topics:

- [Feature Services, page 19-1](#)
- [Network Services, page 19-7](#)
- [Service Activation, page 19-11](#)
- [Control Center, page 19-12](#)
- [Services Configuration Checklist, page 19-13](#)
- [Where to Find More Information, page 19-14](#)

Feature Services

After a Cisco Unified CallManager installation, the system does not automatically activate feature services, which are Cisco Unified CallManager related services that are required if you want to use Cisco Unified CallManager features. In Cisco Unified CallManager Serviceability, you can activate, start, and stop feature services. After you activate feature services, you can modify associated service parameters in Cisco Unified CallManager Administration. If you are upgrading Cisco Unified CallManager, those services that you activated on the system prior to the upgrade automatically activate and start after the upgrade.

Activation turns on and starts the service. After you activate a service in the Service Activation window, you do not need to start it in the Control Center—Feature Services window. If the service does not start for any reason, you must start it in the Control Center—Features Services window.

In the Service Activation window, Cisco Unified CallManager Serviceability categorizes feature services into the following groups:

- [CM Services, page 19-2](#)
- [CTI Services, page 19-4](#)

- [CDR Services, page 19-4](#)
- [Database and Admin Services, page 19-5](#)
- [Performance and Monitoring Services, page 19-5](#)
- [Security Services, page 19-6](#)
- [Directory Services, page 19-7](#)

In the Control Center—Feature Services window, Cisco Unified CallManager Serviceability categorizes services into the same groups that display in the Service Activation window.

**Tip**

For service activation recommendations, see the [“Service Activation” section on page 19-11](#) and the [“Activating and Deactivating Feature Services” section on page 15-1](#).

CM Services

Cisco CallManager

The Cisco CallManager service provides software-only call processing as well as signaling and call control functionality for Cisco Unified CallManager.

**Tip**

Before you activate this service, verify that the Cisco Unified CallManager displays in the Cisco Unified CallManager Find/List window in Cisco Unified CallManager Administration. If the server does not display, add the Cisco Unified CallManager before you activate this service. For information on how to add the Cisco Unified CallManager, refer to the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

**Tip**

If you deactivate the Cisco CallManager or CTIManager services in Service Activation, the Cisco Unified CallManager where you deactivated the service no longer exists in the database. This means that you cannot choose that Cisco Unified CallManager system for configuration operations in Cisco Unified CallManager Administration because it will not display in the graphical user interface (GUI). If you then reactivate the services on the same Cisco Unified CallManager system, the database creates an entry for Cisco Unified CallManager again and adds a “CM_” prefix to the server name or IP address; for example, if you reactivate the Cisco CallManager or CTIManager service on a server with an IP address of 172.19.140.180, then CM_172.19.140.180 displays in Cisco Unified CallManager Administration. You can now choose the Cisco Unified CallManager, with the new “CM_” prefix, in Cisco Unified CallManager Administration.

The following services rely on Cisco CallManager service activation:

- [Cisco CTIManager, page 19-3](#)
- [CDR Services, page 19-4](#)

Cisco TFTP

Cisco Trivial File Transfer Protocol (TFTP) builds and serves files that are consistent with the trivial file transfer protocol, a simplified version of FTP. Cisco TFTP serves embedded component executable, ringer files, and device configuration files.

A configuration file includes a list of Cisco Unified CallManagers to which devices (telephones and gateways) make connections. When a device boots, the component queries a Dynamic Host Configuration Protocol (DHCP) server for its network configuration information. The DHCP server responds with an IP address for the device, a subnet mask, a default gateway, a Domain Name System (DNS) server address, and a TFTP server name or address. The device requests a configuration file from the TFTP server. The configuration file contains a list of Cisco Unified CallManagers and the TCP port through which the device connects to those Cisco Unified CallManagers.

Cisco IP Voice Media Streaming App

The Cisco IP Voice Media Streaming Application service provides voice media streaming functionality for the Cisco Unified CallManager for use with MTP, conferencing, music on hold (MOH), and annunciator. The Cisco IP Voice Media Streaming Application relays messages from the Cisco Unified CallManager to the IP voice media streaming driver, which handles RTP streaming.

Cisco Messaging Interface

The Cisco Messaging Interface allows you to connect a simplified message desk interface (SMDI)-compliant external voice-messaging system with the Cisco Unified CallManager. The CMI service provides the communication between the voice-messaging system and Cisco Unified CallManager. The SMDI defines a way for a phone system to provide a voice-messaging system with the information that is needed to intelligently process incoming calls.

Cisco CTIManager

The CTI Manager contains the CTI components that interface with applications. With CTI Manager, applications can access resources and functionality of all Cisco Unified CallManagers in the cluster and have improved failover capability. Although one or more CTI Managers can be active in a cluster, only one CTI Manager can exist on an individual server. An application (JTAPI/TAPI) can have simultaneous connections to multiple CTI Managers; however, an application can only use one connection at a time to open a device with media termination.

Cisco Unified CallManager Attendant Console Server

The Cisco CallManager Attendant Console Server service provides centralized services for Cisco Unified CallManager Attendant Console clients and pilot points. For Attendant Console clients, this service provides call-control functionality, line state information for any accessible line within the Cisco Unified CallManager domain, and caching of directory information. For pilot points, this service provides automatic redirection to directory numbers that are listed in hunt groups and failover during a Cisco Unified CallManager failure.

Cisco Extended Functions

The Cisco Extended Functions service provides support for some Cisco Unified CallManager features, including Quality Report Tool (QRT). For more information about individual features, refer to the *Cisco Unified CallManager System Guide, Release 5.0(4)* and the *Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager*.

Cisco CallManager IP Phone Services

When activated, the Cisco CallManager IP Phone Service initializes the service URLs for the Cisco IP Phone services that you configured in Cisco Unified CallManager Administration.

Cisco Dialed Number Analyzer

The Cisco Dialed Number Analyzer service supports the Cisco Unified CallManager Dialed Number Analyzer application, and you can activate/deactivate it from Cisco Unified CallManager Serviceability.

When activated, this application consumes a lot of resources. Cisco does not recommend activating the service on all the nodes in a cluster. Cisco recommends that you activate this service only during off-peak hours or only on one of the nodes of a cluster where call-processing activity is the least.

Cisco DHCP Monitor Service

Cisco DHCP Monitor Service monitors IP address changes for IP phones in the database tables. When a change is detected, it modifies the `/etc./dhcpd.conf` file and restarts the DHCPD daemon.

CTI Services

Cisco IP Manager Assistant

This service supports the Cisco Unified CallManager Assistant application. When activated, Cisco IP Manager Assistant enables managers and their assistants to work together more effectively. Cisco IP Manager Assistant supports two modes of operation: proxy line support and shared line support. The Cisco IP Manager Assistant service supports both proxy line and shared line support in a cluster. Refer to the *Cisco Unified CallManager Features and Services Guide, Release 5.0(4)*.

The feature comprises a call-routing service, enhancements to phone capabilities for the manager, and desktop interfaces that are primarily used by the assistant.

The service intercepts calls that are made to managers and routes them to selected assistants, to managers, or to other targets on the basis of preconfigured call filters. The manager can change the call routing dynamically; for example, by pressing a softkey on the phone, the manager can instruct the service to route all calls to the assistant and can receive status on these calls.

Cisco Unified CallManager users comprise managers and assistants. The routing service intercepts manager calls and routes them appropriately. An assistant user handles calls on behalf of a manager. Cisco IP Manager Assistant comprises features for managers and features for assistants.

Cisco WebDialer Web Service

Cisco WebDialer provides click-to-dial functionality. It allows users in a Cisco Unified CallManager cluster to initiate a call to other users inside or outside the cluster by using a web page or a desktop application. Cisco WebDialer provides a web page that enables users to call each other within a cluster. Cisco WebDialer comprises two components: WebDialer servlet and Redirector servlet.

The Redirector servlet provides the ability for third-party applications to use Cisco WebDialer. The Redirector servlet finds the appropriate Cisco Unified CallManager cluster for the WebDialer user and redirects the request to the WebDialer in that cluster. The Redirector functionality only applies for HTTP/HTML-based WebDialer client applications because it is not available for Simple Object Access Protocol (SOAP)-based WebDialer applications.

CDR Services

Cisco SOAP - CDRonDemand Service

The Cisco SOAP - CDRonDemand Service, which is a SOAP/HTTPS-based service, runs on the CDR Repository node, which is the first node. It receives SOAP requests for CDR file name lists based on a user-specified time interval (up to a maximum of one hour) and returns a list of file names that fit the

time duration that is specified in the request. This service also receives requests for delivery of a specific CDR/CMR file with the file name and the transfer method (sftp/ftp, server name, login info, directory) that is specified in the request.

If you are using a third-party billing application that accesses CDR data via an HTTPS/SOAP interface, activate this service.

Cisco CAR Scheduler

The Cisco CAR Scheduler service allows you to schedule CAR-related tasks; for example, you can schedule report generation or CDR file loading into the CAR database.

Cisco CAR Web Service

The Cisco CAR Web Service loads the user interface for CAR, a web-based reporting application that generates either csv or pdf reports by using CDR data.

Database and Admin Services

Cisco AXL Web Service

The Cisco AXL Web Service allows you to modify Cisco Unified CallManager database entries and execute stored procedures from client-based applications that use AXL.

Cisco Bulk Provisioning Service

You can activate the Cisco Bulk Provisioning Service only on the first node. If you use the Cisco Unified Bulk Administration Tool (BAT) to administer phones and users, you must activate this service.

Cisco TAPS Service

The Cisco TAPS Service supports the Cisco Unified CallManager Auto-Registered Phone Tool, which allows a user to upload a customized configuration on an autoregistered phone after a user responds to Interactive Voice Response (IVR) prompts.

You activate this service on the first node; when you want to create dummy MAC addresses for the tool, ensure that the Cisco Bulk Provisioning Service is activated on the same node.



The Cisco Unified CallManager Auto-Register Phone Tool relies on Cisco Customer Response Solutions (CRS). Before the tool can work as designed, verify that the CRS server is configured and running, as described in the CRS documentation.

Performance and Monitoring Services

Cisco Serviceability Reporter

The Cisco Serviceability Reporter service generates the following daily reports:

- Device Statistics
- Server Statistics
- Service Statistics
- Call Activities

- Alert
- Performance Protection Report

This service gets installed on all the Cisco Unified CallManager nodes in the cluster. Reporter generates reports once a day based on logged information. You can access the reports that Reporter generates in Cisco Unified CallManager Serviceability from the Tools menu.

Each summary report comprises different charts that display the statistics for that particular report.

Cisco Serviceability Reporter comprises two service parameters:

- Report Generation Time—Number of minutes after midnight. Reports generate at this time for the last day.
- Report Deletion Age—Number of days that the report must be kept in the disk. The system deletes the reports that are older than the specified age.

Cisco CCM SNMP Service

This service provides SNMP access to provisioning and statistics information that is available for Cisco Unified CallManager.

Security Services

Cisco CTL Provider

The Cisco CTL Provider service, which runs with local system account privileges, works with the Cisco CTL Provider Utility, a client-side plug-in, to change the security mode for the cluster from nonsecure to mixed mode. When you install the plug-in, the Cisco CTL Provider service retrieves a list of all Cisco Unified CallManager and Cisco TFTP servers in the cluster for the CTL file, which contains a list of security tokens and servers in the cluster.

After you activate the service, the Cisco CTL Provider service reverts to the default CTL port, which is 2444. If you want to change the port, refer to the Cisco Unified CallManager security documentation for more information. You must install and configure the Cisco CTL Client and activate this service for the clusterwide security mode to change from nonsecure to secure.

Cisco Certificate Authority Proxy Function (CAPF)

Working in conjunction with the CAPF application, the Cisco Certificate Authority Proxy Function (CAPF) service can perform the following tasks, depending on your configuration:

- Issue locally significant certificates to supported Cisco Unified IP Phone models.
- Using SCEP, request certificates from third-party certificate authorities on behalf of supported Cisco Unified IP Phone models.
- Upgrade existing certificates on the phones.
- Retrieve phone certificates for troubleshooting.
- Delete locally significant certificates on the phone.



Note

When you view real-time information in RTMT, the Cisco Certificate Authority Proxy Function (CAPF) service displays only for the first node.

Directory Services

Cisco DirSync

Unlike Windows versions of Cisco Unified CallManager, Cisco Unified CallManager 5.1 does not contain an embedded directory. Because of this change, the Cisco Unified CallManager database stores all user information. If you use an integrated corporate directory, for example, Microsoft Active Directory or Netscape/iPlanet Directory, with Cisco Unified CallManager, the Cisco DirSync service migrates the user data to the Cisco Unified CallManager database. The Cisco DirSync service does not synchronize the passwords from the corporate directory.

Network Services

Installed automatically with Cisco Unified CallManager, network services include services that the Cisco Unified CallManager system requires for the cluster to function; for example, database and platform services. Because these services are required for basic Cisco Unified CallManager functionality, you cannot activate them in the Service Activation window. If necessary, for example, for troubleshooting purposes, you may need to stop and start (or restart) a network service in the Call Control—Network Services window.

After the Cisco Unified CallManager installation, network services start automatically, as noted in the Call Control—Network Services window.

In the Control Center—Network Services window, Cisco Unified CallManager Serviceability categorizes services into the following groups:

- [Platform Services, page 19-7](#)
- [DB Services, page 19-8](#)
- [CCM Services, page 19-9](#)
- [Performance and Monitoring Services, page 19-10](#)
- [Service Activation, page 19-11](#)
- [SOAP Services, page 19-10](#)
- [Backup and Restore Services, page 19-11](#)
- [CDR Services, page 19-11](#)

Platform Services

A Cisco DB

A Cisco DB is the Progress database engine.

A Cisco DB Replicator

The A Cisco DB Replicator service ensures database configuration and data synchronization between the first and subsequent nodes in the cluster.

Cisco Tomcat

The Cisco Tomcat service supports the web server in Cisco Unified CallManager 5.1.

SNMP Master Agent

This service, which acts as the agent protocol engine, provides authentication, authorization, access control, and privacy functions that relate to SNMP requests.

MIB2 Agent

This service provides SNMP access to variables that are defined in RFC 1213, which read and write variables; for example, system, interfaces, IP, and so on.

Host Resources Agent

This service provides SNMP access to host information, such as storage resources, process tables, device information, and installed software base.

Native Agent Adaptor

This service allows you to forward SNMP requests to another SNMP agent that runs on the system.

System Application Agent

This service provides SNMP access to the applications that are installed and executing on the system. This implements the SYSAPPL-MIB.

Cisco CDP Agent

This service uses the Cisco Discovery Protocol to provide SNMP access to network connectivity information on the Cisco Unified CallManager node.

Cisco Syslog Agent

This service supports gathering of syslog messages that various Cisco Unified CallManager components generate.

Cisco Electronic Notification

This service works with the Cisco Unified Communications Platform Administration, so you can send e-mails about software updates.

Cisco License Manager

Cisco License Manager keeps track of the licenses that a customer purchases and uses. It controls licenses checkins and checkouts, and it takes responsibility for issuing and reclaiming licenses. Cisco License Manager manages the Cisco Unified CallManager application and the number of IP phone unit licenses. When the number of phones exceeds the number of licenses, it issues alarms to notify the administrator. This service runs on all the nodes, but the service on the first node has the responsibility for issuing and reclaiming licenses.

Cisco Certificate Expiry Monitor

This service periodically checks the expiration status of certificates that Cisco Unified CallManager generates and sends notification when a certificate gets close to its expiration date.

DB Services

Cisco Database Layer Monitor

The Cisco Database Layer Monitor service monitors aspects of the database layer. This server takes responsibility for change notification and monitoring.

CCM Services

Cisco CallManager Admin

The Cisco CallManager Admin service supports Cisco Unified CallManager Administration, the web application/interface that you use to configure Cisco Unified CallManager settings. After the Cisco Unified CallManager installation, this service starts automatically and allows you access to the web pages. If you stop this service on a server, you cannot access the Cisco Unified CallManager Administration graphical user interface when you browse into that server.

Cisco CallManager Serviceability

The Cisco CallManager Serviceability service supports Cisco Unified CallManager Serviceability, the web application/interface that you use to troubleshoot Cisco Unified CallManager issues. After the Cisco Unified CallManager installation, this service starts automatically and allows you access to the web pages. If you stop this service on a server, you cannot access the Cisco Unified CallManager Serviceability GUI when you browse into that server.

Cisco CallManager Personal Directory

The Cisco CallManager Personal Directory service supports Cisco Personal Directory.

Cisco Log Partition Monitoring Tool

The Cisco Log Partition Monitoring Tool service supports the Log Partition Monitoring feature, which monitors the disk usage of the log partition on a server (or all servers in the cluster) by using configured thresholds and a polling interval.

Cisco CDP

Cisco CDP advertises Cisco Unified CallManager to other applications, so the application, for example, SNMP or CiscoWorks2000, can perform network management tasks for Cisco Unified CallManager.

Cisco Trace Collection Servlet

The Cisco Trace Collection Servlet, along with the Cisco Trace Collection Service, supports trace collection and allows users to view traces by using the RTMT client. After Cisco Unified CallManager installation, this service starts automatically. If you stop this service on a server, you cannot collect or view traces on that server.

Cisco Trace Collection Service

The Cisco Trace Collection Service, along with the Cisco Trace Collection Servlet, supports trace collection and allows users to view traces by using the RTMT client. After Cisco Unified CallManager installation, this service starts automatically. If you stop this service on a server, you cannot collect or view traces on that server.



If necessary, Cisco recommends that, to reduce the initialization time, you restart the Cisco Trace Collection Service before restarting Cisco Trace Collection Servlet.

Cisco RIS Data Collector

The Real-time Information Server (RIS) maintains real-time Cisco Unified CallManager information such as device registration status, performance counter statistics, critical alarms generated, and so on. The Cisco RIS Data Collector service provides an interface for applications, such as Real-Time Monitoring Tool (RTMT), SOAP applications, Cisco Unified CallManager Administration and AlertMgrCollector (AMC) to retrieve the information that is stored in all RIS nodes in the cluster.

Cisco AMC Service

Used for the real-time monitoring tool (RTMT), this service, Alert Manager and Collector service, existed as a component of the Cisco RIS Data Collector service in previous Windows releases of Cisco Unified CallManager. This service allows RTMT to retrieve real-time information that exists on nodes in the cluster.

Cisco Extension Mobility Application

The Cisco Extension Mobility service allows you to define login settings such as duration limits on phone configuration for the Cisco Extension Mobility feature. The Cisco Extension Mobility feature allows users within a Cisco Unified CallManager cluster to temporarily configure any Cisco Unified IP Phone 7960/7940 in the cluster as their own phone by logging in to that phone. After a user logs in, the phone adopts the personal phone number(s), speed dials, services links, and other user-specific properties of the user. After logout, the phone adopts the original user profile.

Performance and Monitoring Services

Cisco CallManager Serviceability RTMT

The Cisco CallManager Serviceability RTMT service supports the Cisco Unified CallManager Real-Time Monitoring Tool (RTMT), which allows you to collect and view traces, view performance monitoring objects, work with alerts, and monitor devices, system performance, CTI applications, and so on.

Cisco RTMT Reporter Servlet

The Cisco RTMT Reporter servlet allows you to publish reports for RTMT.

Cisco Tomcat Stats Servlet.

The Cisco Tomcat Stats Servlet allows you to monitor the Tomcat perfmon counters by using RTMT or the Command Line Interface. Do not stop this service unless you suspect that this service is using too many resources, such as CPU time.

SOAP Services

Cisco SOAP-Real-Time Service APIs

The Cisco SOAP-Real-Time Service APIs allow you to collect real-time information for devices and CTI applications. This service also provides APIs for activating, starting, and stopping services.

Cisco SOAP Performance Monitoring APIs

The Cisco SOAP Performance Monitoring APIs service allows you to use performance monitoring counters for various applications through SOAP APIs; for example, you can monitor memory information per service, CPU usage, Cisco Callmanager counters, and so on.

Cisco SOAP-Log Collection APIs

The Cisco SOAP-Log Collection APIs service allows you to collect log files and to schedule collection of log files on a remote SFTP server. Examples of log files that you can collect include syslog, core dump files, Cisco application trace files, and so on.

Backup and Restore Services

Cisco DRF Master

The Cisco DRF Master Agent service supports the DRF Master Agent, which works with the graphical user interface (GUI) or command line interface (CLI) to schedule backups, perform restorations, view dependencies, check status of jobs, and cancel jobs, if necessary. The Cisco DRF Master Agent also provides the storage medium for the backup and restoration process (tape drive in Cisco Unified CallManager 5.1).

Cisco DRF Local

The Cisco DRF Local service supports the Cisco DRF Local Agent, which acts as the workhorse for the DRF Master Agent. Components on a node register with the Cisco DRF Local Agent to use the disaster recovery framework. The Cisco DRF Local Agent executes commands that it receives from the Cisco DRF Master Agent. Cisco DRF Local Agent sends the status, logs, and command results to the Cisco DRF Master Agent.

CDR Services

Cisco CDR Repository Manager

You can start and stop the Cisco CDR Repository Manager service only on the first node, which contains the Cisco Unified CallManager database. This service starts automatically.

Cisco CDR Agent

The Cisco CDR Agent service transfers CDR and CMR files that are generated by Cisco Unified CallManager from the local host to the CDR repository node, where the CDR Repository Manager service runs over a SFTP connection.

For this service to work, activate the Cisco CallManager service on the first node and ensure that it is running.

Service Activation

You can activate or deactivate multiple feature services or choose default services to activate from the Service Activation window in Cisco Unified CallManager Serviceability. Cisco Unified CallManager Serviceability activates feature services in automatic mode and checks for service dependencies based on a single-server configuration. When you choose to activate a feature service, Cisco Unified CallManager Serviceability prompts you to select all the other services, if any, that depend on that service to run based on a single-server configuration. When you click the Set Default button, Cisco Unified CallManager Serviceability chooses those services that are required to run Cisco Unified CallManager based on a single-server configuration. Activating a service automatically starts the service. You start/stop services from Control Center.

Control Center

From Control Center in Cisco Unified CallManager Serviceability, you can view status and start and stop one service at a time for a particular server in the cluster. To perform these tasks, Cisco Unified CallManager Serviceability provides two Control Center windows. To start, stop, and restart network services, access the Control Center—Network Services window. To start, stop, and restart feature services, access the Control Center—Feature Services window.

**Tip**

Use the Related Links drop-down list box and the Go button to navigate to Control Center and Service Activation windows.

Starting and stopping a Cisco CallManager (feature) service causes all Cisco Unified IP Phones and gateways that are currently registered to that Cisco CallManager service to fail over to their secondary Cisco CallManager service. Devices and phones need to restart only if they cannot register with another Cisco CallManager service. Starting and stopping a Cisco CallManager service causes other installed applications (such as Conference Bridge or Cisco Messaging Interface) that are homed to that Cisco CallManager to start and stop as well.

**Caution**

Stopping a Cisco CallManager service also stops call processing for all devices that the service controls. When a Cisco CallManager service is stopped, calls from an IP phone to another IP phone will stay up; calls in progress from an IP phone to a Media Gateway Control Protocol (MGCP) gateway also stay up, but other types of calls drop.

Services Configuration Checklist

Table 19-1 lists the steps for installing and configuring services.

Table 19-1 **Services Configuration Checklist**

Configuration Steps		Procedures and Related Topics
Step 1	Activate the feature services that you want to run on your Cisco Unified CallManager servers. Note If you are upgrading from a previous version of Cisco Unified CallManager, Cisco Unified CallManager Serviceability automatically activates and starts the services that were started before you began the upgrade.	• Feature Services, page 19-1 • Activating and Deactivating Feature Services, Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)
Step 2	Configure the appropriate service parameters.	• <i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i> • ?-button help in Service Parameter window in Cisco Unified CallManager Administration
Step 3	Troubleshoot problems by using the Cisco Unified CallManager Serviceability trace tools, if needed.	• Trace Configuration, <i>Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)</i> • Trace Collection and Log Central in RTMT, <i>Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)</i>

Where to Find More Information

Related Topics

- [Control Center, page 19-12](#)
- [Feature Services, page 19-1](#)
- [Network Services, page 19-7](#)

Additional Cisco Documentation

- *Cisco Unified CallManager System Guide, Release 5.0(4)*
- *Cisco Unified CallManager Administration Guide, Release 5.0(4)*
- *Cisco Unified CallManager Features and Services Guide, Release 5.0(4)*
- *Cisco Unified CallManager Security Guide, Release 5.0(4)*
- *Troubleshooting Guide for Cisco Unified CallManager, Release 5.0(4)*



Alarms

This chapter provides information on Serviceability Alarms and contains the following topics:

- [Understanding Alarms, page 20-1](#)
- [Alarm Configuration, page 20-2](#)
- [Alarm Definitions, page 20-2](#)
- [Viewing Alarm Information, page 20-2](#)
- [Alarm Configuration Checklist, page 20-3](#)
- [Where to Find More Information, page 20-4](#)

Understanding Alarms

Cisco Unified CallManager Serviceability Alarms allows you to configure alarms and events and provides alarm message definitions. Both functions assist the system administrator and support personnel in troubleshooting Cisco Unified CallManager problems.

You use alarms to provide run-time status and state of the Cisco Unified CallManager system and to take corrective action for problem resolution; for example, to determine whether phones are registered and working. Alarms contain information such as explanation and recommended action. Alarm information includes application name, machine name, and cluster name to help you perform troubleshooting, even for problems that are not on your local Cisco Unified CallManager.

You configure the alarm interface to send alarm information to multiple destinations, and each destination can have its own alarm event level (from debug to emergency). You can direct alarms to the Syslog Viewer (local syslog), Syslog file (remote syslog), an SDI trace log file, an SDL trace log file (for Cisco CallManager and CTIManager only), or to all destinations. When a service issues an alarm, the alarm interface sends the alarm to the chosen monitors (for example, SDI trace). The monitor forwards the alarm or writes it to its final destination (such as a log file).



Tip

For the Remote Syslog Server, do not specify the Cisco Unified CallManager node, which cannot accept syslog messages from other servers.

You use the trace and log central option in the Cisco Unified CallManager Real-Time Monitoring Tool (RTMT) to collect alarms that are sent to an SDI or SDL trace log file. You use the SysLog Viewer in the real-time monitoring tool to view alarms that are sent to the local syslog.

The alarm definitions describe alarm messages: what they mean and how to recover from them. You search the Alarm Definitions window for alarm information. When you click on any service-specific alarm, a description of the alarm information (including any user-defined text that you have added) and a recommended action display.

Alarm Configuration

You configure alarm information that will be used for trace and troubleshooting. You can configure alarms for services, such as Cisco CallManager and Cisco CTIManager, on a particular server, or you configure alarms for a particular service on all servers in the cluster.

You choose an alarm event level, such as Error, and a destination(s), such as Syslog Viewer (local syslog), for the alarms for an individual service and the monitor destination. Choosing an event level accomplishes two tasks: helps the administrator narrow the types of alarms that Cisco Unified CallManager collects and prevents the Syslog and trace files from becoming overloaded.

Alarm Definitions

Cisco Unified CallManager stores alarm definitions and recommended actions in a standard query language (SQL) server database. The system administrator can search the database for definitions of all the alarms. The definitions include the alarm name, description, explanation, recommended action, severity, parameters, and monitors. This information aids the administrator in troubleshooting problems that Cisco Unified CallManager encounters.

Serviceability Alarm Definitions allow administrators to add additional explanation or recommendations for an alarm. All administrators have access to the added information. Administrators directly enter information into the User Defined Text box that displays in the Alarm Details window. Standard horizontal and vertical scroll bars support scrolling. Cisco Unified CallManager Serviceability adds the information to the database.

Viewing Alarm Information

You view alarm information to determine whether Cisco Unified CallManager problems exist. The method that you use to view the alarm depends on the destination that you chose when you configured the alarm. You can view alarm information that is sent to the SDI or SDL trace log file by using the trace and log central option in RTMT or by using a text editor. You can view alarm information that is sent to local syslog by using the SysLog Viewer.

**Tip**

You can also use CiscoWorks2000 report viewer to view remote syslog messages.

Alarm Configuration Checklist

Table 20-1 provides an overview of the steps for configuring alarms.

Table 20-1 Alarm Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Choose the server and service for which you want the alarm information.	Understanding Alarms, page 20-1 Configuring or Updating an Alarm for a Service, Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)
Step 2	Choose the destination of the alarm. - All services can go to the SDI log (but must be configured in Trace also). - All services can go to the SysLog Viewer. - To send syslog messages to the Remote Syslog Server, check the Remote Syslog destination and specify a host name. - Only Cisco CallManager and Cisco CTIManager use the SDL log.	Configuring or Updating an Alarm for a Service, Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1) Alarm Destination Settings, Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)
Step 3	Choose the alarm event level.	Configuring or Updating an Alarm for a Service, Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1) Alarm Event Level Settings, Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)
Step 4	If desired, add a definition to an alarm.	Alarm Definitions, Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)
Step 5	If you chose an SDI or SDL trace file as the alarm destination, collect traces and view with the trace and log central option of RTMT.	Trace Collection and Log Central in RTMT, Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4) Using Local Browse, Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4) Using the Query Wizard, Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)
Step 6	If you chose local syslog as the alarm destination, view the alarms in the SysLog Viewer.	Using SysLog Viewer in RTMT, Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)
Step 7	See the corresponding alarm definition for the description and recommended action.	Viewing Alarm Definitions and Adding User-Defined Descriptions, Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)

Where to Find More Information

Related Topics

- [Alarm Event Level Settings](#), *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*
- Alarm Definition Catalog Descriptions, *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)*
- Trace Collection and Log Central in RTMT, *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)*



Trace

This chapter provides information on the Cisco Unified CallManager Serviceability trace tools and contains the following topics:

- [Understanding Trace, page 21-1](#)
- [Trace Configuration, page 21-2](#)
- [Troubleshooting Trace Setting, page 21-2](#)
- [Trace Collection, page 21-3](#)
- [Trace Configuration and Collection Checklist, page 21-4](#)
- [Where to Find More Information, page 21-5](#)

Understanding Trace

Cisco Unified CallManager Serviceability provides trace tools to assist the system administrator and support personnel in troubleshooting Cisco Unified CallManager problems. Cisco Unified CallManager Serviceability supports SDI (System Diagnostic Interface) trace, SDL (Signaling Distribution Layer) trace, and Log4J trace (for Java applications).

You use the Trace Configuration window to specify the level of information that you want traced as well the type of information that you want to trace to be included in each trace file. If the service is a call-processing application such as Cisco Unified CallManager or Cisco CTIManager, you can configure a trace on devices such as phones and gateway.

You use the Alarm Configuration window to direct various levels of alarms to destinations, including SDI or SDL trace log files.

After you have configured information that you want to include in the trace files for the various services, you can collect and view trace files by using the trace and log central option in the Cisco Unified CallManager Real-Time Monitoring Tool (RTMT).

Trace Configuration

You can configure trace parameters for any Cisco CallManager service that is available on any Cisco Unified CallManager server in the cluster. Use the Trace Configuration window to specify the parameters that you want to trace for troubleshooting Cisco Unified CallManager problems.

You can configure the level of information that you want traced (debug level), what information you want to trace (trace fields), and information about the trace files (such as number of files per service, size of file, and time that the data is stored in the trace files.) You can configure trace for a single service or apply the trace settings for that service to all servers in the cluster.

If the service is a call-processing application such as Cisco Unified CallManager or Cisco CTIManager, you can configure a trace on devices such as phones and gateways; for example, you can narrow the trace to all enabled phones with a directory number beginning with 555.

If you want to use predetermined troubleshooting trace settings rather than choosing your own trace fields, you can use the Troubleshooting Trace window. For more information on troubleshooting trace, see the [“Troubleshooting Trace Setting” section on page 21-2](#).

After you have configured information that you want to include in the trace files for the various services, you can collect trace files by using the trace and log central option in RTMT. For more information regarding trace collection, see the [“Trace Collection” section on page 21-3](#).

Troubleshooting Trace Setting

The Troubleshooting Trace Settings window allows you to choose the services in Cisco Unified CallManager for which you want to set predetermined troubleshooting trace settings. Using this window, you can choose the required services on different Cisco Unified CallManager nodes in the cluster, so the trace settings of the chosen services get changed to reflect the predetermined trace settings. You can choose specific activated services for a single node, all activated services for the node, specific activated services for all nodes in the cluster, or all activated services for all nodes in the cluster. In the window, N/A displays next to inactive services.

**Note**

The predetermined troubleshooting trace settings for a service include SDL, SDI, and Log4j trace settings. Before Cisco Unified CallManager applies the troubleshooting trace settings, the system backs up the original trace settings. When you reset the troubleshooting trace settings, the original trace settings get restored.

When you open the Troubleshooting Trace Settings window after you apply troubleshooting trace settings to a service, the service that you set for troubleshooting displays as checked. You can reset the trace settings to the original settings by choosing one of the Reset Troubleshooting Traces buttons.

When you apply Troubleshooting Trace Setting to a service, the Trace Configuration window displays a message that troubleshooting trace is set for the given service(s). From the Related Links drop-down list box, you can choose the Troubleshooting Trace Settings option if you want to reset the settings for the service. The Trace Configuration window displays all the settings as read-only, except for some parameters of trace output settings; for example, Maximum No. of Files. You can modify these parameters even after you apply troubleshooting trace settings.

Trace Collection

Use trace and log central, an option within the Cisco Unified CallManager Real-Time Monitoring Tool, to collect, view, and zip various Cisco Unified CallManager service traces and/or other Cisco Unified CallManager log files. With the trace and log central option, you can collect Cisco Unified CallManager SDL/SDI traces, Cisco Unified CallManager Application Logs (such as Bulk Administration Tool logs), System Logs (such as Event View Application, Security, and System logs), and crash dump files.

The trace and log central option provides several methods to collect and view trace files, as described in the following list:

- **Remote Browse**—After the system has generated trace files, allows you to view them on the server by using the viewers within the Cisco Unified CallManager Real-Time Monitoring Tool. You can also use the remote browse feature to download the traces to your PC.
- **Collect Files**—Collects and downloads traces for services, applications, and system logs on one or more servers in the cluster for an absolute date and time range (such as between July 8, 2004 at 12:30 and August 8, 2004 at 12:30) or for a relative time (such as, within the last 30 minutes).

For example, to collect CSA logs, check the Cisco Security Agent check box in the Select System Logs tab. To access user logs that provide information about users that are logging in and out, check the Security Logs check box in the Select System Logs tab.

- **Query Wizard**—Collects trace files for services, applications, and system logs, for an absolute or relative time range, that contain text strings that you specify. You can view the collected trace file and/or download the trace files to your PC. You can also save the trace collection query criteria for later use. If you save the query as a regular query, you can only run the query on the node on which it was created. If you save the query as a generic query, you can run it on any node in any cluster.
- **Schedule Collection**—Schedules a recurring trace collection and allows users to perform a specified action, including run another query, generate a syslog, or download the trace files on a SFTP server.
- **Local Browse**—After you have collected trace files and downloaded them to your PC, allows you to view them with a text editor that can handle UNIX variant line terminators such as WordPad on your PC, or you can view them by using the viewers within the Cisco Unified CallManager Real-Time Monitoring Tool.



Note Do not use NotePad to view collected trace files.

- **Collect Crash Dump**—Collects a crash dump file for one or more servers on your network.
- **Real Time Trace**—Comprises two options: view real-time data and monitor user events. The view real-time data option allows you to view the current trace file that is being written on the server for an application. The monitor user event option enables the system to monitor real-time trace files and perform a specified action when a search string displays in the trace file. Actions include generating an alert, generating local or remote syslogs, or downloading trace files via SFTP.
- **Job Status**—Allows you to view the status of the trace collection jobs that are running on the system as well as recently processed jobs.

After the system has generated trace files, you can view them on the server by using the remote browse option.

You can collect individual traces files or zip multiple traces into a single file. You can manually delete the collected trace files from the server, or you can set the trace and log central option to delete the trace files from the server after collection.

After you collect the files, you can view them in the Local Browse option. The file displays in the appropriate viewer, such as the QRT Viewer, Q931 Translator, Log Viewer, or Generic Viewer.

**Note**

For devices that support encryption, the SRTP keying material does not display in the trace file.

Trace Configuration and Collection Checklist

Table 21-1 provides an overview of the steps for configuring and collecting trace for Cisco Unified CallManager services.

Table 21-1 Trace Configuration and Collection Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Choose System > Enterprise Parameters in Cisco Unified CallManager Administration and configure the maximum number of devices that are available for tracing. Enter a value in the Max Number of Device Level Trace field. The default specifies 12.	<i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 2	Configure the trace setting for the service for which you want to collect traces. You can configure trace for the service on one server or on all servers in the cluster. To configure trace settings, choose what information you want to include in the trace log by choosing the debug level and trace fields. You can also configure trace for specific devices if you are configuring trace for the Cisco CallManager service or the Cisco CTIManager service. If you want to run predetermined traces on services, set troubleshooting trace for those services.	Trace Configuration, <i>Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)</i> Troubleshooting Trace Setting Configuration , <i>Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)</i>
Step 3	Install the Cisco Unified CallManager Real-Time Monitoring Tool on a local PC.	Real-Time Monitoring Configuration , <i>Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)</i>
Step 4	If you want to generate an alarm when the specified search string exists in a monitored trace file, enable the TraceCollectionToolEvent alert.	Setting Alert Properties, <i>Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)</i>
Step 5	If you want to automatically capture traces for alerts such as CriticalServiceDownand CodeYellow, check the Enable TCT Download check box in Set Alert/Properties dialog box for the alerts.	Setting Alert Properties, <i>Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)</i>
Step 6	Collect Cisco Unified CallManager traces, applications, and system traces within the Cisco Unified CallManager cluster.	Trace Collection and Log Central in RTMT, <i>Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)</i>

Table 21-1 Trace Configuration and Collection Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 7	View the log file in the appropriate viewer.	Using Local Browse, <i>Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)</i> Using the Query Wizard, <i>Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)</i> Using Q931 Translator, <i>Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)</i> Displaying QRT Report Information, <i>Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)</i>
Step 8	If you enabled troubleshooting trace, reset the trace settings services on the Cisco Unified CallManager nodes, so the original settings get restored. Note Leaving Troubleshooting trace enabled for a long time increases the size of the trace files and may impact the performance of the services.	Troubleshooting Trace Setting Configuration , <i>Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)</i>

Where to Find More Information

Related Topics

- Alarm Configuration, *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)*
- Trace Configuration, *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)*
- Trace Collection and Log Central in RTMT, *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)*
- Setting Alert Properties, *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)*
- Using Q931 Translator, *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)*
- [Troubleshooting Trace Setting Configuration](#), *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*



Real-Time Monitoring Tool

This chapter contains information on the following topics:

- [Understanding the Real-Time Monitoring Tool, page 22-1](#)
- [RTMT Components, page 22-3](#)
- [RTMT Services, Servlets and Service Parameters, page 22-4](#)
- [RTMT Collector, Alert Manager, and RTMT Reporter, page 22-4](#)
- [Viewing a Summary, page 22-6](#)
- [Monitoring Server Status, page 22-6](#)
- [Understanding Server Logs, page 22-7](#)
- [Monitoring Call-Processing Activity, page 22-7](#)
- [Understanding Call-Processing Logs, page 22-9](#)
- [Monitoring Services, page 22-10](#)
- [Understanding Service Logs, page 22-11](#)
- [Monitoring Devices, page 22-11](#)
- [Understanding Device Logs, page 22-13](#)
- [Monitoring CTI Applications, Devices, and Lines, page 22-13](#)
- [Where to Find More Information, page 22-13](#)

Understanding the Real-Time Monitoring Tool

Real-Time Monitoring Tool, which runs as a client-side application, uses HTTPS and TCP to monitor device status, system performance, device discovery, and CTI applications in the Cisco Unified CallManager cluster. The tool also connects directly to devices via HTTPS to troubleshoot system problems.



Note

Even when RTMT does not run, tasks such as alarm and performance monitoring updates occur in the background.

RTMT allows you to perform the following tasks:

- Monitor a set of management objects that are preconfigured
- Generate various alerts, in the form of e-mails, for objects when values go over/below user-configured thresholds
- Collect and view traces in various default viewers that exist in RTMT
- Translate Q931 messages
- View syslog messages in SysLog Viewer
- Work with performance-monitoring counters

You can install RTMT, which works for resolutions 800*600 and above, on a Windows 98, Windows XP, Windows 2000, or Red Hat Linux with KDE and/or Gnome client. To avoid CPU spiking while you collect and zip files, do not install RTMT on a server where you installed Cisco Unified CallManager. For information on how to install and launch RTMT, see the following sections:

- [Installing the Real-Time Monitoring Tool \(RTMT\), page 18-1](#)
- [Using RTMT, page 18-3](#)

To connect to any node in the Cisco Unified CallManager cluster, you must enter the CCM Administrator application user authentication information in the User Name and Password fields when you launch the tool. Likewise, you must enter either the IP address or host name of the first node. If the authentication fails for any reason, the tool prompts you to reenter the server and authentication details. After the authentication succeeds, RTMT launches the monitoring module from local cache or from a remote node when the local cache does not contain a monitoring module that matches the backend version.

After you initially load RTMT, the load includes a default configuration that is called CM-Default. The first time that you use RTMT, it will use the CM-Default profile and display the summary page in the monitor pane. CM-Default dynamically monitors all registered phones for all Cisco Unified CallManager nodes. If your cluster contains five configured Cisco Unified CallManager nodes, CM-Default displays the registered phones for each node in a Cisco Unified CallManager cluster, as well as calls in progress and active gateway ports and channels.

You can configure RTMT to display the information that interests you, such as different performance counters for different features, in the monitor pane of RTMT and save the framework of your configuration in a profile. You can then restore the profile at a later time during the same session or the next time that you log in to RTMT. By creating multiple profiles, so each profile displays unique information, you can quickly display different information by switching profiles.

You save, restore, and delete Cisco Unified CallManager configuration information by using Profile in the System menu, as described in [“Working with Configuration Profiles” section on page 18-5](#).

RTMT generates daily reports in PDF format for precanned objects, as described in the [“RTMT Collector, Alert Manager, and RTMT Reporter” section on page 22-4](#).

RTMT arranges the preconfigured monitoring objects into the following major categories:

- Summary
- Server
- Call Process
- Service
- Device

- CTI
- Performance

RTMT Components

The RTMT window comprises the following main components:

- Menu Bar, which includes the following menu options:
 - System—Allows you to save, restore, and delete existing RTMT profiles, monitor Java Heap Memory Usage, go to the Serviceability Report Archive window in Cisco Unified CallManager Serviceability, log off or exit RTMT.
 - Monitor—Allows you to monitor precanned objects.
 - Search—Allows you to search for devices, such as phones and H.323 devices, and for CTI applications, devices, and lines to monitor.
 - Edit—Allows you to configure categories (for table format view), set the polling rate for devices and performance monitoring counters, hide the quick launch channel, and edit the trace setting for RTMT.
 - Devices—Allows you to search for devices and to view phone information, port/channel status, and so on.
 - Performance—Allows you to work with performance monitoring counters.
 - Tools—Allows you to work with alerts, collect traces, and view syslog messages.
 - Window—Allows you to close a single RTMT window or all RTMT windows.
 - Application—Allows you to browse to Cisco Unified CallManager Administration or Cisco Unified CallManager Serviceability
 - Help—Allows you to access RTMT documentation online help or to view the RTMT version.
- Quick Launch Channel—Pane on the left side of RTMT window that displays icons that you can click to monitor various objects.
- View/Tool tabs—Allows you to display preconfigured categories in the Quick Launch Channel; Tool tab displays alert, trace, and syslog viewer categories.

The View and Tools tabs differ in that anything related to the View tab gets saved as a profile that can be restored at any time that RTMT is invoked. The Tools tab relates only to the systemwide alert functionality. You cannot save the states.

- Monitor pane—Pane where monitoring results display.

RTMT Services, Servlets and Service Parameters

RTMT uses the following services/servlets:

- AMC service—This service starts up automatically after the installation and allows RTMT to retrieve real-time information that exists on nodes in the cluster.

The following list comprises some AMC service parameters that are associated with RTMT. For the latest list of parameters, choose **System > Service Parameters** in Cisco Unified CallManager Administration. Then, choose the server and the AMC service.

- Primary Collector
- Failover Collector
- Data Collection Enabled
- Data Collection Polling Rate
- Data Collection Reenumeration Interval
- RIS Client Timeout
- Server Synchronization Period
- RMI Port Number
- Alert Manager Enabled
- Logger Enabled
- Alarm Enabled
- PerfMon Log Deletion Age

For information on these service parameters, click the ? button that displays in the Service Parameter window of Cisco Unified CallManager Administration.

- Cisco CallManager Serviceability RTMT service (in the Control Center—Network Services window)—Supporting the Cisco Unified CallManager Real-Time Monitoring Tool (RTMT), this service installs with Cisco Unified CallManager and starts up automatically after the installation.
- Cisco RTMT Reporter servlet (in the Control Center—Network Services window)—This service, which installs with Cisco Unified CallManager and starts up automatically after the installation, allows you to publish reports for RTMT.

RTMT Collector, Alert Manager, and RTMT Reporter

RTMT Collector, a component that automatically gets installed with Cisco Unified CallManager, logs preconfigured monitoring objects information while Alert Manager, also automatically installed, logs alert histories into log files. Each preconfigured object belongs to one of several categories: devices, services, servers, call activities, and PPR. Each category has a separate log file, and alert details get logged in a separate file. Also, a separate log file exists to log important perfmon object values for Cisco CallManager-related services and processes.



Tip

Although they require no configuration tasks to run, RTMT Collector and Alert Manager support redundancy. If the primary collector or manager fails for any reason, the secondary collector and manager perform the tasks until primary support becomes available. RTMT Collector, Alert Manager, and RTMT Reporter run on the first node to minimize call-processing interruptions.

The locally written log files appear in the primary collector server at `cm/log/amc`. Because the primary collector changes because of failover and fallback scenarios, the log files can exist on more than one server in the Cisco Unified CallManager cluster.

You can display log files, except an alert log file, by using the Performance log viewer in RTMT or by using the native Microsoft Performance viewer. For more information on using the Performance log viewer in RTMT, refer to “Displaying Log Files on the Perfmon Log Viewer” in the *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)*. You can view an alert log file by using any text editor.

To download log files to a local machine, you can use the collect files option in Trace and Log Central in RTMT. For more information on downloading log files by using the collect files option, refer to “Trace Collection and Log Central in RTMT” in the *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)*.

Alternatively, from the command line interface (CLI), you can use the file list command to display a list of files and the file get command to download files by SFTP. For more information on using CLI commands, refer to the *Cisco Unified Communications Operating System Administration Guide, Release 5.0(4)*.

Log files exist in csv format. New log files get created every day at 00:00 hours on the local system. New logs for devices, services, servers, and calls get created when the time zone changes, when a new node is added to the cluster, or during failover/fallback scenarios. The first column of all these logs comprises the time zone information and the number of minutes from the Greenwich Meridian Time (GMT). RTMT Reporter uses these log files as a data source to generate daily summary reports. The report, which is based on the default monitoring objects, generates every 24 hours for the following information:

- Call Activity Status—Number of call attempted and number of calls completed for each Cisco Unified CallManager, each gateway, trunk, and overall cluster. Number of channels available, in-service for each gateway.
- Device Status—Number of registered phones, gateways and trunks per each server and overall cluster.
- Server Status—% CPU load, % memory used, % disk space used per server.
- Service Status —For each CTI Manager, number of opened devices and lines. For each TFTP server, number attempted and failed requests.
- Alert Status—Number of alerts per server. Number of alert per severity level for the cluster, including the top 10 alerts in the cluster.
- Performance Protection Report—Trend analysis information on default monitoring objects that allows you to track overall system health. The report includes information for the for the last 7 days for each server.

**Tip**

The RTMT reports display in English only.

The following service parameters apply to RTMT report generation: RTMT Reporter Designated Node, RTMT Report Generation Time, and RTMT Report Deletion Age. For information on these parameters, click the ? button that displays in the Service Parameter window in Cisco Unified CallManager Administration.

For more information on the Serviceability reports, see the “Serviceability Reports Archive” in the *Cisco Unified CallManager Serviceability System Guide, Release 5.0(4)*.

Viewing a Summary

The Summary option in RTMT allows you to monitor important common information in a single monitoring pane. In a summary, you can monitor the following information:

- Virtual Memory usage
- CPU usage
- Registered phones
- Calls in progress
- Active gateway ports and channels

Monitoring Server Status

The Servers category monitors CPU and memory usage, processes, disk space usage, and critical services on each Cisco Unified CallManager server.

The CPU and Memory monitor provide information about the CPU usage and Virtual memory usage on each Cisco Unified CallManager server. For each CPU, the information includes the percentage of time that each processor spends executing processes in different modes and operations (User, Nice, System, Idle, IRQ, SoftIRQ, and IOWait). The percentage of CPU equals the total time spent executing in all the different modes and operations excluding the Idle time. For memory, the information includes the Total, Used, Free, Shared, Buffers, Cached, Total Swap, Used Swap, and Free Swap memory in Kbytes, and the percentage of Virtual Memory in Use.

The Processes monitor provide information about the processes that are running on the system. These processes include the process, process ID (PID), CPU percentage, Status, Shared Memory (KB), Nice (level), VmRSS (KB), VmSize (KB), VmData (KB), Thread Count, Page Fault Count, and Data Stack Size (KB).

The Critical Services monitoring category provides the name of the critical service, the status (whether the service is up, down, or activated), and the elapsed time during which the services have existed in a particular status for a particular Cisco Unified CallManager node.

[Table 22-1](#) provides information about the objects that RTMT monitors, the alert, thresholds, and defaults. For information on daily CPU, memory, and disk usage reports, see the “Server Statistics Report” in the *Cisco Unified CallManager Serviceability System Guide, Release 5.0(4)*.

Table 22-1 Servers Category

Monitored Objects (displayed)	Alert/Threshold/Default
• CPU Usage (100% Idle) on each server • Virtual Memory Usage (% memory in use out of total) on each server • CPU and memory usage for all processes on each server	• Call Processing node - CPU usage pegged X% over X seconds. Default specifies 90%, 30 seconds. • Non-CallProcessing node - CPU Usage pegged X% over X seconds. Default specifies 99%, 120 seconds. • Available memory equals less than X%. Default specifies 10%. • When CPU peg or excessive memory usage alerts occur, the name of the top process displays in the alert message. In case of dllhost service, the real meaningful name displays instead of generic name dllhost.
Disk space usage for all logical drives on each server	Available disk space on the largest logical drive equals less than X%. Default specifies 10%.
State of activated critical services on each server	Service state changed from Up->Down.

Understanding Server Logs

Every 5 minutes, the server data gets logged into the file as a single record. The system logs the data every 5 minutes for the following counters, based on the following calculation:

- **cpuUsage**—Average of all the values that were collected in the last 5 minutes
- **MemoryInUse**—Average of all the values that were collected in the last 5 minutes
- **DiskSpaceInUse**—Average of all the values that were collected in the last 5 minutes for the active partition

The AMC service logs the server data in csv format. The header of the log comprises the time zone information and a set of columns with the previous counters for a Cisco Unified CallManager node. These sets of columns repeat for every node.

The following file name format of the server log applies: `ServerLog_MM_DD_YYYY_hh_mm.csv`. The first line of each log file comprises the header.

To download the server logs for viewing on your local computer, refer to “Trace Collection and Log Central in RTMT” in the *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)*.

Monitoring Call-Processing Activity

The Call Process monitoring category monitors the following items:

- **Call Activity**—You can monitor the number of calls that were attempted, calls that were completed, and call in progress for a particular Cisco Unified CallManager node or the entire cluster.

- **Gateway Activity**—You can monitor gateway activity for each gateway type. Gateway activity monitoring includes the number of active ports, the number of ports in service, and the number of calls that were completed for each gateway type for a particular Cisco Unified CallManager node or the entire cluster.
- **Trunk Activity**—The system monitors trunk activity by trunk type for a particular node or cluster. Trunk activity monitoring includes the number of calls in progress and the number of calls that were completed for a particular trunk type.
- **SDL Queue**—SDL queue monitoring monitors the number of signals in the SDL queue and the number of signals that were processed for a particular signal distribution layer (SDL) queue type. The SDL queue types comprise high, normal, low, and lowest queue. You can monitor the SDL queue for a particular node or the entire cluster.
- **SIP Activity**—The system displays a summary of SIP requests, SIP responses, total number of failed incoming responses (4xx, 5xx, and 6xx), total number of failed outgoing responses (4xx, 5xx, and 6xx), number of retry requests, and number of retry responses.

Table 22-3 provides information about the objects that RTMT monitors, the alert, thresholds, and defaults. For information on Cisco Unified CallManager call activity daily reports, see the “Call Activities Report” in the *Cisco Unified CallManager Serviceability System Guide, Release 5.0(4)*.

Table 22-2 Call Activities Category

Monitored Objects (displayed)	Alert/Threshold/Default
CallsAttempted, CallsCompleted, and CallsInProgress for each Cisco Unified CallManager node and cluster.	N/A
CallsAttempted, CallsCompleted, and CallsInProgress of each type of MGCP FXS/FXO/PRI/T1CAS/H.323 gateway, as well as SIP and H.323 Trunks for each Cisco Unified CallManager node and cluster.	N/A
Channel/Port Status of each MGCP FXS/FXO/PRI/T1CAS gateway.	N/A
SDL Queue activity on each Cisco Unified CallManager node.	N/A
MGCP FXS Gateway - Number of In-Service and Active ports for each Cisco Unified CallManager node and cluster.	Route-List exhausted
MGCP FXO Gateway - Number of In-Service and Active ports for each Cisco Unified CallManager node and cluster.	Route-List exhausted

Table 22-2 *Call Activities Category (continued)*

Monitored Objects (displayed)	Alert/Threshold/Default
MGCP PRI Gateway - Number of In-Service and Active channels for each Cisco Unified CallManager node and cluster.	• D-Channel out of service • Route List exhausted
MGCP T1CAS Gateway - Number of In-Service and Active ports for each Cisco Unified CallManager node and cluster.	Route List exhausted

Understanding Call-Processing Logs

The system accumulates call-processing data in the memory whenever RTMT calls the LogCall API. Every 5 minutes, RTMT logs the data into the file as a single record and cleans the memory.

The system logs data every 5 minutes for the following counters on the basis of the following calculation:

- cmCallsAttempted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- cmCallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- cmCallsInProgress—Average of all the values that were collected in last 5 minutes
- gwMGCP_FXS_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwMGCP_FXO_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwMGCP_PRI_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwMGCP_T1_CAS_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwH323_CallsAttempted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwH323_CallsInProgress—Average of all the values that were collected in last 5 minutes
- gwH323_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- trunkH323_CallsAttempted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- trunkH323_CallsInProgress—Average of all the values collected in last 5 minutes
- trunkH323_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- trunkSIP_CallsAttempted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- trunkSIP_CallsInProgress—Average of all the values that were collected in last 5 minutes

- trunkSIP_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwMGCP_FXS_PortsInService—Average of all the values that were collected in last 5 minutes
- gwMGCP_FXO_PortsInService—Average of all the values that were collected in last 5 minutes
- gwMGCP_PRI_SpansInService—Average of all the values that were collected in last 5 minutes
- gwMGCP_T1_CAS_SpansInService—Average of all the values that were collected in last 5 minutes
- gwMGCP_FXS_ActivePorts—Average of all the values that were collected in last 5 minutes
- gwMGCP_FXO_ActivePorts—Average of all the values that were collected in last 5 minutes
- gwMGCP_PRI_ActiveChannels—Average of all the values that were collected in last 5 minutes
- gwMGCP_T1_CAS_ActiveChannels—Average of all the values that were collected in last 5 minutes

The AMC service logs the call data in windows Performance tool-compatible csv format. The header of the log comprises the time zone information and a set of columns with the previously listed counters for a node. These sets of columns repeat for every node.

The following file name format of the Call Log applies: CallLog_MM_DD_YYYY_hh_mm.csv.

The first line of each log file comprises the header.

Monitoring Services

The Service monitoring category monitors the activities of Cisco TFTP requests, heartbeat of different nodes, and database activities.

The Cisco TFTP service builds and serves files that are consistent with the trivial file transfer protocol, which is a simplified version of the File Transfer Protocol (FTP). Cisco TFTP builds configuration files and serves embedded component executables, ringer files, and device configuration files. You can view the total Cisco TFTP requests, requests not found, and requests that were aborted.

The tool (RTMT) monitors the heartbeat of Cisco CallManagers, Cisco TFTPs, and Cisco CallManager Attendant Console Server services for different nodes. The heartbeat acts as an indicator of the life of whatever it is monitoring. When the heartbeat is lost, a blinking icon appears in the lower, right corner of the RTMT window. To find when the heartbeat loss was detected, click the blinking icon. An e-mail can notify you of the heartbeat loss, if you configure the system to do so.

The database summary provides connection information for each node, such as the change notification requests that are queued in the database, change notification requests that are queued in memory, the total number of active client connections, and the number of devices that are queued for a device reset.

[Table 22-3](#) provides information about the objects that RTMT monitors, the alert, thresholds, and defaults. For information on daily reports for CTI and Cisco TFTP usage statistics, see the “Service Statistics Report” section in the *Cisco Unified CallManager Serviceability System Guide, Release 5.0(4)*.

Table 22-3 Services Category

Monitored Objects (displayed)	Alert/Threshold/Default
Number of open devices, lines, CTI connections, and active Cisco CallManager links for each CTI Manager.	N/A
TotalTftpRequests and TotalTftpRequestsAborted for each Cisco TFTP server.	N/A
Connection and replication status for each Directory server.	• Connection failed. • Replication failed.
Heartbeat rate for each Cisco CallManager, Cisco TFTP, and Cisco CallManager Attendant Console Server services.	• Cisco Unified CallManager heartbeat rate equals <0.x. Default equals 0.5. • Cisco TFTP heartbeat rate equals <0.x. Default specifies 0.5. • Cisco CallManager Attendant Console Server heartbeat rate equals <0.x. Default specifies 0.5.

Understanding Service Logs

The service data accumulates in the memory whenever RTMT calls the LogService API. Every 5 minutes, RTMT logs the data into the file as a single record and cleans the memory.

The system logs data every 5 minutes for the following counters, based on the following calculation:

- `ctiOpenDevices`—Average of all the values that were collected in last 5 minutes
- `ctiLines`—Average of all the values that were collected in last 5 minutes
- `ctiConnections`—Average of all the values that were collected in last 5 minutes
- `ctiActiveCMLinks`—Average of all the values that were collected in last 5 minutes
- `tftpRequests`—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- `tftpAbortedRequests`—Cumulative (difference between last collected value and the first collected value in last 5 minutes)

The AMC service logs the service data in csv format. The header of the log comprises the time zone information and a set of columns with the counters that were previously listed for a Cisco Unified CallManager node. These sets of columns repeat for every node.

The following file name format of the Service Log applies: `ServiceLog_MM_DD_YYYY_hh_mm.csv`.

The first line of each log comprises the header.

Monitoring Devices

The Device monitoring category provides a summary of devices, device search capability, and a summary of phones.

The device summary provides information on the number of registered phones, gateways, and media resource devices on each Cisco Unified CallManager. [Table 22-4](#) provides information about the objects that RTMT monitors, the alert, thresholds, and defaults, and what kind of reports that RTMT generates for those devices. For information on daily reports on number of registered devices, see the “Device Statistics Report” section in the *Cisco Unified CallManager Serviceability System Guide, Release 5.0(4)*.

Table 22-4 **Devices Category**

Monitored Objects (displayed)	Alert/Threshold/Default
Number of registered phones for each Cisco Unified CallManager and cluster.	Total number of registered phones drops by X% in consecutive polls. Default specifies 10%.
Number of registered gateways on each Cisco Unified CallManager and cluster.	• (Warning) Clusterwide total number of registered gateways decreased in consecutive polls. • (Informational) Clusterwide total number of registered gateways increased in consecutive polls.
Number of registered media devices on each Cisco Unified CallManager and cluster.	• (Warning) Clusterwide total number of registered media devices decreased in consecutive polls. • (Informational) Clusterwide total number of registered media devices increased in consecutive polls. • Media List exhausted.

The Device Search menu comprises the following items on which you can search: phones, gateway devices, H.323 devices, CTI devices, voice-messaging devices, media resources, hunt lists, and SIP trunks.

You can search on any device in the Cisco Unified CallManager cluster and choose the status of the devices, including registered, unregistered, rejected, any status, and devices that are only configured in the database. You can also search by any model, or a specific device model, and set up criteria that include several different attributes. For phones, you can also search on the basis of phone protocol.



Tip

To find the matching item, RTMT requires that you activate the RIS service in the Service Activation window.

Results display in a table with a row for each matched device, a column for each of the specified attributes, and a time stamp of the device that has been opened/closed and the application that controls the device media.

The phone summary provides information on the number of registered phones, SIP phones, SCCP Phones, partially registered phones, and the number of failed registration attempts.

Understanding Device Logs

The device data accumulates in the memory whenever RTMT calls the LogDevice API. Every 5 minutes, RTMT logs the data into the file as a single record and cleans the memory.

The data gets logged every 5 minutes for the following counters based on the following calculation:

- gatewayDevicesFXS—Average of all the values that were collected in last 5 minutes
- gatewayDevicesFXO—Average of all the values that were collected in last 5 minutes
- gatewayDevicesPRI—Average of all the values that were collected in last 5 minutes
- gatewayDevicesT1—Average of all the values that were collected in last 5 minutes
- gatewayDevicesH323—Average of all the values that were collected in last 5 minutes

The AMC service logs the device data in csv format. The header of the log comprises the time zone information and a set of columns with the previously listed counters for a node. These sets of columns repeat for every node.

The following file name format of the Device Log applies: DeviceLog_MM_DD_YYYY_hh_mm.csv.

The first line of each log file comprises the header.

Monitoring CTI Applications, Devices, and Lines

The CTI search menu allows you to search on the following CTI components:

- CTI Applications
- CTI Devices
- CTI Lines

The CTI category monitors CTI Manager activities and provides CTI search capability. With CTI Manager, you can monitor the number of open devices, lines, and CTI connections. You can specify criteria for the CTI applications, devices, and lines that include CTI status, device name, application pattern, and attributes.



To find the matching item, RTMT requires that you activate the RIS service in the Service Activation window in Cisco Unified CallManager Serviceability.

Results display in a table with a row for each matched device, a column for each of the specified attributes, and a time stamp of the device that has been opened/closed and the application that controls the device media.

Where to Find More Information

Related Topics

- Alert Configuration in RTMT, *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)*
- Configuring and Using Performance Monitoring, *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)*

- Trace Collection and Log Central in RTMT, *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)*
- Alerts, *Cisco Unified CallManager Serviceability System Guide, Release 5.0(4)*
- [Performance Objects and Counters](#), *Cisco Unified CallManager New and Changed Information Guide, Release 5.0(4)*



Performance Objects and Counters

This chapter, which provides an overview of Cisco Unified CallManager-related objects and counters, contains information on the following topics:

- [Working with Performance Objects and Counters, page 23-1](#)
- [Using RTMT for Performance Monitoring, page 23-59](#)
- [Category Tabs, page 23-60](#)
- [Sample Rate, page 23-61](#)
- [Adding Counters to Monitor, page 23-61](#)
- [Alert Notification for Counters, page 23-61](#)
- [Zoom Counter, page 23-61](#)
- [Counter Properties, page 23-61](#)
- [Understanding Perfmon Logs, page 23-62](#)
- [Troubleshooting Guide for Cisco Unified CallManager, Release 5.0\(4\), page 23-62](#)
- [Where to Find More Information, page 23-63](#)

Working with Performance Objects and Counters

Cisco Unified CallManager directly updates Performance counters (called PerfMon counters), which are call-processing-related counters. The counters contain simple, useful counts such as number of registered phones, number of active calls, and number of available conference bridge resources.

The Cisco Unified CallManager object contains most of the performance counters, and these counters have only one instance. The instance-based counters that belong to the other objects can have zero or more instances. For example, if two phones are registered to Cisco Unified CallManager, two instances of each counter that belong to the Cisco phones object exist.

For information on specific counters, click the blue text in the following list to go to the object:

- [Cisco Analog Access, page 23-3](#)
- [Cisco Annunciator Device, page 23-4](#)
- [Cisco CallManager, page 23-4](#)
- [Cisco CallManager Attendant Console, page 23-11](#)
- [Cisco CallManager System Performance, page 23-12](#)
- [Cisco CTIManager, page 23-15](#)

- Cisco Dual-Mode Mobility, page 23-16
- Cisco Extension Mobility, page 23-17
- Cisco Gatekeeper, page 23-17
- Cisco H.323, page 23-18
- Cisco Hunt Lists, page 23-19
- Cisco HW Conference Bridge Device, page 23-20
- Cisco IP Manager Assistant, page 23-20
- Cisco Lines, page 23-21
- Cisco Locations, page 23-21
- Cisco Media Streaming Application, page 23-22
- Cisco Messaging Interface, page 23-25
- Cisco MGCP FXO Device, page 23-25
- Cisco MGCP FXS Device, page 23-26
- Cisco MGCP Gateways, page 23-26
- Cisco MGCP PRI Device, page 23-27
- Cisco MGCP T1 CAS Device, page 23-27
- Cisco Music On Hold (MOH) Device, page 23-28
- Cisco MTP Device, page 23-29
- Cisco Phones, page 23-29
- Cisco Presence Feature, page 23-30
- Cisco QSIG Features, page 23-30
- Cisco SIP, page 23-30
- Cisco SIP Stack, page 23-31
- Cisco SW Conf Bridge Device, page 23-39
- Cisco TFTP Server, page 23-40
- Cisco Tomcat Connector, page 23-43
- Cisco Tomcat JVM, page 23-45
- Cisco Tomcat Web Application, page 23-46
- Cisco Transcode Device, page 23-47
- Cisco Video Conference Bridge, page 23-47
- Cisco WebDialer, page 23-48
- Cisco WSM Connector, page 23-48
- Database Change Notification Client, page 23-49
- Database Change Notification Server, page 23-50
- Database Change Notification Subscription, page 23-50
- Database Local DSN, page 23-50
- Database Local DSN, page 23-50
- DB User Host Information Counters, page 23-51

- Enterprise Replication DBSpace Monitors, page 23-51
- Enterprise Replication Perfmon Counters, page 23-51
- IP, page 23-51
- Memory, page 23-53
- Network Interface, page 23-54
- Number of Replicates Created and State of Replication, page 23-55
- Partition, page 23-55
- Process, page 23-56
- Processor, page 23-57
- System, page 23-58
- TCP, page 23-58
- Thread, page 23-59

**Tip**

For the latest performance monitoring counters, objects, and counter descriptions that are available for Cisco Unified CallManager, access the performance monitoring counters in the Real-Time Monitoring Tool. In RTMT, you can review a counter description, as described in the “Displaying a Counter Description” section in the *Cisco CallManager Serviceability Administration Guide, Release 5.0(4)*.

Cisco Analog Access

The Cisco Analog Access object provides information about registered Cisco Analog Access gateways. [Table 23-1](#) contains information about Cisco Analog Access counters.

Table 23-1 **Cisco Analog Access**

Counters	Counter Descriptions
OutboundBusyAttempts	This counter represents the total number of times that Cisco Unified CallManager attempts a call through the Analog Access gateway when all ports were busy.
PortsActive	This counter represents the number of ports that are currently in use (active). A port appears active when a call is in progress on that port.
PortsOutOfService	This counter represents the number of ports that are currently out of service. Counter applies only to loop-start and ground-start trunks.

Cisco Annunciator Device

The Cisco Annunciator Device object provides information about registered Cisco annunciator devices. [Table 23-2](#) contains information about Cisco Annunciator counters.

Table 23-2 *Cisco Annunciator Device*

Counters	Counter Descriptions
OutOfResources	This counter represents the total number of times that Cisco Unified CallManager attempted to allocate an annunciator resource from an annunciator device and failed; for example, because all resources were already in use.
ResourceActive	This counter represents the total number of annunciator resources that are currently active (in use) for an annunciator device.
ResourceAvailable	This counter represents the total number of resources that are not active and are still available to be used at the current time for the annunciator device.
ResourceTotal	This counter represents the total number of annunciator resources that are configured for an annunciator device.

Cisco CallManager

The Cisco CallManager object provides information about calls, applications, and devices that are registered with the Cisco Unified CallManager. [Table 23-3](#) contains information about Cisco CallManager counters.

Table 23-3 *Cisco CallManager*

Counters	Counter Descriptions
AnnunciatorOutOfResources	This counter represents the total number of times that Cisco Unified CallManager attempted to allocate an annunciator resource from those that are registered to a Cisco Unified CallManager when none were available.
AnnunciatorResourceActive	This counter represents the total number of annunciator resources that are currently in use on all annunciator devices that are registered with a Cisco Unified CallManager.
AnnunciatorResourceAvailable	This counter represents the total number of annunciator resources that are not active and are currently available.
AnnunciatorResourceTotal	This counter represents the total number of annunciator resources that are provided by all annunciator devices that are currently registered with Cisco Unified CallManager.
AuthenticatedCallsActive	This counter represents the number of authenticated calls that are currently active (in use) on Cisco Unified CallManager. An authenticated call designates one in which all the endpoints that are participating in the call are authenticated. An authenticated phone uses the Transport Layer Security (TLS) authenticated Skinny protocol signaling with Cisco Unified CallManager.

Table 23-3 *Cisco CallManager (continued)*

Counters	Counter Descriptions
AuthenticatedCallsCompleted	This counter represents the number of authenticated calls that connected and subsequently disconnected through Cisco Unified CallManager. An authenticated call designates one in which all the endpoints that are participating in the call are authenticated. An authenticated phone uses the TLS authenticated Skinny protocol signaling with Cisco Unified CallManager.
AuthenticatedPartiallyRegisteredPhone	This counter represents the number of partially registered, authenticated SIP phones.
AuthenticatedRegisteredPhones	This counter represents the total number of authenticated phones that are registered to Cisco Unified CallManager. An authenticated phone uses the TLS authenticated Skinny protocol signaling with Cisco Unified CallManager.
BRChannelsActive	This counter represents the number of BRI voice channels that are currently in an active call on this Cisco Unified CallManager.
BRISpansInService	This counter represents the number of BRI spans that are currently available for use.
CallManagerHeartBeat	This counter represents the heartbeat of Cisco Unified CallManager. This incremental count indicates that Cisco Unified CallManager is up and running. If the count does not increment, that indicates that Cisco Unified CallManager is down.
CallsActive	This counter represents the number of voice or video streaming connections that are currently in use (active); in other words, the number of calls that actually have a voice path that is connected on Cisco Unified CallManager.
CallsAttempted	This counter represents the total number of attempted calls. An attempted call occurs any time that a phone goes off hook and back on hook, regardless of whether any digits were dialed, or whether it connected to a destination. The system considers some call attempts during feature operations (such as transfer and conference) to be attempted calls.
CallsCompleted	This counter represents the number of calls that were actually connected (a voice path or video stream was established) through Cisco Unified CallManager. This number increases when the call terminates.
CallsInProgress	This counter represents the number of voice or video calls that are currently in progress on Cisco Unified CallManager, including all active calls. When a phone, that is registered as Skinny Client Control Protocol (SCCP) phone goes off hook, the CallsInProgress progress counter increments. until it goes back on hook. For Cisco Unified IP Phones 7902, 7905, 7912, 7940, and 7960 that register as SIP phones, the CallsInProgress counter increments when the dial softkey is pressed. For all other SIP phones, the CallsInProgress counter increments when the first digit is pressed. When all voice or video calls that are in progress are connected, the number of CallsInProgress represents the number of CallsActive. The counter decreases by one when a phone goes back on hook.

Table 23-3 *Cisco CallManager (continued)*

Counters	Counter Descriptions
EncryptedCallsActive	This counter represents the number of encrypted calls that are currently active (in use) on this Cisco Unified CallManager. An encrypted call represents one in which all the endpoints that are participating in the call are encrypted.
EncryptedCallsCompleted	This counter represents the number of encrypted calls that were connected and subsequently disconnected through this Cisco Unified CallManager. An encrypted call represents one in which all the endpoints that are participating in the call are encrypted.
EncryptedPartiallyRegisteredPhones	This counter represents the number of partially registered, encrypted SIP phones.
EncryptedRegisteredPhones	This counter represents the total number of encrypted phones that are registered on this Cisco Unified CallManager.
FXOPortsActive	This counter represents the number of FXO ports that are currently in use (active) on a Cisco Unified CallManager.
FXOPortsInService	This counter represents the number of FXO ports that are currently available for use in the system.
FXSPortsActive	This counter represents the number of FXS ports that are currently in use (active) on a Cisco Unified CallManager.
FXSPortsInService	This counter represents the number of FXS ports that are currently available for use in the system.
HuntListsInService	This counter represents the number of hunt lists that are currently in service on Cisco Unified CallManager.
HWConferenceActive	This counter represents the total number of hardware conference resources that are provided by all hardware conference bridge devices that are currently registered with Cisco Unified CallManager.
HWConferenceCompleted	This counter represents the total number of conferences that used a hardware conference bridge (hardware-based conference devices such as Cisco Catalyst 6000, Cisco Catalyst 4000, Cisco VG200, Cisco series 26xx and 36xx) that is allocated from Cisco Unified CallManager and that have completed, which means that the conference bridge has been allocated and released. A conference activates when the first call connects to the bridge. The conference completes when the last call disconnects from the bridge.
HWConferenceOutOfResources	This counter represents the total number of times that Cisco Unified CallManager attempted to allocate a hardware conference resource from those that are registered to a Cisco Unified CallManager when none was available.
HWConferenceResourceActive	This counter represents the total number of conference resources that are in use on all hardware conference devices (such as Cisco Catalyst 6000, Catalyst 4000, Cisco VG200, Cisco series 26xx and 36xx) that are registered with Cisco Unified CallManager. System considers conference to be active when one or more calls are connected to a bridge.
HWConferenceResourceAvailable	This counter represents the number of hardware conference resources that are not in use and that are available to be allocated on all hardware conference devices (such as Cisco Catalyst 6000, Cisco Catalyst 4000, Cisco VG200, Cisco series 26xx and 36xx) that are allocated from Cisco Unified CallManager and that have been completed, which means that the conference bridge has been allocated and released. A conference activates when the first call connects to the bridge. The conference completes when the last call disconnects from the bridge.

Table 23-3 *Cisco CallManager (continued)*

Counters	Counter Descriptions
HWConferenceResourceTotal	This counter represents the number of active conferences on all hardware conference devices that are registered with Cisco Unified CallManager.
InitializationState	This counter represents the current initialization state of Cisco Unified CallManager. Cisco Unified CallManager includes the following initialization state values: 1-Database; 2-Regions; 3-Locations; 4-Calling Search Space; 5-Time Of Day; 6-AAR Neighborhoods; 7-Digit Analysis; 8-Route Plan; 9-Call Control; 10-Supplementary Services; 11-Directory; 12-SDL Link; 13-Device; 100-Initialization Complete. Not all states displays when this counter is used. This does not indicate that an error occurred; it simply indicates that the state(s) initialized and completed within the refresh period of the performance monitor.
LocationOutOfResources	This counter represents the total number of times that a call through Locations failed due to the lack of bandwidth.
MOHMulticastResourceActive	This counter represents the total number of multicast MOH resources that are currently in use (active) on all MOH servers that are registered with a Cisco Unified CallManager.
MOHMulticastResourceAvailable	This counter represents the total number of active multicast MOH connections that are not being used on all MOH servers that are registered with a Cisco Unified CallManager.
MOHOutOfResources	This counter represents the total number of times that the Media Resource Manager attempted to allocate an MOH resource when all available resources on all MOH servers that are registered with a Cisco Unified CallManager were already active.
MOHTotalMulticastResources	This counter represents the total number of multicast MOH resources or connections that are provided by all MOH servers that are currently registered with a Cisco Unified CallManager.
MOHTotalUnicastResources	This counter represents the total number of unicast MOH resources or streams that are provided by all MOH servers that are currently registered with Cisco Unified CallManager. Each MOH unicast resource uses one stream.
MOHUnicastResourceActive	This counter represents the total number of unicast MOH resources that are currently in use (active) on all MOH servers that are registered with Cisco Unified CallManager. Each MOH unicast resource uses one stream.
MOHUnicastResourceAvailable	This counter represents the total number of unicast MOH resources that are currently available on all MOH servers that are registered with Cisco Unified CallManager. Each MOH unicast resource uses one stream.
MTPOutOfResources	This counter represents the total number of times Cisco Unified CallManager attempted but failed to allocate an MTP resource from one MTP device that is registered with Cisco Unified CallManager. This also means that no transcoders were available to act as MTPs.
MTPResourceActive	This counter represents the total number of MTP resources that are currently in use (active) on all MTP devices that are registered with a Cisco Unified CallManager. Each MTP resource uses two streams. An MTP in use represents one MTP resource that has been allocated for use in a call.

Table 23-3 *Cisco CallManager (continued)*

Counters	Counter Descriptions
MTPResourceAvailable	This counter represents the total number of MTP resources that are not in use and are available to be allocated on all MTP devices that are registered with Cisco Unified CallManager. Each MTP resource uses two streams. An MTP in use represents one MTP resource that has been allocated for use in a call.
MTPResourceTotal	This counter represents the total number of media termination point (MTP) resources that are provided by all MTP devices that are currently registered with Cisco Unified CallManager.
PartiallyRegisteredPhone	This counter represents the number of partially registered SIP phones.
PRChannelsActive	This counter represents the number of PRI voice channels that are in an active call on a Cisco Unified CallManager.
PRISpansInService	This counter represents the number of PRI spans that are currently available for use.
RegisteredAnalogAccess	This counter represents the number of registered Cisco analog access gateways that are registered with system. The count does not include the number of Cisco analog access ports.
RegisteredHardwarePhones	This counter represents the number of Cisco hardware IP phones (for example, Cisco Unified IP Phone models 7960, 7940, 7910, and so on.) that are currently registered in the system.
RegisteredMGCPGateway	This counter represents the number of MGCP gateways that are currently registered in the system.
RegisteredOtherStationDevices	This counter represents the number of station devices other than Cisco hardware IP phones that are currently registered in the system (for example, Cisco IP SoftPhone, CTI port, CTI route point, Cisco voice-mail port).
SIPLineServerAuthorizationChallenges	This counter represents the number of authentication challenges for incoming SIP requests that the Cisco Unified CallManager server issued to SIP phones. An authentication challenge occurs when a SIP phone with Digest Authentication enabled sends a SIP line request to Cisco Unified CallManager.
SIPLineServerAuthorizationFailures	This counter represents the number of authentication challenge failures for incoming SIP requests from SIP phones to the Cisco Unified CallManager server. An authentication failure occurs when a SIP phone with Digest Authentication enabled sends a SIP line request with bad credentials to Cisco Unified CallManager.
SIPTrunkApplicationAuthorization	This counter represents the number of application-level authorization checks for incoming SIP requests that the Cisco Unified CallManager server issued to SIP trunks. An application-level authorization check occurs when the Cisco Unified CallManager system compares an incoming SIP request to the application-level settings on the SIP Trunk Security Profile window in Cisco Unified CallManager Administration.
SIPTrunkApplicationAuthorizationFailures	This counter represents the number of application-level authorization failures for incoming SIP requests that occurred on Cisco Unified CallManager SIP trunks. An application-level authorization failure occurs when Cisco Unified CallManager compares an incoming SIP request to the application-level settings on the SIP Trunk Security Profile window in Cisco Unified CallManager Administration and finds that application-level authorization for one or more of the features on that window is not allowed.

Table 23-3 *Cisco CallManager (continued)*

Counters	Counter Descriptions
SIPTrunkServerAuthenticationChallenges	This counter represents the number of authentication challenges for incoming SIP requests that Cisco Unified CallManager issued to SIP trunks. An authentication challenge occurs when a SIP trunk with Digest Authentication enabled sends a SIP request to Cisco Unified CallManager.
SIPTrunkServerAuthenticationFailures	This counter represents the number of authentication challenge failures that occurred for incoming SIP requests from SIP trunks to Cisco Unified CallManager. An authentication failure occurs when a SIP trunk with Digest Authentication enabled sends a SIP request with bad credentials to Cisco Unified CallManager.
SWConferenceActive	This counter represents the number of active conferences on all software conference devices that are registered with Cisco Unified CallManager.
SWConferenceCompleted	This counter represents the total number of conferences that used a software conference bridge that was allocated from a Cisco Unified CallManager and that have been completed, which means that the conference bridge has been allocated and released. A conference activates when the first call connects to the bridge. The conference completes when the last call disconnects from the bridge.
SWConferenceOutOfResources	This counter represents the total number of times that Cisco Unified CallManager attempted to allocate a software conference resource from those that are registered to Cisco Unified CallManager when none were available. Counter includes failed attempts to add a new participant to an existing conference.
SWConferenceResourceActive	This counter represents the total number of conference resources that are in use on all software conference devices that are registered with Cisco Unified CallManager. The system considers a conference to be active when one or more calls connect to a bridge. One resource is equal to one stream.
SWConferenceResourceAvailable	This counter represents the number of new software-based conferences that can be started at the same time, for Cisco Unified CallManager. You must have a minimum of three streams available for each new conference. One resource is equal to one stream.
SWConferenceResourceTotal	This counter represents the total number of software conference resources that are provided by all software conference bridge devices that are currently registered with Cisco Unified CallManager.
SystemCallsAttempted	This counter represents the total number of server originated calls and attempted calls to the Unity Message waiting indicator (MWI).
T1ChannelsActive	This counter represents the number of T1 CAS voice channels that are in an active call on a Cisco Unified CallManager.
T1SpansInService	This counter represents the number of T1 CAS spans that are currently available for use.
TLSConnectedSIPTrunks	This counter represents the number of SIP trunks that are configured and connected via Transport Layer Security (TLS).
TLSConnectedWSM	This counter represents the number of WSM Connectors that is configured and connected to Motorola WSM via Transport Layer Security (TLS).
TranscoderOutOfResources	This counter represents the total number of times that Cisco Unified CallManager attempted to allocate a transcoder resource from a transcoder device that is registered to a Cisco Unified CallManager when none was available.

Table 23-3 *Cisco CallManager (continued)*

Counters	Counter Descriptions
TranscoderResourceActive	This counter represents the total number of transcoders that are in use on all transcoder devices that are registered with Cisco Unified CallManager. A transcoder in use represents one transcoder resource that has been allocated for use in a call. Each transcoder resource uses two streams.
TranscoderResourceAvailable	This counter represents the total number of transcoders that are not in use and that are available to be allocated on all transcoder devices that are registered with Cisco Unified CallManager. Each transcoder resource uses two streams.
TranscoderResourceTotal	This counter represents the total number of transcoder resources that are provided by all transcoder devices that are currently registered with Cisco Unified CallManager.
VCBConferenceActive	This counter represents the total number of active video conferences on all video conference bridge devices that are registered with Cisco Unified CallManager.
VCBConferenceAvailable	This counter represents the total number of new video conferences on all video conference bridge devices that are registered with Cisco Unified CallManager.
VCBConferenceCompleted	This counter represents the total number of video conferences that used a video conference bridge that are allocated from Cisco Unified CallManager and that have been completed, which means that the conference bridge has been allocated and released. A conference activates when the first call connects to the bridge. The conference completes when the last call disconnects from the bridge.
VCBConferenceTotal	This counter represents the total number of video conferences that are supported on all video conference bridge devices that are registered with Cisco Unified CallManager.
VCBOutOfConferences	This counter represents the total number of times that Cisco Unified CallManager attempted to allocate a video conference resource from those that are registered to Cisco Unified CallManager when none was available.
VCBOutOfResources	This counter represents the total number of failed new video conference requests. A conference request can fail because, for example, the configured number of conferences is already in use.
VCBResourceActive	This counter represents the total number of video conference resources that are currently in use on all video conference devices that are registered with Cisco Unified CallManager.
VCBResourceAvailable	This counter represents the total number of video conference resources that are not active and are currently available.
VCBResourceTotal	This counter represents the total number of video conference resources that are provided by all video conference bridge devices that are currently registered with Cisco Unified CallManager.
VideoCallsActive	This counter represents the number of active video calls with active video streaming connections on all video conference bridge devices that are registered with Cisco Unified CallManager.

Table 23-3 *Cisco CallManager (continued)*

Counters	Counter Descriptions
VideoCallsCompleted	This counter represents the number of video calls that were actually connected with video streams and then released.
VideoOutOfResources	This counter represents the total number of times that Cisco Unified CallManager attempted to allocate a video-streaming resource from one of the video conference bridge devices that is registered to Cisco Unified CallManager when none was available.

Cisco CallManager Attendant Console

The Cisco CallManager Attendant Console (Cisco CallManager Attendant Console Server service) object provides information about the Cisco Unified CallManager Attendant Console. [Table 23-4](#) contains information about Cisco CallManager Attendant Console counters.

Table 23-4 *Cisco CallManager Attendant Console*

Counters	Counter Descriptions
CallsActive	Do not use this counter. Information in this counter may not accurately reflect the total number of active calls.
CallsRedirected	This counter represents the total number of redirected calls for the Cisco CallManager Attendant Console Server service. This number increases every time that a pilot point receives a call and redirects the call to a member of its hunt group.
CallsTotal	This counter represents the total number of all calls that have been made since the Cisco CallManager Attendant Console Server service started.
CcmLineLinkState	This counter represents the line state. Values include 0, 1, 10, or 11. A value of 0 indicates that the Cisco CallManager Attendant Console Server service has not registered or has not received line link state information from Cisco CallManager; 1 indicates that the Cisco CallManager Attendant Console Server service has registered and is receiving line link state information from Cisco CallManager; 10 indicates that the Cisco CallManager Attendant Console Server service has logged into CTI but has not registered or has not received line link state information from Cisco CallManager; 11 indicates that the Cisco CallManager Attendant Console Server service has logged into CTI and has registered and is receiving line link state information.
ClientsOnline	This counter represents the total number of Cisco Unified CallManager attendant console clients that are currently online. Attendant Console clients include all users that are configured in the attendant console User Configuration window in Cisco Unified CallManager Administration that are currently online. This number increases by one for each client that goes online and decreases by one for each client that goes offline.
ClientsRegistered	This counter represents the total number of registered clients for the Cisco CallManager Attendant Console Server service. This number increases by one for each new registration of a Cisco Unified CallManager attendant console client when the client application logs in.

Table 23-4 *Cisco CallManager Attendant Console (continued)*

Counters	Counter Descriptions
ClientsTotal	This counter represents the total number of Cisco Unified CallManager Attendant Console clients that are currently registered with the Cisco CallManager Attendant Console Server service. Attendant console clients represent all users that are configured in the Attendant Console User Configuration window in Cisco Unified CallManager Administration.
HeartBeat	This counter represents the heartbeat of the Cisco CallManager Attendant Console Server service. This incremental count indicates that Cisco CallManager Attendant Console Server service is up and running. If the count does not increase, this means that the service is down.
LinesActive	Do not use this counter. Information in this counter may not accurately reflect the total number of active lines.
LinesIdle	Do not use this counter. Information in this counter may not accurately reflect the total number of idle lines.
LinesTotal	Do not use this counter. Information in this counter may not accurately reflect the total number of lines.
PilotPointsTotal	This counter represents the total number of pilot points that are configured in Cisco Unified CallManager.
StartTime	This counter represents the time in milliseconds since the Cisco CallManager Attendant Console Server service started. The real-time clock in the computer, which is simply a reference point that indicates the current time and the time that has elapsed, in milliseconds, since the service started provides the basis for this time. The reference point specifies midnight, January 1, 1970.
Version	This counter represents the version of the Cisco CallManager Attendant Console Server service.

Cisco CallManager System Performance

The Cisco CallManager System Performance object provides system performance information about Cisco Unified CallManager. [Table 23-5](#) contains information about Cisco CallManager system performance counters.

Table 23-5 *Cisco CallManager System Performance*

Counters	Counter Descriptions
AverageExpectedDelay	This counter represents the current average expected delay before any incoming message gets handled.
CallsRejectedDueToCallThrottling	This counter represents the total number of calls that were rejected since the start of service due to call throttling.
CallThrottlingGenericCounter3	This counter represents a generic counter that is used for call-throttling purpose.
CodeRedEntryExit	This counter indicates whether Cisco Unified CallManager has entered or exited a Code Red state (call-throttling mode). Valid values include 0 (Exit) and 1 (Entry).

Table 23-5 *Cisco CallManager System Performance (continued)*

Counters	Counter Descriptions
CodeYellowEntryExit	This counter indicates whether Cisco Unified CallManager has entered or exited a Code Yellow state (call-throttling mode). Valid values include 0 (Exit) and 1 (Entry).
EngineeringCounter1	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
EngineeringCounter2	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
EngineeringCounter3	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
EngineeringCounter4	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
EngineeringCounter5	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
EngineeringCounter6	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
EngineeringCounter7	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
EngineeringCounter8	Do not use this counter unless directed by a Cisco Engineering Special build. Cisco uses information in this counter for diagnostic purposes.
QueueSignalsPresent 1-High	This counter indicates the number of high-priority signals in the Cisco Unified CallManager queue. High-priority signals include timeout events, internal Cisco Unified CallManager keepalives, certain gatekeeper events, and internal process creation, among other events. A large number of high-priority events will cause degraded performance on Cisco Unified CallManager and result in slow call connection or loss of dial tone. Use this counter in conjunction with the QueueSignalsProcessed 1-High counter to determine the processing delay on Cisco Unified CallManager.
QueueSignalsPresent 2-Normal	This counter indicates the number of normal-priority signals in the Cisco Unified CallManager queue. Normal-priority signals include call-processing functions, key presses, on-hook and off-hook notifications, among other events. A large number of normal-priority events will cause degraded performance on Cisco Unified CallManager, sometimes resulting in delayed dial tone, slow call connection, or loss of dial tone. Use this counter in conjunction with the QueueSignalsProcessed 2-Normal counter to determine the call-processing delay on Cisco Unified CallManager. Remember that high-priority signals must complete before normal-priority signals begin to process, so check the high-priority counters as well to get an accurate picture of the potential delay.
QueueSignalsPresent 3-Low	This counter indicates the number of low-priority signals in the Cisco Unified CallManager queue. Low-priority signals include station device registration (except the initial station registration request message), among other events. A large number of signals in this queue could result in delayed device registration, among other events.

Table 23-5 *Cisco CallManager System Performance (continued)*

Counters	Counter Descriptions
QueueSignalsPresent 4-Lowest	This counter indicates the number of lowest priority signals in the Cisco Unified CallManager queue. Lowest priority signals include the initial station registration request message during device registration, among other events. A large number of signals in this queue could result in delayed device registration, among other events.
QueueSignalsProcessed 1-High	This counter indicates the number of high-priority signals that Cisco Unified CallManager processes for each 1-second interval. Use this counter in conjunction with the QueueSignalsPresent 1-High counter to determine the processing delay on this queue.
QueueSignalsProcessed 2-Normal	This counter indicates the number of normal-priority signals that Cisco Unified CallManager processes for each 1-second interval. Use this counter in conjunction with the QueueSignalsPresent 2-Normal counter to determine the processing delay on this queue. Remember that high-priority signals get processed before normal-priority signals.
QueueSignalsProcessed 3-Low	This counter indicates the number of low-priority signals that Cisco Unified CallManager processes for each 1-second interval. Use this counter in conjunction with the QueueSignalsPresent 3-Low counter to determine the processing delay on this queue. The number of signals processed gives an indication of how much device registration activity is being processed in this time interval.
QueueSignalsProcessed 4-Lowest	This counter indicates the number of lowest priority signals that Cisco Unified CallManager processes for each 1-second interval. Use this counter in conjunction with the QueueSignalsPresent 4-Lowest counter to determine the processing delay on this queue. The number of signals that are processed gives an indication of how many devices began the Cisco Unified CallManager registration process in this time interval.
QueueSignalsProcessed Total	This counter provides a sum total of all queue signals that Cisco Unified CallManager processes for each 1-second period for all queue levels: high, normal, low, and lowest.
SkinnyDevicesThrottled	This counter represents the total number of Skinny devices that are being throttled. A Skinny device gets throttled (asked to shut down and reregister) when the total number of events that the Skinny device generated exceeds the configured maximum threshold value (default value specifies 2000 events) within a 5-second interval.
ThrottlingSampleActivity	This counter indicates how many samples, out of the configured sample size, have non-zero averageExpectedDelay values. This counter gets reset when any sample has an averageExpectedDelay value of zero. This process repeats for each batch of samples. A batch represents the configured sample size.
TotalCodeYellowEntry	This counter indicates the number of times that Cisco Unified CallManager call processing enters the code yellow state. This counter remains cumulative from the start of the Cisco Unified CallManager process.

Cisco CTIManager

The Cisco CTI Manager object provides information about Cisco CTI Manager. [Table 23-6](#) contains information about Cisco CTIManager counters.

Table 23-6 *Cisco CTI Manager*

Counters	Counter Descriptions
CcmLinkActive	This counter represents the total number of active Cisco Unified CallManager links. CTI Manager maintains links to all active Cisco Unified CallManagers in the cluster.
CTIConnectionActive	This counter represents the total number of CTI clients that are currently connected to the CTIManager. This counter increases by one when new connection is established and decreases by one when a connection is released. The CTIManager service parameter MaxCTIConnections determines the maximum number of active connections.
DevicesOpen	This counter represents the total number of devices that are configured in Cisco Unified CallManager that CTI applications control and/or monitor. Devices include hardware IP phones, CTI ports, CTI route points, and so on.
LinesOpen	This counter represents the total number of lines that are configured in Cisco Unified CallManager that control and/or monitor CTI applications.
QbeVersion	This counter represents the version number of the Quick Buffer Encoding (QBE) interface that the CTIManager uses.

Cisco Dual-Mode Mobility

The Cisco Dual-Mode Mobility object provides information about the dual-mode mobility application on Cisco Unified CallManager. [Table 23-6](#) contains information about Cisco Dual-Mode Mobility counters.

Table 23-7 Cisco Dual-Mode Mobility

Counters	Counter Descriptions
CallsAnchored	This counter represents the number of calls that are placed or received on dual-mode phones that are anchored in Cisco Unified CallManager. The counter increments when a call is received from or placed to a dual-mode phone. The counter increments twice if a dual-mode phone calls another dual-mode phone.
DMMSRegistered	This counter represents the number of Dual-mode Mobile Station (DMMS) subscribers that are registered in the wireless LAN (WLAN).
FollowMeAborted	This counter represents the number of failed follow-me operations.
FollowMeAttempted	This counter represents the number of follow-me operations that Cisco Unified CallManager attempted. The counter increments when a SIP 302 - Moved Temporarily message is received from the Wireless Service Manager (WSM) and Cisco Unified CallManager redirects the call to the DMMS in WLAN.
FollowMeCompleted	This counter represents the number of follow-me operations that were successfully completed. The counter increments when the DMMS in WLAN answers the call and the media (voice path) is successfully established with the calling device.
FollowMeInProgress	This counter represents the number of follow-me operations that are currently in progress. The counter increments when a follow-me is attempted, and it decrements when the follow-me operation is aborted or completed.
H1HandOutAttempted	This counter represents the number of H1 hand-out operations that dual-mode phones attempt. The counter increments when Cisco Unified CallManager processes a call to the H1 number from a DMMS.
H1HandOutCompleted	This counter represents the number of successfully completed H1 hand-out operations. The counter increments when the DMMS in WLAN successfully reestablishes a media (voice path).
H2HandOutCompleted	This counter represents the number of successfully completed H2 hand-out operations. The counter increments when the DMMS in WLAN successfully reestablishes a media (voice path).
H2HandOutsAttempted	This counter represents the number of H2 hand-out operations that dual-mode phones attempt. The counter increments when Cisco Unified CallManager receives a call to the H2 number from a DMMS.
HandInAborted	This counter represents the number of hand-in operations that failed.
HandInAttempted	This counter represents the number of hand-in operations that dual-mode phones attempt.
HandInCompleted	This counter represents the number of successfully completed hand-in operations. The counter increments when the DMMS in WLAN successfully reestablishes a media (voice path).

Table 23-7 Cisco Dual-Mode Mobility (continued)

Counters	Counter Descriptions
HandInInProgress	This counter represents the number of hand-in operations that are currently in progress. The counter increments when a hand-in is attempted, and the counter decrements when the hand-in is aborted or completed.
HandOutAborted	This counter represents the number of hand-out operations that failed.
HandOutInProgress	This counter represents the number of H1 and H2 hand-out operations that are currently in progress. The counter increments when a H1 or H2 hand-out is attempted, and it decrements when the hand-out is aborted or completed.

Cisco Extension Mobility

The Cisco Extension Mobility object provides information about the extension mobility application.

[Table 23-8](#) contains information about Cisco Extension Mobility counters.

Table 23-8 Cisco Extension Mobility Application

Counters	Counter Descriptions
RequestsHandled	This counter represents the total number of HTTP requests that the extension mobility application handled since the last restart of the Cisco CallManager service. A typical login would constitute two HTTP requests: one to query the initial login state of the device and another to log in the user on a device. Similarly, a typical logout also results in two HTTP requests.
RequestsInProgress	This counter represents the number of HTTP requests that the extension mobility application currently is handling. A typical login would constitute two HTTP requests: one to query the initial login state of the device and another to log in the user on a device. Similarly, a typical logout also results in two HTTP requests.
RequestsThrottled	This counter represents the total number of Login/Logout Requests that failed due to throttling.
LoginsSuccessful	This counter represents the total number of successful login requests that were completed through EM Service.
LogoutsSuccessful	This counter represents the total number of successful logout requests that were completed through EM Service
Total Login/LogoutRequestsAttempted	This counter represents the total number of Login and Logout requests that were attempted through this EM Service. This number includes both successful and unsuccessful attempts.

Cisco Gatekeeper

The Cisco Gatekeeper object provides information about registered Cisco gatekeeper devices.

[Table 23-9](#) contains information about Cisco gatekeeper device counters.

Table 23-9 *Cisco Gatekeeper*

Counters	Counter Descriptions
ACFsReceived	This counter represents the total number of RAS Admission Confirm messages that are received from the configured gatekeeper and its alternate gatekeepers.
ARQsAttempted	This counter represents the total number of RAS Admission Request messages that are attempted by using the configured gatekeeper and its alternate gatekeepers.
RasRetries	This counter represents the number of retries due to loss or delay of all RAS acknowledgement messages on the configured gatekeeper and its alternate gatekeepers.
VideoOutOfResources	This counter represents the total number of video-stream requests to the configured gatekeeper or its alternate gatekeepers that failed, most likely due to lack of bandwidth.

Cisco H.323

The Cisco H.323 object provides information about registered Cisco H.323 devices. [Table 23-10](#) contains information about Cisco H.323 device counters.

Table 23-10 *Cisco H.323*

Counters	Counter Descriptions
CallsActive	This counter represents the number of streaming connections that are currently active (in use) on the configured H.323 device; in other words, the number of calls that actually have a voice path that is connected.
CallsAttempted	This counter represents the total number of calls that have been attempted on a device, including both successful and unsuccessful call attempts.
CallsCompleted	This counter represents the total number of successful calls that were made from a device.
CallsInProgress	This counter represents the number of calls that are currently in progress on a device.
VideoCallsActive	This counter represents the number of video calls with video streaming connections that are currently active (in use) on all H.323 trunks that are registered with a Cisco Unified CallManager; in other words, the number of calls that actually have video-streaming connections on a Cisco Unified CallManager.
VideoCallsCompleted	This counter represents the number of video calls that were actually connected with video streams for all H.323 trunks that were registered with a Cisco Unified CallManager. This number increases when the call terminates.

Cisco Hunt Lists

The Cisco Hunt Lists object provides information about the hunt lists that are defined in Cisco Unified CallManager administration. [Table 23-11](#) contains information about Cisco hunt list counters.

Table 23-11 *Cisco Hunt Lists*

Counters	Counter Descriptions
CallsAbandoned	This counter represents the number of abandoned calls that occurred through a hunt list. An abandoned call represents one in which a caller hangs up before the call is answered.
CallsActive	This counter represents the number of calls that are currently active (in use) that occurred through a hunt list. An active call represents one that gets distributed and answered, and to which a voice path connects.
CallsBusyAttempts	This counter represents the number of times that calls through a hunt list were attempted when all members of the line and/or route groups were busy.
CallsInProgress	This counter represents the number of calls that are currently in progress through a hunt list. A call in progress represents one that the Call Distributor is attempting to extend to a member of a line or route group and that has not yet been answered. Examples of a hunt list member include a line, a station device, a trunk device, or a port/channel of a trunk device.
CallsRingNoAnswer	This counter represents the total number of calls through a hunt list that rang but that called parties did not answer.
HuntListInService	This counter specifies whether the particular hunt list is currently in service. A value of 0 indicates that the hunt list is out of service; a value of 1 indicates that the hunt list is in service. Reasons that a hunt list could be out of service include the hunt list is not running on a primary Cisco Unified CallManager based on its Cisco Unified CallManager Group or the hunt list has been disabled in Cisco Unified CallManager Administration.
MembersAvailable	This counter represents the total number of available or idle members of line and route groups that belong to an in-service hunt list. An available member currently handles a call and will accept a new call. An idle member does not handle any call and will accept a new call. A hunt list member can comprise a route group, line group, or a combination. A member of a line group represents a directory number of a line on an IP phone or a voice-mail port. A member of a route group represents a station gateway, a trunk gateway, or port/channel of a trunk gateway.

Cisco HW Conference Bridge Device

The Cisco HW Conference Bridge Device object provides information about registered Cisco hardware conference bridge devices. [Table 23-12](#) contains information about Cisco hardware conference bridge device counters.

Table 23-12 *Cisco HW Conference Bridge Device*

Counters	Counter Descriptions
HWConferenceActive	This counter represents the number of conferences that are currently active (in use) on a HW conference bridge device. One resource represents one stream.
HWConferenceCompleted	This counter represents the total number of conferences that have been allocated and released on a HW conference device. A conference starts when the first call connects to the bridge. The conference completes when the last call disconnects from the bridge.
OutOfResources	This counter represents the total number of times that an attempt was made to allocate a conference resource from a HW conference device and failed, for example, because all resources were already in use.
ResourceActive	This counter represents the number of resources that are currently in use (active) for this HW conference device. One resource represents one stream.
ResourceAvailable	This counter represents the total number of resources that are not active and are still available to be used now for a HW conference device. One resource represents one stream.
ResourceTotal	This counter represents the total number of resources for a HW conference bridge device. This counter equals the sum of the counters ResourceAvailable and ResourceActive. One resource represents one stream.

Cisco IP Manager Assistant

The Cisco IP Manager Assistant (IPMA) Service object provides information about the Cisco Unified CallManager Assistant application. [Table 23-13](#) contains information on Cisco IPMA counters.

Table 23-13 *Cisco IP Manager Assistant Service*

Counters	Counter Descriptions
AssistantsActive	This counter represents the number of assistant consoles that are currently active. An active assistant console exists when an assistant is logged in from his or her assistant console desktop application.
LinesOpen	This counter represents the number of phone lines that the Cisco Unified CallManager Assistant application opened. An open phone line exists when the application assumes line control from CTI.
ManagersActive	This counter represents the current number of managers that the Cisco IPMA is servicing.
SessionsCurrent	This counter represents the total number of managers assistants that are currently using the Cisco Unified CallManager Assistant application. Each manager and each assistant constitutes an active session, so for one manager/assistant pair, this counter would reflect two sessions.

Cisco Lines

The Cisco Lines object represents the number of Cisco lines (directory numbers) that can dial and connect to a device. Lines represent all directory numbers that terminate on an endpoint. The directory number that is assigned to it identifies the line. The Cisco Lines object does not include directory numbers that include wildcards such as a pattern for a Digital or Analog Access gateway.

The Active counter represents the state of the line, either active or not active. A zero indicates the line is not in use. When the number is greater than zero, this indicates that the line is active, and the number represents the number of calls that are currently in progress on that line. If more than one call is active, this indicates the call is on hold either because of being placed on hold specifically (user hold) or because of a network hold operation (for example, a transfer is in progress, and it is on transfer hold). This applies to all directory numbers that are assigned to any device.

Cisco Locations

The Cisco Location object provides information about locations that are defined in Cisco Unified CallManager. [Table 23-14](#) contains information on Cisco location counters.

Table 23-14 *Cisco Locations*

Counters	Counter Descriptions
BandwidthAvailable	This counter represents the current bandwidth in a given location. A value of 0 indicates that no bandwidth is available.
BandwidthMaximum	This counter represents the maximum bandwidth that is available in a given location. A value of 0 indicates that infinite bandwidth is available.
CallsInProgress	This counter represents the number of calls that are currently in progress on a particular Cisco Unified CallManager.
OutOfResources	This counter represents the total number of times that a call on a particular Cisco Unified CallManager through the location failed due to lack of bandwidth.
RSVP AudioReservationErrorCounts	This counter represents the number of RSVP reservation errors in the audio stream.
RSVP MandatoryConnectionsInProgress	This counter represents the number of connections with mandatory RSVP that are in progress.
RSVP OptionalConnectionsInProgress	This counter represents the number of connections with optional RSVP that are in progress.
RSVP TotalCallsFailed	This counter represents the number of total calls that failed due to a RSVP reservation failure.
RSVP VideoCallsFailed	This counter represents the number of video calls that failed due to a RSVP reservation failure.
RSVP VideoReservationErrorCounts	This counter represents the number of RSVP reservation errors in the video stream
VideoBandwidthAvailable	This counter represents the bandwidth that is currently available for video in the location where the person who initiated the video conference resides. A value of 0 indicates that no bandwidth is available.

Table 23-14 *Cisco Locations (continued)*

Counters	Counter Descriptions
VideoBandwidthMaximum	This counter represents the maximum bandwidth that is available for video in the location where the person who initiated the video conference resides. A value of 0 indicates that no bandwidth is allocated for video.
VideoOutOfResources	This counter represents the total number of failed video-stream requests (most likely due to lack of bandwidth) in the location where the person who initiated the video conference resides.

Cisco Media Streaming Application

The Cisco IP Voice Media Streaming Application object provides information about the registered MTPs, MOH servers, conference bridge servers, and annunciators. [Table 23-15](#) contains information on Cisco IP Voice Media Streaming Application counters.


Note

One object exists for each Cisco Unified CallManager in the Cisco Unified CallManager group that is associated with the device pool that the annunciator device is configured to use.

Table 23-15 *Cisco Media Streaming Application*

Counter	Counter Descriptions
ANNConnectionsLost	This counter represents the total number of times since the last restart of the Cisco IP Voice Media Streaming Application that a Cisco Unified CallManager connection was lost.
ANNConnectionState	For each Cisco Unified CallManager that is associated with an annunciator, this counter represents the current registration state to Cisco Unified CallManager; 0 indicates no registration to Cisco Unified CallManager; 1 indicates registration to the primary Cisco Unified CallManager; 2 indicates connection to the secondary Cisco Unified CallManager (connected to Cisco Unified CallManager but not registered until the primary Cisco Unified CallManager connection fails).
ANNConnectionsTotal	This counter represents the total number of annunciator instances that have been started since the Cisco IP Voice Media Streaming Application service started.
ANNInstancesActive	This counter represents the number of actively playing (currently in use) announcements.
ANNStreamsActive	This counter represents the total number of currently active simplex (one direction) streams for all connections. Each stream direction counts as one stream. One internal stream provides the audio input and another output stream to the endpoint device.
ANNStreamsAvailable	This counter represents the remaining number of streams that are allocated for the annunciator device that are available for use. This counter starts as 2 multiplied by the number of configured connections (defined in the Cisco IP Voice Media Streaming App service parameter for the Annunciator, Call Count) and is reduced by one for each active stream that started.
ANNStreamsTotal	This counter represents the total number of simplex (one direction) streams that connected to the annunciator device since the Cisco IP Voice Media Streaming Application service started.

Table 23-15 Cisco Media Streaming Application (continued)

Counter	Counter Descriptions
CFBConferencesActive	This counter represents the number of active (currently in use) conferences.
CFBConferencesTotal	This counter represents the total number of conferences that started since the Cisco IP Voice Media Streaming Application service started.
CFBConnectionsLost	This counter represents the total number of times since the last restart of the Cisco IP Voice Media Streaming Application that a Cisco Unified CallManager connection was lost.
CFBConnectionState	For each Cisco Unified CallManager that is associated with a SW Conference Bridge, this counter represents the current registration state to Cisco Unified CallManager; 0 indicates no registration to Cisco Unified CallManager; 1 indicates registration to the primary Cisco Unified CallManager; 2 indicates connection to the secondary Cisco Unified CallManager (connected to Cisco Unified CallManager but not registered until the primary Cisco Unified CallManager connection fails).
CFBStreamsActive	This counter represents the total number of currently active simplex (one direction) streams for all conferences. Each stream direction counts as one stream. In a three-party conference, the number of active streams equals 6.
CFBStreamsAvailable	This counter represents the remaining number of streams that are allocated for the conference bridge that are available for use. This counter starts as 2 multiplied by the number of configured connections (defined in the Cisco IP Voice Media Streaming App service parameter for Conference Bridge, Call Count) and is reduced by one for each active stream started.
CFBStreamsTotal	This counter represents the total number of simplex (one direction) streams that connected to the conference bridge since the Cisco IP Voice Media Streaming Application service started.
MOHAudioSourcesActive	This counter represents the number of active (currently in use) audio sources for this MOH server. Some of these audio sources may not be actively streaming audio data if no devices are listening. The exception exists for multicast audio sources, which will always be streaming audio. When an audio source is in use, even after the listener has disconnected, this counter will always have one input stream for each configured MOH codec. For unicast streams, the stream may exist in a suspended state where no audio data is received until a device connects to listen to the stream. Each MOH multicast resource uses one stream for each audio source and codec combination. For example, if the default audio source is configured for multicast, G.711 mu-law and wideband codecs, then two streams get used (default audio source + G.711 mu-law and default audio source + wideband).
MOHConnectionsLost	This counter represents the total number of times since the last restart of the Cisco IP Voice Media Streaming Application that a Cisco Unified CallManager connection was lost.
MOHConnectionState	For each Cisco Unified CallManager that is associated with an MOH, this counter represents the current registration state to Cisco Unified CallManager; 0 indicates no registration to Cisco Unified CallManager; 1 indicates registration to the primary Cisco Unified CallManager; 2 indicates connection to the secondary Cisco Unified CallManager (connected to Cisco Unified CallManager but not registered until the primary Cisco Unified CallManager connection fails).

Table 23-15 *Cisco Media Streaming Application (continued)*

Counter	Counter Descriptions
MOHStreamsActive	This counter represents the total number of active (currently in use) simplex (one direction) streams for all connections. One output stream exists for each device that is listening to a unicast audio source, and one input stream exists for each active audio source, multiplied by the number of MOH codecs. When an audio source has been used once, it will always have one input stream for each configured MOH codec. For unicast streams, the stream may exist in a suspended state where no audio data is received until a device connects to listen to the stream. Each MOH multicast resource uses one stream for each audio source and codec combination. For example, if the default audio source is configured for multicast, G.711 mu-law and wideband codecs, then two streams get used (default audio source + G.711 mu-law and default audio source + wideband).
MOHStreamsAvailable	This counter represents the remaining number of streams that are allocated for the MOH device that are available for use. This counter starts as 408 plus the number of configured half-duplex unicast connections and is reduced by 1 for each active stream that started. The counter gets reduced by 2 for each multicast audio source, multiplied by the number of MOH codecs that are configured. The counter gets reduced by 1 for each unicast audio source, multiplied by the number of MOH codecs configured.
MOHStreamsTotal	This counter represents the total number of simplex (one direction) streams that have connected to the MOH server since the Cisco IP Voice Media Streaming Application service started.
MTPConnectionsLost	This counter represents the total number of times since the last restart of the Cisco IP Voice Streaming Application that a Cisco Unified CallManager connection was lost.
MTPConnectionState	For each Cisco Unified CallManager that is associated with an MTP, this counter represents the current registration state to Cisco Unified CallManager; 0 indicates no registration to Cisco Unified CallManager; 1 indicates registration to the primary Cisco Unified CallManager; 2 indicates connection to the secondary Cisco Unified CallManager (connected to Cisco Unified CallManager but not registered until the primary Cisco Unified CallManager connection fails).
MTPConnectionsTotal	This counter represents the total number of MTP instances that have been started since the Cisco IP Voice Media Streaming Application service started.
MTPInstancesActive	This counter represents the number of active (currently in use) instances of MTP.
MTPStreamsActive	This counter represents the total number of currently active simplex (one direction) streams for all connections. Each stream direction counts as one stream.
MTPStreamsAvailable	This counter represents the remaining number of streams that are allocated for the MTP device that are available for use. This counter starts as 2 multiplied by the number of configured connections (defined in the Cisco IP Voice Media Streaming App service parameter for MTP, Call Count) and is reduced by one for each active stream started.
MTPStreamsTotal	This counter represents the total number of simplex (one direction) streams that connected to the MTP device since the Cisco IP Voice Media Streaming Application service started.

Cisco Messaging Interface

The Cisco Messaging Interface object provides information about the Cisco Messaging Interface (CMI) service. [Table 23-16](#) contains information on Cisco Messaging Interface (CMI) counters.

Table 23-16 *Cisco Messaging Interface*

Counters	Counter Descriptions
HeartBeat	This counter represents the heartbeat of the CMI service. This incremental count indicates that the CMI service is up and running. If the count does not increase (increment), the CMI service is down.
SMDIMessageCountInbound	This counter represents the running count of inbound SMDI messages since the last restart of the CMI service.
SMDIMessageCountInbound24Hour	This counter represents the rolling count of inbound SMDI messages in the last 24 hours.
SMDIMessageCountOutbound	This counter represents the running count of outbound SMDI messages since the last restart of the CMI service.
SMDIMessageCountOutbound24Hour	This counter represents the rolling count of outbound SMDI messages in the last 24 hours.
StartTime	This counter represents the time in milliseconds when the CMI service started. The real-time clock in the computer, which simply acts as a reference point that indicates the current time and the time that has elapsed, in milliseconds, since the service started, provides the basis for this time. The reference point specifies midnight, January 1, 1970.

Cisco MGCP FXO Device

The Cisco Media Gateway Control Protocol (MGCP) Foreign Exchange Office (FXO) Device object provides information about registered Cisco MGCP FXO devices. [Table 23-17](#) contains information on Cisco MGCP FXO device counters.

Table 23-17 *Cisco MGCP FXO Device*

Counters	Counter Descriptions
CallsCompleted	This counter represents the total number of successful calls that were made from the port on an MGCP FXO device.
OutboundBusyAttempts	This counter represents the total number of times that a call through the port on this MGCP FXO device was attempted when no voice channels were available.
PortStatus	This counter represents the status of the FXO port associated with this MGCP FXO device.

Cisco MGCP FXS Device

The Cisco MGCP Foreign Exchange Station (FXS) Device object provides information about registered Cisco MGCP FXS devices. One instance of this object gets created for each port on a Cisco Catalyst 6000 24 port FXS Analog Interface Module gateway. For example, a fully configured Catalyst 6000 Analog Interface Module would represent 24 separate instances of this object. [Table 23-18](#) contains information on Cisco MGCP FXS device counters.

Table 23-18 *Cisco MGCP FXS Device*

Counters	Counter Descriptions
CallsCompleted	This counter represents the total number of successful calls that were made from this port on the MGCP FXS device.
OutboundBusyAttempts	This counter represents the total number of times that a call through this port on the MGCP FXS device was attempted when no voice channels were available.
PortStatus	This counter represents the status of the FXS port that is associated with a MGCP FXS device.

Cisco MGCP Gateways

The Cisco MGCP Gateways object provides information about registered MGCP gateways. [Table 23-19](#) contains information on Cisco MGCP gateway counters.

Table 23-19 *Cisco MGCP Gateways*

Counters	Counter Descriptions
BRISpansActive	This counter represents the number of BRI voice channels that are currently active in a call in the gateway.
BRISpansInService	This counter represents the number of BRI spans that are currently available for use in the gateway.
FXOPortsActive	This counter represents the number of FXO ports that are currently active in a call in the gateway.
FXOPortsInService	This counter represents the number of FXO ports that are currently available for use in the gateway.
FXSPortsActive	This counter represents the number of FXS ports that are currently active in a call in the gateway.
FXSPortsInService	This counter represents the number of FXS ports that are currently available for use in the gateway.
PRISpansActive	This counter represents the number of PRI voice channels that are currently active in a call in the gateway.
PRISpansInService	This counter represents the number of PRI spans that are currently available for use in the gateway.
T1ChannelsActive	This counter represents the number of T1 CAS voice channels that are currently active in a call in the gateway.
T1SpansInService	This counter represents the number of T1 CAS spans that are currently available for use in the gateway.

Cisco MGCP PRI Device

The Cisco MGCP Primary Rate Interface (PRI) Device object provides information about registered Cisco MGCP PRI devices. [Table 23-20](#) contains information on Cisco MGCP PRI device counters.

Table 23-20 *Cisco MGCP PRI Device*

Counters	Counter Descriptions
CallsActive	This counter represents the number of calls that are currently active (in use) on this MGCP PRI device.
CallsCompleted	This counter represents the total number of successful calls that were made from this MGCP PRI device.
Channel 1 Status through Channel 15 Status (consecutively numbered)	This counter represents the status of the indicated B-Channel that is associated with a MGCP PRI device. Possible values: 0 (Unknown) indicates that the status of the channel could not be determined; 1 (Out of service) indicates that this channel is not available for use; 2 (Idle) indicates that this channel has no active call and is ready for use; 3 (Busy) indicates that an active call exists on this channel; 4 (Reserved) indicates that this channel has been reserved for use as a D-Channel or for use as a Synch-Channel for E-1.
Channel 16 Status	This counter represents the status of the indicated B-Channel that is associated with a MGCP PRI Device. Possible values: 0-Unknown, 1-Out of service, 2-Idle, 3-Busy, 4-Reserved, for an E1 PRI Interface, this channel is reserved for use as a D-Channel.
Channel 17 Status through Channel 31 Status (consecutively numbered)	This counter represents the status of the indicated B-Channel that is associated with the MGCP PRI Device. 0-Unknown, 1-Out of service, 2-Idle, 3-Busy, 4-Reserved.
DatalinkInService	This counter represents the state of the Data Link (D-Channel) on the corresponding digital access gateway. This value will be set to 1 (one) if the Data Link is up (in service) or 0 (zero) if the Data Link is down (out of service).
OutboundBusyAttempts	This counter represents the total number of times that a call through an MGCP PRI device was attempted when no voice channels were available.

Cisco MGCP T1 CAS Device

The Cisco MGCP T1 Channel Associated Signaling (CAS) Device object provides information about registered Cisco MGCP T1 CAS devices. [Table 23-21](#) contains information on Cisco MGCP TI CAS device counters.

Table 23-21 *Cisco MGCP T1 CAS Device*

Counters	Counter Descriptions
CallsActive	This counter represents the number of calls that are currently active (in use) on this MGCP T1 CAS device.
CallsCompleted	This counter represents the total number of successful calls that were made from this MGCP T1 CAS device.

Table 23-21 *Cisco MGCP T1 CAS Device (continued)*

Counters	Counter Descriptions
Channel 1 Status through Channel 24 Status (consecutively numbered)	This counter represents the status of the indicated B-Channel that is associated with an MGCP T1 CAS device. Possible values: 0 (Unknown) indicates the status of the channel could not be determined; 1 (Out of service) indicates that this channel is not available for use; 2 (Idle) indicates that this channel has no active call and is ready for use; 3 (Busy) indicates that an active call exists on this channel; 4 (Reserved) indicates that this channel has been reserved for use as a D-Channel or for use as a Synch-Channel for E-1.
OutboundBusyAttempts	This counter represents the total number of times that a call through the MGCP T1 CAS device was attempted when no voice channels were available.

Cisco Music On Hold (MOH) Device

The Cisco Music On Hold (MOH) Device object provides information about registered Cisco MOH devices. [Table 23-22](#) contains information on Cisco MOH device counters.

Table 23-22 *Cisco MOH Device*

Counters	Counter Descriptions
MOHHighestActiveResources	This counter represents the largest number of simultaneously active MOH connections for an MOH server. This number includes both multicast and unicast connections.
MOHMulticastResourceActive	This counter represents the number of currently active multicast connections to multicast addresses that are served by an MOH server. Each MOH multicast resource uses one stream for each audio source and codec combination. For example, if the default audio source is configured for multicast, G.711 mu-law and wideband codecs, two streams get used (default audio source + G.711 mu-law and default audio source + wideband).
MOHMulticastResourceAvailable	This counter represents the number of multicast MOH connections to multicast addresses that are served by an MOH server that are not active and are still available to be used now for the MOH server. Each MOH multicast resource uses one stream for each audio source and codec combination. For example, if the default audio source is configured for multicast, G.711 mu-law and wideband codecs, two streams get used (default audio source + G.711 mu-law and default audio source + wideband).
MOHOutOfResources	This counter represents the total number of times that the Media Resource Manager attempted to allocate an MOH resource when all available resources on all MOH servers that are registered with a Cisco Unified CallManager were already active.
MOHTotalMulticastResources	This counter represents the total number of multicast MOH connections that are allowed to multicast addresses that are served by an MOH server. Each MOH multicast resource uses one stream for each audio source and codec combination. For example, if the default audio source is configured for multicast, G.711 mu-law and wideband codecs, two streams get used (default audio source + G.711 mu-law and default audio source + wideband).

Table 23-22 *Cisco MOH Device (continued)*

Counters	Counter Descriptions
MOHTotalUnicastResources	This counter represents the total number of unicast MOH connections that are allowed by an MOH server. Each MOH unicast resource uses one stream.
MOHUnicastResourceActive	This counter represents the number of active unicast MOH connections to an MOH server. Each MOH unicast resource uses one stream.
MOHUnicastResourceAvailable	This counter represents the number of unicast MOH connections that are not active and are still available to be used now for an MOH server. Each MOH unicast resource uses one stream.

Cisco MTP Device

The Cisco Media Termination Point (MTP) Device object provides information about registered Cisco MTP devices. [Table 23-23](#) contains information on Cisco MTP device counters.

Table 23-23 *Cisco MTP Device*

Counters	Counter Descriptions
OutOfResources	This counter represents the total number of times that an attempt was made to allocate an MTP resource from an MTP device and failed; for example, because all resources were already in use.
ResourceActive	This counter represents the number of MTP resources that are currently in use (active) for an MTP device. Each MTP resource uses two streams. An MTP in use represents one MTP resource that has been allocated for use in a call.
ResourceAvailable	This counter represents the total number of MTP resources that are not active and are still available to be used now for an MTP device. Each MTP resource uses two streams. An MTP in use represents one MTP resource that has been allocated for use in a call.
ResourceTotal	This counter represents the total number of MTP resources that an MTP device provides. This counter equals the sum of the counters ResourceAvailable and ResourceActive.

Cisco Phones

The Cisco Phones object provides information about the number of registered Cisco Unified IP Phones, including both hardware-based and other station devices.

The CallsAttempted counter represents the number of calls that have been attempted from this phone. This number increases each time that the phone goes off hook and on hook.

Cisco Presence Feature

The Cisco Presence object provides information about presence subscriptions, such as statistics that are related to the speed dial or call list Busy Lamp Field (BLF) subscriptions. [Table 23-24](#) contains information on Cisco Presence feature.

Table 23-24 *Cisco Presence*

Counters	Counter Descriptions
ActiveCallListAndTrunkSubscriptions	This counter represents the active presence subscriptions for the call list feature as well as presence subscriptions through SIP trunk.
ActiveSubscriptions	This counter represents all active incoming and outgoing presence subscriptions.
CallListAndTrunkSubscriptionsThrottled	This counter represents the cumulative number of rejected call list and trunk side presence subscriptions due to throttling for the call list feature.
IncomingLineSideSubscriptions	This counter represents the cumulative number of presence subscriptions that were received on the line side.
IncomingTrunkSideSubscriptions	This counter represents the cumulative number of presence subscriptions that were received on the trunk side.
OutgoingTrunkSideSubscriptions	This counter represents the cumulative number of presence subscriptions that were sent on the trunk side.

Cisco QSIG Features

The Cisco QSIG Feature object provides information regarding the operation of various QSIG features, such as call diversion and path replacement. [Table 23-25](#) contains information on the Cisco QSIG feature counters.

Table 23-25 *Cisco QSIG*

Counters	Counter Descriptions
CallForwardByRerouteCompleted	This counter represents the number of successful calls that has been forwarded by rerouting. Call forward by rerouting enables the path for a forwarded call to be optimized (minimizes the number of B-Channels in use) from the originator perspective. This counter gets reset when the Cisco Unified CallManager service parameter Call Forward by Reroute Enabled is enabled or disabled, or when the Cisco CallManager service restarts.
PathReplacementCompleted	This counter represents the number of successful path replacements that have occurred. Path replacement in a QSIG network optimizes the path between two edge PINX (PBXs) that are involved in a call. This counter resets when the Cisco CallManager service parameter Path Replacement Enabled is enabled or disabled, or when the Cisco CallManager service restarts.

Cisco SIP

The Cisco Session Initiation Protocol (SIP) object provides information about configured SIP devices. [Table 23-26](#) contains information on the Cisco SIP counters.

Table 23-26 *Cisco SIP*

Counters	Counter Descriptions
CallsActive	This counter represents the number of calls that are currently active (in use) on this SIP device.
CallsAttempted	This counter represents the number of calls that have been attempted on this SIP device, including both successful and unsuccessful call attempts.
CallsCompleted	This counter represents the number of calls that were actually connected (a voice path was established) from a SIP device. This number increases when the call terminates.
CallsInProgress	This counter represents the number of calls that are currently in progress on a SIP device, including all active calls. When all calls that are in progress are connected, the number of CallsInProgress equals the number of CallsActive.
VideoCallsActive	This counter represents the number of video calls with streaming video connections that are currently active (in use) on this SIP device.
VideoCallsCompleted	This counter represents the number of video calls that were actually connected with video streams for this SIP device. This number increments when the call terminates.

Cisco SIP Stack

The Cisco SIP Stack object provides information about Session Initiation Protocol (SIP) stack statistics that are generated or used by SIP devices such as SIP Proxy, SIP Redirect Server, SIP Registrar, and SIP User Agent. [Table 23-27](#) contains information on Cisco SIP Stack counters.

Table 23-27 *Cisco SIP Stack*

Counters	Counter Descriptions
AckIns	This counter represents the total number of ACK requests that the SIP device received.
AckOuts	This counter represents the total number of ACK requests that the SIP device sent.
ByeIns	This counter represents the total number of BYE requests that the SIP device received. This number includes retransmission.
ByeOuts	This counter represents the total number of BYE requests that the SIP device sent. This number includes retransmission.
CancelIns	This counter represents the total number of CANCEL requests that the SIP device received. This number includes retransmission.
CancelOuts	This counter represents the total number of CANCEL requests that the SIP device sent. This number includes retransmission.
GlobalFailedClassIns	This counter represents the total number of 6xx class SIP responses that the SIP device has received. This number includes retransmission. This class of responses indicates that a SIP device, that is providing a client function, received a failure response message. Generally, the responses indicate that a server had definitive information on a particular called party and not just the particular instance in the Request-URI.

Table 23-27 *Cisco SIP Stack (continued)*

Counters	Counter Descriptions
GlobalFailedClassOuts	This counter represents the total number of 6xx class SIP responses that the SIP device sent. This number includes retransmission. This class of responses indicates that a SIP device, that is providing a server function, received a failure response message. Generally, the responses indicate that a server had definitive information on a particular called party and not just the particular instance in the Request-URI.
InfoClassIns	This counter represents the total number of 1xx class SIP responses that the SIP device received. This includes retransmission. This class of responses provides information on the progress of a SIP request.
InfoClassOuts	This counter represents the total number of 1xx class SIP responses that the SIP device sent. This includes retransmission. This class of responses provides information on the progress of processing a SIP request.
InfoIns	This counter represents the total number of INFO requests that the SIP device has received. This number includes retransmission.
InfoOuts	This counter represents the total number of INFO requests that the SIP device has sent. This number includes retransmission.
InviteIns	This counter represents the total number of INVITE requests that the SIP device received. This number includes retransmission.
InviteOuts	This counter represents the total number of INVITE requests that the SIP device has sent. This number includes retransmission.
NotifyIns	This counter represents the total number of NOTIFY requests that the SIP device has received. This number includes retransmission.
NotifyOuts	This counter represents the total number of NOTIFY requests that the SIP device has sent. This number includes retransmission.
OptionsIns	This counter represents the total number of OPTIONS requests that the SIP device received. This number includes retransmission.
OptionsOuts	This counter represents the total number of OPTIONS requests that the SIP device has sent. This number includes retransmission.
PRackIns	This counter represents the total number of PRACK requests that the SIP device has received. This number includes retransmission.
PRackOuts	This counter represents the total number of PRACK requests that the SIP device has sent. This number includes retransmission.
RedirClassIns	This counter represents the total number of 3xx class SIP responses that the SIP device has received. This number includes retransmission. This class of responses provides information about redirections to addresses where the callee may be reachable.
RedirClassOuts	This counter represents the total number of 3xx class SIP responses that the SIP device has sent. This number includes retransmission. This class of responses provides information about redirections to addresses where the callee may be reachable.
ReferIns	This counter represents the total number of REFER requests that the SIP device has received. This number includes retransmission.

Table 23-27 *Cisco SIP Stack (continued)*

Counters	Counter Descriptions
ReferOuts	This counter represents the total number of REFER requests that the SIP device has sent. This number includes retransmission.
RegisterIns	This counter represents the total number of REGISTER requests that the SIP device has received. This number includes retransmission.
RegisterOuts	This counter represents the total number of REGISTER requests that the SIP device has sent. This number includes retransmission.
RequestsFailedClassIns	This counter represents the total number of 4xx class SIP responses that the SIP device has received. This number includes retransmission. This class of responses indicates a request failure by a SIP device that is providing a client function.
RequestsFailedClassOuts	This counter represents the total number of 4xx class SIP responses that the SIP device has sent. This number includes retransmission. This class of responses indicates a request failure by a SIP device that is providing a server function.
RetryByes	This counter represents the total number of BYE retries that the SIP device has sent. To determine the number of first BYE attempts, subtract the value of this counter from the value of the sipStatsByeOuts counter.
RetryCancels	This counter represents the total number of CANCEL retries that the SIP device has sent. To determine the number of first CANCEL attempts, subtract the value of this counter from the value of the sipStatsCancelOuts counter.
RetryInfo	This counter represents the total number of INFO retries that the SIP device has sent. To determine the number of first INFO attempts, subtract the value of this counter from the value of the sipStatsInfoOuts counter.
RetryInvites	This counter represents the total number of INVITE retries that the SIP device has sent. To determine the number of first INVITE attempts, subtract the value of this counter from the value of the sipStatsInviteOuts counter.
RetryNotify	This counter represents the total number of NOTIFY retries that the SIP device has sent. To determine the number of first NOTIFY attempts, subtract the value of this counter from the value of the sipStatsNotifyOuts counter.
RetryPRACK	This counter represents the total number of PRACK retries that the SIP device has sent. To determine the number of first PRACK attempts, subtract the value of this counter from the value of the sipStatsPRACKOuts counter.
RetryRefer	This counter represents the total number of REFER retries that the SIP device has sent. To determine the number of first REFER attempts, subtract the value of this counter from the value of the sipStatsReferOuts counter.
RetryRegisters	This counter represents the total number of REGISTER retries that the SIP device has sent. To determine the number of first REGISTER attempts, subtract the value of this counter from the value of the sipStatsRegisterOuts counter.
RetryRel1xx	This counter represents the total number of Reliable 1xx retries that the SIP device has sent.
RetryResponsesFinal	This counter represents the total number of Final Response retries that the SIP device has sent.
RetryResponsesNonFinal	This counter represents the total number of non-Final Response retries the SIP device has sent.

Table 23-27 *Cisco SIP Stack (continued)*

Counters	Counter Descriptions
RetrySubscribe	This counter represents the total number of SUBSCRIBE retries that the SIP device has sent. To determine the number of first SUBSCRIBE attempts, subtract the value of this counter from the value of the sipStatsSubscribeOuts counter.
RetryUpdate	This counter represents the total number of UPDATE retries that the SIP device has sent. To determine the number of first UPDATE attempts, subtract the value of this counter from the value of the sipStatsUpdateOuts counter.
ServerFailedClassIns	This counter represents the total number of 5xx class SIP responses that the SIP device has received. This number includes retransmission. This class of responses indicates that failure responses were received by a SIP device that is providing a client function.
ServerFailedClassOuts	This counter represents the total number of 5xx class SIP responses that the SIP device has sent. This number includes retransmission. This class of responses indicates that failure responses were received by a SIP device that is providing a server function.
StatusCode1xxIns	This counter represents the total number of 1xx response messages, including retransmission, that the SIP device has received. This count includes the following 1xx responses: • 100 Trying • 180 Ringing • 181 Call is being forwarded • 182 Queued • 183 Session Progress
StatusCode1xxOuts	This counter represents the total number of 1xx response messages, including retransmission, that the SIP device has sent. This count includes the following 1xx responses: • 100 Trying • 180 Ringing • 181 Call is being forwarded • 182 Queued • 183 Session Progress
StatusCode2xxIns	This counter represents the total number of 2xx response messages, including retransmission, that the SIP device has received. This count includes the following 2xx responses: • 200 OK • 202 Success Accepted
StatusCode2xxOuts	This counter represents the total number of 2xx response messages, including retransmission, that the SIP device has sent. This count includes the following 2xx responses: • 200 OK • 202 Success Accepted

Table 23-27 *Cisco SIP Stack (continued)*

Counters	Counter Descriptions
StatusCode3xxins	This counter represents the total number of 3xx response messages, including retransmission, that the SIP device has received. This count includes the following 3xx responses: • 300 Multiple Choices • 301 Moved Permanently • 302 Moved Temporarily • 303 Incompatible Bandwidth Units • 305 Use Proxy • 380 Alternative Service
StatusCode302Outs	This counter represents the total number of 302 Moved Temporarily response messages, including retransmission, that the SIP device has sent.

Table 23-27 *Cisco SIP Stack (continued)*

Counters	Counter Descriptions
StatusCode4xxIns	This counter represents the total number of 4xx response messages, including retransmission, that the SIP device has received. This count includes the following 4xx responses: • 400 Bad Request • 401 Unauthorized • 402 Payment Required • 403 Forbidden • 404 Not Found • 405 Method Not Allowed • 406 Not Acceptable • 407 Proxy Authentication Required • 408 Request Timeout • 409 Conflict • 410 Gone • 413 Request Entity Too Large • 414 Request-URI Too Long • 415 Unsupported Media Type • 416 Unsupported URI Scheme • 417 Unknown Resource Priority • 420 Bad Extension • 422 Session Expires Value Too Small • 423 Interval Too Brief • 480 Temporarily Unavailable • 481 Call/Transaction Does Not Exist • 482 Loop Detected • 483 Too Many Hops • 484 Address Incomplete • 485 Ambiguous • 486 Busy Here • 487 Request Terminated • 488 Not Acceptable Here • 489 Bad Subscription Event • 491 Request Pending

Table 23-27 *Cisco SIP Stack (continued)*

Counters	Counter Descriptions
StatusCode4xxOuts	This counter represents the total number of 4xx response messages, including retransmission, that the SIP device has sent. This count includes the following 4xx responses: • 400 Bad Request • 401 Unauthorized • 402 Payment Required • 403 Forbidden • 404 Not Found • 405 Method Not Allowed • 406 Not Acceptable • 407 Proxy Authentication Required • 408 Request Timeout • 409 Conflict • 410 Gone • 413 Request Entity Too Large • 414 Request-URI Too Long • 415 Unsupported Media Type • 416 Unsupported URI Scheme • 417 Unknown Resource Priority • 420 Bad Extension • 422 Session Expires Value Too Small • 423 Interval Too Brief • 480 Temporarily Unavailable • 481 Call/Transaction Does Not Exist • 482 Loop Detected • 483 Too Many Hops • 484 Address Incomplete • 485 Ambiguous • 486 Busy Here • 487 Request Terminated • 488 Not Acceptable Here • 489 Bad Subscription Event • 491 Request Pending

Table 23-27 *Cisco SIP Stack (continued)*

Counters	Counter Descriptions
StatusCode5xxIns	This counter represents the total number of 5xx response messages, including retransmission, that the SIP device has received. This count includes the following 5xx responses: • 500 Server Internal Error • 501 Not Implemented • 502 Bad Gateway • 503 Service Unavailable • 504 Server Timeout • 505 Version Not Supported • 580 Precondition Failed
StatusCode5xxOuts	This counter represents the total number of 5xx response messages, including retransmission, that the SIP device has sent. This count includes the following 5xx responses: • 500 Server Internal Error • 501 Not Implemented • 502 Bad Gateway • 503 Service Unavailable • 504 Server Timeout • 505 Version Not Supported • 580 Precondition Failed
StatusCode6xxIns	This counter represents the total number of 6xx response messages, including retransmission, that the SIP device has received. This count includes the following 6xx responses: • 600 Busy Everywhere • 603 Decline • 604 Does Not Exist Anywhere • 606 Not Acceptable
StatusCode6xxOuts	This counter represents the total number of 6xx response messages, including retransmission, that the SIP device has sent. This count includes the following 6xx responses: • 600 Busy Everywhere • 603 Decline • 604 Does Not Exist Anywhere • 606 Not Acceptable
SubscribeIns	This counter represents the total number of SUBSCRIBE requests that the SIP device has received. This number includes retransmission.
SubscribeOuts	This counter represents the total number of SUBSCRIBE requests that the SIP device has sent. This number includes retransmission.

Table 23-27 *Cisco SIP Stack (continued)*

Counters	Counter Descriptions
SuccessClassIns	This counter represents the total number of 2xx class SIP responses that the SIP device has received. This includes retransmission. This class of responses provides information on the successful completion of a SIP request.
SuccessClassOuts	This counter represents the total number of 2xx class SIP responses that the SIP device has sent. This includes retransmission. This class of responses provides information on the successful completion of a SIP request.
SummaryRequestsIn	This counter represents the total number of SIP request messages that have been received by the SIP device. This number includes retransmissions.
SummaryRequestsOut	This counter represents the total number of SIP request messages that the device sent. This number includes messages that originate on the device and messages that are being relayed by the device. When a particular message gets sent more than once, each transmission gets counted separately; for example, a message that is re-sent as a retransmission or as a result of forking.
SummaryResponsesIn	This counter represents the total number of SIP response messages that the SIP device received. This number includes retransmission.
SummaryResponsesOut	This counter represents the total number of SIP response messages that the SIP device sent (originated and relayed). This number includes retransmission.
UpdateIns	This counter represents the total number of UPDATE requests that the SIP device has received. This number includes retransmission.
UpdateOuts	This counter represents the total number of UPDATE requests that the SIP device has sent. This number includes retransmission.

Cisco SW Conf Bridge Device

The Cisco SW Conference Bridge Device object provides information about registered Cisco software conference bridge devices. [Table 23-28](#) contains information on the Cisco software conference bridge device counters.

Table 23-28 *Cisco SW Conf Bridge Device*

Counters	Counter Descriptions
OutOfResources	This counter represents the total number of times that an attempt was made to allocate a conference resource from a SW conference device and failed because all resources were already in use.
ResourceActive	This counter represents the number of resources that are currently in use (active) for a SW conference device. One resource represents one stream.
ResourceAvailable	This counter represents the total number of resources that are not active and are still available to be used now for a SW conference device. One resource represents one stream.
ResourceTotal	This counter represents the total number of conference resources that a SW conference device provides. One resource represents one stream. This counter equals the sum of the ResourceAvailable and ResourceActive counters.

Table 23-28 Cisco SW Conf Bridge Device (continued)

Counters	Counter Descriptions
SWConferenceActive	This counter represents the number of software-based conferences that are currently active (in use) on a SW conference device.
SWConferenceCompleted	This counter represents the total number of conferences that have been allocated and released on a SW conference device. A conference starts when the first call connects to the bridge. The conference completes when the last call disconnects from the bridge.

Cisco TFTP Server

The Cisco Trivial File Transfer Protocol (TFTP) Server object provides information about the Cisco TFTP server. [Table 23-29](#) contains information on Cisco TFTP server counters.

Table 23-29 Cisco TFTP Server

Counters	Counter Descriptions
BuildAbortCount	This counter represents the number of times that the build process aborted when it received a Build all request. This counter increases when building of device/unit/softkey/dial rules gets aborted as a result of group level change notifications.
BuildCount	This counter represents the number of times since the TFTP service started that the TFTP server has built all the configuration files in response to a database change notification that affects all devices. This counter increases by one every time the TFTP server performs a new build of all the configuration files.
BuildDeviceCount	This counter represents the number of devices that were processed in the last build of all the configuration files. This counter also updates while processing device change notifications. The counter increases when a new device is added and decreases when an existing device is deleted.
BuildDialruleCount	This counter represents the number of dial rules that were processed in the last build of the configuration files. This counter also updates while processing dial rule change notifications. The counter increases when a new dial rule is added and decreases when an existing dial rule is deleted.
BuildDuration	This counter represents the time in seconds that it took to build the last configuration files.
BuildSignCount	This counter represents the number of security-enabled phone devices for which the configuration file was digitally signed with the Cisco Unified CallManager server key in the last build of all the configuration files. This counter also updates while processing security-enabled phone device change notifications.
BuildSoftKeyCount	This counter represents the number of softkeys that were processed in the last build of the configuration files. This counter increments when a new softkey is added and decrements when an existing softkey is deleted.
BuildUnitCount	This counter represents the number of gateways that were processed in the last build of all the configuration files. This counter also updates while processing unit change notifications. The counter increases when a new gateway is added and decreases when an existing gateway is deleted.

Table 23-29 *Cisco TFTP Server (continued)*

Counters	Counter Descriptions
ChangeNotifications	This counter represents the total number of all the Cisco Unified CallManager database change notifications that the TFTP server received. Each time that a device configuration is updated in Cisco Unified CallManager Administration, the TFTP server gets sent a database change notification to rebuild the XML file for the updated device.
DeviceChangeNotifications	This counter represents the number of times that the TFTP server received database change notification to create, update, or delete configuration files for devices.
DialruleChangeNotifications	This counter represents the number of times that the TFTP server received database change notification to create, update, or delete configuration files for dial rules.
EncryptCount	This counter represents the number of configuration files that were encrypted. This counter gets updated each time a configuration file is successfully encrypted
GKFoundCount	This counter represents the number of GK files that were found in the cache. This counter gets updated each time a GK file is found in the cache
GKNotFoundCount	This counter represents the number of GK files that were not found in the cache. This counter gets updated each time a request to get a GK file results in the cache not finding it
HeartBeat	This counter represents the heartbeat of the TFTP server. This incremental count indicates that the TFTP server is up and running. If the count does not increase, this means that the TFTP server is down.
HttpConnectRequests	This counter represents the number of clients that are currently requesting the HTTP GET file request.
HttpRequests	This counter represents the total number of file requests (such as requests for XML configuration files, phone firmware files, audio files, and so on.) that the HTTP server handled. This counter represents the sum total of the following counters since the HTTP service started: RequestsProcessed, RequestsNotFound, RequestsOverflow, RequestsAborted, and RequestsInProgress.
HttpRequestsAborted	This counter represents the total number of HTTP requests that the HTTP server. canceled (aborted) unexpectedly. Requests could get aborted if the requesting device cannot be reached (for instance, the device lost power) or if the file transfer was interrupted due to network connectivity problems.
HttpRequestsNotFound	This counter represents the total number of HTTP requests where the requested file was not found. When the HTTP server does not find the requested file, a message gets sent to the requesting device.
HttpRequestsOverflow	This counter represents the total number of HTTP requests that were rejected when the maximum number of allowable client connections was reached. The requests may have arrived while the TFTP server was building the configuration files or because of some other resource limitation. The Cisco TFTP advanced service parameter, Maximum Serving Count, sets the maximum number of allowable connections.
HttpRequestsProcessed	This counter represents the total number of HTTP requests that the HTTP server. successfully processed.
HttpServedFromDisk	This counters represents the number of requests that the HTTP server completed with the files that are on disk and not cached in memory.

Table 23-29 *Cisco TFTP Server (continued)*

Counters	Counter Descriptions
LDFoundCount	This counter represents the number of LD files that were found in the cache. This counter gets updated each time a LD file is found in cache memory.
LDNotFoundCount	This counter represents the number of LD files that were not found in cache memory. This counter gets updated each time a request to get an LD file results in the cache not finding it.
MaxServingCount	This counter represents the maximum number of client connections that the TFTP can serve simultaneously. The Cisco TFTP advanced service parameter, Maximum Serving Count, sets this value.
Requests	This counter represents the total number of file requests (such as requests for XML configuration files, phone firmware files, audio files, and so on.) that the TFTP server handles. This counter represents the sum total of the following counters since the TFTP service started: RequestsProcessed, RequestsNotFound, RequestsOverflow, RequestsAborted, and RequestsInProgress.
RequestsAborted	This counter represents the total number of TFTP requests that the TFTP server canceled (aborted) unexpectedly. Requests could be aborted if the requesting device cannot be reached (for instance, the device lost power) or if the file transfer was interrupted due to network connectivity problems.
RequestsInProgress	This counter represents the number of file requests that the TFTP server currently is processing. This counter increases for each new file request and decreases for each file request that is completed. This counter indicates the current load of the TFTP server.
RequestsNotFound	This counter represents the total number of TFTP requests where the requested file was not found. When the TFTP server does not find the requested file, a message gets sent to the requesting device.
RequestsOverflow	This counter represents the total number of TFTP requests that were rejected because the maximum number of allowable client connections was exceeded, because requests arrived while the TFTP server was building the configuration files, or because of some other resource limitation. The Cisco TFTP advanced service parameter, Maximum Serving Count, sets the maximum number of allowable connections.
RequestsProcessed	This counter represents the total number of TFTP requests that the TFTP server successfully processed.
SegmentsAcknowledged	This counter represents the total number of data segments that the client devices acknowledged. Files get sent to the requesting device in data segments of 512 bytes, and for each 512-byte segment, the device sends the TFTP server an acknowledgment message. Each additional data segment gets sent upon receipt of the acknowledgment for the previous data segment until the complete file is successfully transmitted to the requesting device.
SegmentsFromDisk	This counter represents the number of data segments that the TFTP server reads from the files on disk, while serving files.
SegmentSent	This counter represents the total number of data segments that the TFTP server sent. Files get sent to the requesting device in data segments of 512 bytes.
SEPFoundCount	This counter represents the number of SEP files that were successfully found in the cache. This counter gets updated each time a SEP file is found in the cache.

Table 23-29 Cisco TFTP Server (continued)

Counters	Counter Descriptions
SEPNotFoundCount	This counter represents the number of SEP files that were not found in the cache. This counter gets updated each time a request to get a SEP file produces a not found in cache memory result.
SIPFoundCount	This counter represents the number of SIP files that were successfully found in the cache. This counter gets updated each time a SIP file is found in the cache
SIPNotFoundCount	This counter represents the number of SIP files that were not found in the cache. This counter gets updated each time a request to get a SIP file produces a not found in cache memory result.
SoftkeyChangeNotifications	This counter represents the number of times that the TFTP server has received database change notification to create, update, or delete configuration files for softkeys.
UnitChangeNotifications	This counter represents the number of times that the TFTP server received database change notification to create, update, or delete gateway-related configuration files.

Cisco Tomcat Connector

The Tomcat Hypertext Transport Protocol (HTTP)/HTTP Secure (HTTPS) Connector object provides information about Tomcat connectors. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco Unified CallManager related web pages are accessed. The Secure Socket Layer (SSL) status of the URLs for web applications provides the basis for the instance name for each Tomcat HTTP Connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL. [Table 23-30](#) contains information on the Tomcat HTTP connector counters.

Table 23-30 Cisco Tomcat Connector

Counters	Counter Description
Errors	This counter represents the total number of HTTP errors (for example, 401 Unauthorized) that the connector encountered. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco Unified CallManager related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.
MBytesReceived	This counter represents the amount of data that the connector received. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco Unified CallManager related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.

Table 23-30 *Cisco Tomcat Connector (continued)*

Counters	Counter Description
MBytesSent	This counter represents the amount of data that the connector sent. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco Unified CallManager related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.
Requests	This counter represents the total number of request that the connector handled. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco CallManager related windows s are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.
ThreadsTotal	This counter represents the current total number of request processing threads, including available and in-use threads, for the connector. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco Unified CallManager related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.
ThreadsMax	This counter represents the maximum number of request processing threads for the connector. Each incoming request on a Cisco Unified CallManager related window requires a thread for the duration of that request. If more simultaneous requests are received than the currently available request processing threads can handle, additional threads will be created up to the configured maximum shown in this counter. If still more simultaneous requests are received, they accumulate within the server socket that the connector created, up to an internally specified maximum number. Any further simultaneous requests will receive connection refused messages until resources are available to process them. A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The Connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco Unified CallManager related windows are accessed. The Secure Socket Layer (SSL) status of the URLs for the web application provides basis for the instance name for each Tomcat HTTP connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.
ThreadsBusy	This counter represents the current number of busy/in-use request processing threads for the connector. A Tomcat Connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when web pages that are related to Cisco Unified CallManager are accessed. The Secure Sockets Layer (SSL) status of the URLs for the web application provides the basis for the instance name for each Tomcat connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.

Cisco Tomcat JVM

The Cisco Tomcat Java Virtual Machine (JVM) object provides information about the Tomcat JVM, which represents, among other things, a pool of common resource memory that Cisco Unified CallManager related web applications such as Cisco Unified CallManager Administration, Cisco Unified CallManager Serviceability, and more use. [Table 23-31](#) contains information on the Tomcat JVM counters.

Table 23-31 Tomcat JVM

Counters	Counter Description
KBytesMemoryFree	This counter represents the amount of free dynamic memory block (heap memory) in the Tomcat Java Virtual Machine. The dynamic memory block stores all objects that Tomcat and its web applications such as Cisco Unified CallManager Administration and Cisco Unified CallManager Serviceability create. When the amount of free dynamic memory is low, more memory gets automatically allocated, and total memory size (represented by the KbytesMemoryTotal counter) increases but only up to the maximum (represented by the KbytesMemoryMax counter). You can determine the amount of memory in use by subtracting KBytesMemoryFree from KbytesMemoryTotal.
KBytesMemoryMax	This counter represents the amount of free dynamic memory block (heap memory) in the Tomcat Java Virtual Machine. The dynamic memory block stores all objects that Tomcat and its web applications such as Cisco Unified CallManager Administration and Cisco Unified CallManager Serviceability create.
KBytesMemoryTotal	This counter represents the current total dynamic memory block size, including free and in-use memory, of Tomcat Java Virtual Machine. The dynamic memory block stores all objects that Tomcat and its web applications such as Cisco Unified CallManager Administration and Cisco Unified CallManager Serviceability create.

Cisco Tomcat Web Application

The Cisco Tomcat Web Application object provides information about how to running Cisco Unified CallManager web applications. The URLs for the web application provide basis for the instance name for each Tomcat Web Application. For example, Cisco Unified CallManager Administration (<https://<IP Address>:8443/ccmadmin>) gets identified by ccmadmin, Cisco Unified CallManager Serviceability gets identified by ccmservice, Cisco Unified CallManager User Options gets identified by ccmuser, and URLs that do not have an extension, such as <https://<IP Address>:8443> or <http://<IP Address>:8080>, get identified by _root. [Table 23-32](#) contains information on the Tomcat Web Application counters.

Table 23-32 Tomcat Web Application

Counters	Counter Description
Errors	This counter represents the total number of HTTP errors (for example, 401 Unauthorized) that a Cisco Unified CallManager related web application encountered. The URLs for the web application provide the basis instance name for each Tomcat Web Application. For example, Cisco Unified CallManager Administration (<a href="https://<IP Address>:8443/ccmadmin">https://<IP Address>:8443/ccmadmin) gets identified by ccmadmin, Cisco Unified CallManager Serviceability gets identified by ccmservice, Cisco Unified CallManager User Options gets identified by ccmuser, and URLs that do not have an extension, such as <a href="https://<IP Address>:8443">https://<IP Address>:8443 or <a href="http://<IP Address>:8080">http://<IP Address>:8080 , get identified by _root.
Requests	This counter represents the total number of requests that the web application handles. Each time that a web application is accessed, its Requests counter increments accordingly. The URLs for the web application provide the basis instance name for each Tomcat Web Application. For example, Cisco Unified CallManager Administration (<a href="https://<IP Address>:8443/ccmadmin">https://<IP Address>:8443/ccmadmin) gets identified by ccmadmin, Cisco Unified CallManager Serviceability gets identified by ccmservice, Cisco Unified CallManager User Options gets identified by ccmuser, and URLs that do not have an extension, such as <a href="https://<IP Address>:8443">https://<IP Address>:8443 or <a href="http://<IP Address>:8080">http://<IP Address>:8080 , get identified by _root.
SessionsActive	This counter represents the number of sessions that the web application currently has active (in use). The URLs for the web application provide the basis instance name for each Tomcat Web Application. For example, Cisco Unified CallManager Administration (<a href="https://<IP Address>:8443/ccmadmin">https://<IP Address>:8443/ccmadmin) gets identified by ccmadmin, Cisco Unified CallManager Serviceability gets identified by ccmservice, Cisco Unified CallManager User Options gets identified by ccmuser, and URLs that do not have an extension, such as <a href="https://<IP Address>:8443">https://<IP Address>:8443 or <a href="http://<IP Address>:8080">http://<IP Address>:8080 , get identified by _root.

Cisco Transcode Device

The Cisco Transcode Device object provides information about registered Cisco transcoding devices. [Table 23-33](#) contains information on Cisco transcoder device counters.

Table 23-33 *Cisco Transcode Device*

Counters	Counter Descriptions
OutOfResources	This counter represents the total number of times that an attempt was made to allocate a transcoder resource from a transcoder device and failed; for example, because all resources were already in use.
ResourceActive	This counter represents the number of transcoder resources that are currently in use (active) for a transcoder device. Each transcoder resource uses two streams.
ResourceAvailable	This counter represents the total number of resources that are not active and are still available to be used now for a transcoder device. Each transcoder resource uses two streams.
ResourceTotal	This counter represents the total number of transcoder resources that a transcoder device provided. This counter equals the sum of the counters ResourceActive and ResourceAvailable.

Cisco Video Conference Bridge

The Cisco Video Conference Bridge object provides information about registered Cisco video conference bridge devices. [Table 23-34](#) contains information on Cisco video conference bridge device counters.

Table 23-34 *Cisco Video Conference Bridge*

Counters	Counter Descriptions
ConferencesActive	This counter represents the total number of video conferences that are currently active (in use) on a video conference bridge device. The system specifies a conference as active when the first call connects to the bridge.
ConferencesAvailable	This counter represents the number of video conferences that are not active and are still available on a video conference device.
ConferencesCompleted	This counter represents the total number of video conferences that have been allocated and released on a video conference device. A conference starts when the first call connects to the bridge. The conference completes when the last call disconnects from the bridge.
ConferencesTotal	This counter represents the total number of video conferences that are configured for a video conference device.
OutOfConferences	This counter represents the total number of times an attempt was made to initiate a video conference from a video conference device and failed because the device already had the maximum number of active conferences allowed (as specified by the TotalConferences counter).

Table 23-34 *Cisco Video Conference Bridge (continued)*

Counters	Counter Descriptions
OutOfResources	This counter represents the total number of times that an attempt was made to allocate a conference resource from a video conference device and failed, for example, because all resources were already in use.
ResourceActive	This counter represents the total number of resources that are currently active (in use) on a video conference bridge device. One resource gets used per participant.
ResourceAvailable	This counter represents the total number of resources that are not active and are still available on a device to handle additional participants for a video conference bridge device.
ResourceTotal	This counter represents the total number of resources that are configured on a video conference bridge device. One resource gets used per participant.

Cisco WebDialer

The Cisco WebDialer object provides information about the Cisco Unified WebDialer application and the Redirector servlet. [Table 23-35](#) contains information on the Cisco WebDialer counters.

Table 23-35 *Cisco WebDialer*

Counters	Counter Descriptions
CallsCompleted	This counter represents the number of Make Call and End Call requests that the Cisco Unified WebDialer application successfully completed.
CallsFailed	This counter represents the number of Make Call and End Call requests that were unsuccessful.
RedirectorSessionsHandled	This counter represents the total number of HTTP sessions that the Redirector servlet handled since the last service startup.
RedirectorSessionsInProgress	This counter represents the number of HTTP sessions that are currently being serviced by the Redirector servlet.
RequestsCompleted	This counter represents the number of Make Call and End Call requests that the WebDialer servlet has successfully completed.
RequestsFailed	This counter represents the number of Make Call and End Call requests that failed.
SessionsHandled	This counter represents the total number of CTI sessions that the Cisco WebDialer servlet handled since the last service startup.
SessionsInProgress	This counter represents the number of CTI sessions that the Cisco WebDialer servlet is currently servicing.

Cisco WSM Connector

The WSM object provides information on WSMConnectors that are configured on Cisco Unified CallManager. Each WSMConnector represents a physical Motorola WSM device. [Table 23-36](#) contains information on the Cisco WSM Connector counters.

Table 23-36 Cisco WSM Connector

Counters	Counter Description
CallsActive	This counter represents the number of calls that are currently active (in use) on the WSMConnector device.
CallsAttempted	This counter represents the number of calls that have been attempted on the WSMConnector device, including both successful and unsuccessful call attempts.
CallsCompleted	This counter represents the number of calls that are connected (a voice path was established) through the WSMConnector device. The counter increments when the call terminates.
CallsInProgress	This counter represents the number of calls that are currently in progress on the WSMConnector device. This includes all active calls. When the number of CallsInProgress equals the number of CallsActive, this indicates that all calls are connected.
DMMSRegistered	This counter represents the number of DMMS subscribers that are registered to the WSM.

Database Change Notification Client

The Database Change Notification Client object provides information on change notification clients. [Table 23-37](#) contains information on the Database Change Notification Client counters.

Table 23-37 Database Change Notification Client

Counters	Counter Descriptions
MessagesProcessed	This counter represents the number of database change notifications that have been processed. This counter refreshes every 15 seconds.
MessagesProcessing	This counter represents the number of change notification messages that are currently being processed or are waiting to be processed in the change notification queue for this client. This counter refreshes every 15 seconds.
QueueHeadPointer	This counter represents the head pointer to the change notification queue. The head pointer acts as the starting point in the change notification queue. To determine the number of notifications in the queue, subtract the head pointer value from the tail pointer value. By default, this counter refreshes every 15 seconds.
QueueMax	This counter represents the largest number of change notification messages that will be processed for this client. This counter remains cumulative since the last restart of the Cisco Database Layer Monitor service.
QueueTailPointer	This counter represents the tail pointer to the change notification queue. The tail pointer represents the ending point in the change notification queue. To determine the number of notifications in the queue, subtract the head pointer value from the tail pointer value. By default, this counter refreshes every 15 seconds.
TablesSubscribed	This counter represents the number of tables in which this client has subscribed.

Database Change Notification Server

The Database Change Notification Server object provides information on different change-notification-related statistics. [Table 23-37](#) contains information on the Database Change Notification Server counters.

Table 23-38 *Database Change Notification Server*

Counter	Counter Descriptions
Clients	This counter represents the number of change notification clients (services/servlets) that have subscribed for change notification.
QueuedRequestsInDB	This counter represents the number of change notification records that are in the DBCNQueue (Database Change Notification Queue) table via direct TCP/IP connection (not queued in shared memory). This counter refreshes every 15 seconds.
QueuedRequestsInMemory	This counter represents the number of change notification requests that are queued in the DBCNQueue (Database Change Notification Queue) table in shared memory (rather than via direct TCP/IP connection).

Database Change Notification Subscription

The Database Change Notification Subscription object displays the names of tables where the client will receive Change Notifications.

The SubscribedTable object displays the table with the service or servlet that will receive change notifications. Because the counter does not increment, this display occurs for informational purposes only.

Database Local DSN

The Database Local Data Source Name (DSN) object and LocalDSN counter provide the DSN information for the local machine. [Table 23-39](#) contains information on the Database local DSN.

Table 23-39 *Database Local Data Source Name*

Counters	Counter Descriptions
CcmDbSpace_Used	This counter represents the amount of Ccm DbSpace that is being consumed.
CcmtempDbSpace_Used	This counter represents the amount of Ccmtemp DbSpace that is being consumed.
LocalDSN	This counter represents the data source name (DSN) that is being referenced from the local machine.
RootDbSpace_Used	This counter represents the amount of RootDbSpace that is being consumed.

DB User Host Information Counters

The DB User Host Information object provides information on DB User Host.

The DB:User:Host Instance object displays the number of connections that are present for each instance of DB:User:Host.

Enterprise Replication DBSpace Monitors

The enterprise replication DBSpace monitors object displays the usage of various ER DbSpaces.

[Table 23-40](#) contains information on the enterprise replication DB monitors.

Table 23-40 Enterprise Replication DBSpace Monitors

Counters	Counter Descriptions
ERDbSpace_Used	This counter represents the amount of enterprise replication DbSpace that was consumed.
ERSBDbSpace_Used	This counter represents the amount of ERDbSpace that was consumed.

Enterprise Replication Perfmon Counters

The Enterprise Replication Perfmon Counter object provides information on the various replication counters.

The ServerName:ReplicationQueueDepth counter displays the server name followed by the replication queue depth.

IP

The IP object provides information on the IP statistics on your system. [Table 23-41](#) contains information on the IP counters.

Table 23-41 IP

Counters	Counter Descriptions
Frag Creates	This counter represents the number of IP datagrams fragments that have been generated at this entity.
Frag Fails	This counter represents the number of IP datagrams that were discarded at this entity because the datagrams could not be fragmented, such as datagrams where the Do not Fragment flag was set.
Frag OKs	This counter represents the number of IP datagrams that were successfully fragmented at this entity.
In Delivers	This counter represents the number of input datagrams that were delivered to IP user protocols. This includes Internet Control Message Protocol (ICMP).

Table 23-41 *IP (continued)*

Counters	Counter Descriptions
In Discards	This counter represents the number of input IP datagrams where no problems were encountered, but which were discarded. Lack of buffer space provides one possible reason. This counter does not include any datagrams that were discarded while awaiting reassembly.
In HdrErrors	This counter represents the number of input datagrams that were discarded with header errors. This includes bad checksums, version number mismatch, other format errors, time-to-live exceeded, and other errors that were discovered in processing their IP options.
In Receives	This counter represents the number of input datagrams that were received from all network interfaces. This counter includes datagrams that were received with errors
In UnknownProtos	This counter represents the number of locally addressed datagrams that were received successfully but discarded because of an unknown or unsupported protocol.
InOut Requests	This counter represents the number of incoming IP datagrams that were received and the number of outgoing IP datagrams that were sent.
Out Discards	This counter represents the number of output IP datagrams that were not transmitted and were discarded. Lack of buffer space provides one possible reason.
Out Requests	This counter represents the total number of IP datagrams that local IP user-protocols (including ICMP) supply to IP in requests transmission. This counter does not include any datagrams that were counted in ForwDatagrams.
Reasm Fails	This counter represents the number of IP reassembly failures that the IP reassembly algorithm detected, including time outs, errors, and so on. This counter does not represent the discarded IP fragments because some algorithms, such as the algorithm in RFC 815, can lose track of the number of fragments because it combines them as they are received.
Reasm OKs	This counter represents the number of IP datagrams that were successfully reassembled.
Reasm Reqds	This counter represents the number of IP fragments that were received that required reassembly at this entity.

Memory

The memory object provides information about the usage of physical memory and swap memory on the server. [Table 23-42](#) contains information on memory counters.

Table 23-42 **Memory**

Counters	Counter Descriptions
% Mem Used	This counter displays the system physical memory utilization as a percentage. The value of this counter equals (Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes) / Total KBytes, which also corresponds to the Used KBytes/Total KBytes.
% Page Usage	This counter represents the percentage of active pages.
% VM Used	This counter displays the system virtual memory utilization as a percentage. The value of this counter equals (Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes + Used Swap KBytes) / (Total KBytes + Total Swap KBytes), which also corresponds to Used VM KBytes/Total VM KBytes.
Buffered KBytes	This counter represents the capacity of buffers in your system in kilobytes.
Cached KBytes	This counter represents the amount of cached memory in kilobytes.
Free KBytes	This counter represents the total amount of memory that is available in your system in kilobytes.
Free Swap KBytes	This counter represents the amount of free swap space that is available in your system in kilobytes.
Pages	This counter represents the number of pages that the system paged in from the disk plus the number of pages that the system paged out to the disk.
Pages Input	This counter represents the number of pages that the system paged in from the disk.
Pages Output	This counter represents the number of pages that the system paged out to the disk.
Shared KBytes	This counter represents the amount of shared memory in your system in kilobytes.
Total KBytes	This counter represents the total amount of memory in your system in kilobytes.
Total Swap KBytes	This counter represents the total amount of swap space in your system in kilobytes.
Total VM KBytes	This counter represents the total amount of system physical and memory and swap space (Total Kbytes + Total Swap Kbytes) that is in use in your system in kilobytes.
Used KBytes	This counter represents the amount of system physical memory that is in use on the system in kilobytes. The value of the Used KBytes counter equals Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes. The Used KBytes value differs from the Linux term that displays in the top or free command output. The Used value that displays in the top or free command output equals the difference in Total KBytes - Free KBytes and also includes the sum of Buffers KBytes and Cached KBytes.
Used Swap KBytes	This counter represents the amount of swap space that is in use on your system in kilobytes.
Used VM KBytes	This counter represents the system physical memory and the amount of swap space that is in use on your system in kilobytes. The value equals Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes + Used Swap KBytes. This corresponds to Used Mem KBytes + Used Swap KBytes.

Network Interface

The network interface object provides information about the network interfaces on the system. [Table 23-43](#) contains information on network interface counters.

Table 23-43 **Network Interface**

Counters	Counter Descriptions
Rx Bytes	This counter represents the number of bytes, including framing characters, that were received on the interface.
Rx Dropped	This counter represents the number of inbound packets that were chosen to be discarded even though no errors had been detected. This prevents the packet from being delivered to a higher layer protocol. Discarding packets to free up buffer space provides one reason.
Rx Errors	This counter represents the number of inbound packets (packet-oriented interfaces) and the number of inbound transmission units (character-oriented or fixed-length interfaces) that contained errors that prevented them from being deliverable to a higher layer protocol.
Rx Multicast	This counter represents the number of multicast packets that were received on this interface.
Rx Packets	This counter represents the number of packets that this sublayer delivered to a higher sublayer. This does not include the packets that were addressed to a multicast or broadcast address at this sublayer.
Total Bytes	This counter represents the total number of received (Rx) bytes and transmitted (Tx) bytes.
Total Packets	This counter represents the total number of Rx packets and Tx packets.
Tx Bytes	This counter represents the total number of octets, including framing characters, that were transmitted out from the interface.
Tx Dropped	This counter represents the number of outbound packets that were chosen to be discarded even though no errors were detected. This action prevents the packet from being delivered to a higher layer protocol. Discarding a packet to free up buffer space represents one reason.
Tx Errors	This counter represents the number of outbound packets (packet-oriented interfaces) and the number of outbound transmission units (character-oriented or fixed-length interfaces) that could not be transmitted because of errors.
Tx Packets	This counter represents the total number of packets that the higher level protocols requested for transmission, including those that were discarded or not sent. This does not include packets that were addressed to a multicast or broadcast address at this sublayer.
Tx QueueLen	This counter represents the length of the output packet queue (in packets).

Number of Replicates Created and State of Replication

The Number of Replicates Created and State of Replication object provides information about the replication state on the system. [Table 23-44](#) contains information on replication counters.

Table 23-44 *Number of Replicates Created and State of Replication*

Counters	Counter Descriptions
Number of Replicates Created	This counter represents the number of replicates created by Informix database for the DB tables. There should be one replicate for every table.
Replicate_State	This counter represents the state of replication. Possible values includes: • 0 (Not Started)—No Subscribers exist, or the Database Layer Monitor service is not running and has not been running since the subscriber was installed. • 1 (Started)—Replication is currently being setup. • 2 (Finished)—Replication setup was completed and is working. • 3 (Broken)—Replication failed during setup and is not working.

Partition

The partition object provides information about the file system and its usage in the system. [Table 23-45](#) contains information on partition counters.

Table 23-45 *Partition*

Counters	Counter Descriptions
% CPU Time	This counter represents the percentage of CPU time that is dedicated to handling I/O requests that were issued to the disk.
% Used	This counter represents the percentage of disk space that is in use on this file system.
Await Read Time	This counter represents the average time, measured in milliseconds, for Read requests that are issued to the device to be served.
Await Time	This counter represents the average time, measured in milliseconds, for I/O requests that were issued to the device to be served. This includes the time spent by the requests in queue and the time spent servicing them.
Await Write Time	This counter represents the average time, measured in milliseconds, for write requests that are issued to the device to be served.
Queue Length	This counter represents the average queue length for the requests that were issued to the disk.
Read Bytes Per Sec	This counter represents the amount of data in bytes per second that was read from the disk.
Total Mbytes	This counter represents the amount of total disk space that is on this file system in megabytes.

Table 23-45 *Partition (continued)*

Counters	Counter Descriptions
Used Mbytes	This counter represents the amount of disk space that is in use on this file system in megabytes.
Write Bytes Per Sec	This counter represents the amount of data that was written to the disk in bytes per second.

Process

The process object provides information about the processes that are running on the system. [Table 23-46](#) contains information on process counters.

Table 23-46 *Process*

Counters	Counter Descriptions
% CPU Time	This counter, which is expressed as a percentage of total CPU time, represents the tasks share of the elapsed CPU time since the last update.
% MemoryUsage	This counter represents the percentage of physical memory that a task is currently using.
Data Stack Size	This counter represents the stack size for task memory status.
Nice	This counter represents the nice value of the task. A negative nice value indicates that the process has a higher priority while a positive nice value indicates that the process has a lower priority. If the nice value equals zero, do not adjust the priority when you are determining the dispatchability of a task.
Page Fault Count	This counter represents the number of major page faults that a task encountered that required the data to be loaded into memory.
PID	This counter displays the task-unique process ID. The ID periodically wraps, but the value will never equal zero.
Process Status	This counter displays the process status: • 0—Running • 1—Sleeping • 2—Uninterruptible disk sleep • 3—Zombie • 4—Stopped • 5—Paging • 6—Unknown
Shared Memory Size	This counter displays the amount of shared memory (KB) that a task is using. Other processes could potentially share the same memory.
STime	This counter displays amount of system time (STime), measured in jiffies, that this process has scheduled in kernel mode. A jiffy corresponds to a unit of CPU time and gets used as a base of measurement. One second consists of 100 jiffies.

Table 23-46 *Process (continued)*

Counters	Counter Descriptions
Thread Count	This counter displays the number of threads that are currently grouped with a task. A negative value (-1) indicates that this counter is currently not available. This happens when thread statistics (which includes all performance counters in the Thread object as well as the Thread Count counter in the Process object) are turned off because the system total processes and threads exceeded the default threshold value.
Total CPU Time Used	This counter displays the total CPU time in jiffies that the task used in user mode and kernel mode since the start of the task. A jiffy corresponds to a unit of CPU time and gets used as a base of measurement. One second consists of 100 jiffies.
UTime	This counter displays the time, measured in jiffies, that a task has scheduled in user mode.
VmData	This counter displays the virtual memory usage of the heap for the task in kilobytes (KB).
VmRSS	This counter displays the virtual memory (Vm) resident set size (RSS) that is currently in physical memory in kilobytes (KB). This includes the code, data, and stack.
VmSize	This counter displays the total virtual memory usage for a task in kilobytes (KB). It includes all code, data, shared libraries, and pages that have been swapped out: Virtual Image = swapped size + resident size.

Processor

The processor object provides information on different processor time usage in percentages. [Table 23-47](#) contains information on processor counters.

Table 23-47 *Processor*

Counters	Counter Descriptions
% CPU Time	This counter displays the processors share of the elapsed CPU time, excluding idle time, since the last update. This share gets expressed as a percentage of total CPU time.
Idle Percentage	This counter displays the percentage of time that the processor is in the idle state and did not have an outstanding disk I/O request.
IOwait Percentage	This counter represents the percentage of time that the processor is in the idle state while the system had an outstanding disk I/O request.
Irq Percentage	This counter represents the percentage of time that the processor spends executing the interrupt request that is assigned to devices, including the time that the processor spends sending a signal to the computer.
Nice Percentage	This counter displays the percentage of time that the processor spends executing at the user level with nice priority.
Softirq Percentage	This counter represents the percentage of time that the processor spends executing the soft IRQ and deferring task switching to get better CPU performance.

Table 23-47 *Processor (continued)*

Counters	Counter Descriptions
System Percentage	This counter displays the percentage of time that the processor is executing processes in system (kernel) level.
User Percentage	This counter displays the percentage of time that the processor is executing normal processes in user (application) level.

System

The System object provides information on file descriptors on your system. [Table 23-48](#) contains information on system counters

Table 23-48 *System*

Counters	Counter Descriptions
Allocated FDs	This counter represents the total number of allocated file descriptors.
Being Used FDs	This counter represents the number of file descriptors that are currently in use in the system.
Freed FDs	This counter represents the total number of allocated file descriptors on the system that are freed.
Max FDs	This counter represents the maximum number of file descriptors that are allowed on the system.
Total CPU Time	This counter represents the total time in jiffies that the system has been up and running.
Total Processes	This counter represents the total number of processes on the system.
Total Threads	This counter represents the total number of threads on the system.

TCP

The TCP object provides information on the TCP statistics on your system. [Table 23-49](#) contains information on the TCP counters.

Table 23-49 *TCP*

Counters	Counter Description
Active Opens	This counter displays the number of times that the TCP connections made a direct transition to the SYN-SENT state from the CLOSED state.
Attempt Fails	This counter displays the number of times that the TCP connections have made a direct transition to the CLOSED state from either the SYN-RCVD state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYS-RCVD state.
Curr Estab	This counter displays the number of TCP connections where the current state is either ESTABLISHED or CLOSE- WAIT.

Table 23-49 TCP (continued)

Counters	Counter Description
Estab Resets	This counter displays the number of times that the TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
In Segs	This counter displays the total number of segments that were received, including those received in error. This count only includes segments that are received on currently established connections.
InOut Segs	This counter displays the total number of segments that were sent and the total number of segments that were received.
Out Segs	This counter displays the total number of segments that were sent. This count only includes segments that are sent on currently established connections, but excludes retransmitted octets.
Passive Opens	This counter displays the number of times that TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
RetransSegs	This counter displays the total number of segments that were retransmitted because the segment contains one or more previously transmitted octets.

Thread

The Thread object provides a list of running threads on your system. [Table 23-50](#) contains information on the Thread counters.

Table 23-50 Thread

Counters	Counter Description
% CPU Time	This counter displays the threads share of the elapsed CPU time since the last update. This counter expresses the share as a percentage of the total CPU time.
PID	This counter displays the threads leader process ID.

Using RTMT for Performance Monitoring

RTMT displays performance information of all Cisco Unified CallManager components in a cluster. The tool integrates with Cisco Unified CallManager administration and serviceability software. RTMT provides alert notification for troubleshooting performance. It also monitors various aspects of Cisco Unified CallManager performance by periodically polling performance counter values. Refer to “Displaying a Counter Description” section in the *Cisco CallManager Serviceability Administration Guide, Release 5.0(4)*, for examples on displaying perfmon counters in a chart or table format.

Perfmon monitoring allows you to perform the following tasks:

- From the Cisco Unified CallManager cluster, monitor performance counters including Cisco Unified CallManager nodes, TFTP servers, and database servers.
- Continuously monitor a set of preconfigured objects and receive notification in the form of an e-mail message.

- Associate counter threshold settings to alert notification. An e-mail or popup message provides notification to the administrator.
- Save and restore settings, such as counters being monitored, threshold settings, and alert notifications, for customized troubleshooting tasks.
- Display up to six perfmon counters in one chart for performance comparisons.

RTMT displays performance counters in chart or table format. Chart format looks like a miniature window of information. Up to six charts display in the RTMT performance monitoring pane for each category tab that you create. You can display a particular counter by double clicking the counter in the perfmon monitoring pane. Because chart view represents the default, you configure the performance counters to display in table format when you create a category.

You can remove a counter chart (table entry) with the Remove Chart/TableEntry menu item in the Perfmon menu in the menu bar.

**Tip**

The polling rate in each precanned monitoring window remains fixed, and the default value specifies 30 seconds. If the collecting rate of the AMC (Alert Manager and Collector) changes for Cisco Unified CallManager Administration service parameters, the polling rate in the precanned window also updates. In addition, the local time of the RTMT client application and not the backend server time, provides the basis for the time stamp in each chart.

See the following sections for configuration options in the RTMT perfmon monitoring pane:

- [Category Tabs, page 23-60](#)
- [Sample Rate, page 23-61](#)
- [Adding Counters to Monitor, page 23-61](#)
- [Alert Notification for Counters, page 23-61](#)

Category Tabs

A category comprises monitored performance counters. A tab in the RTMT monitoring pane contains the category name. All performance counters that are monitored in this tab belong to a category. The system polls the performance counters in the tab at the same rate, with each category configured to have its own polling rate.

You can create custom categories in the RTMT monitoring pane to view information that helps you troubleshoot specific performance or device problems. If your Cisco Unified CallManager system is experiencing performance problems with specific objects, create custom categories to monitor the performance of the counters within the object. If the system is experiencing problems with specific devices, create custom categories to monitor the devices within the cluster. In addition, you can create alert notifications for counters and gateways in these custom categories.

To create custom categories, you add a new category tab. When the tab is created, you specify the specific performance counters, devices, and alerts within that tab and then save your custom category by using Profile.

Sample Rate

The Cisco Unified CallManager software polls counters, devices, and gateway ports to gather status information. In the RTMT monitoring pane, you configure the polling intervals for the performance counters, devices, and gateway ports for each category tab that you create.

**Note**

High-frequency polling rate affects Cisco Unified CallManager performance. The minimum polling rate for monitoring a performance counter in chart view equals 5 seconds; the minimum rate for monitoring a performance counter in table view equals 1 second. The default for both specifies 10 seconds.

Adding Counters to Monitor

To troubleshoot system performance problems, you add the counter that is associated with the perfmon object to the RTMT performance monitoring pane, which displays a chart for the counter. Before you add counters, see the [“Category Tabs” section on page 23-60](#).

Category tabs contain up to six perfmon counter charts.

Alert Notification for Counters

Using the alert notification feature, Cisco Unified CallManager notifies you of system problems. Perform the following configuration setup to activate alert notifications for a system counter:

- From the RTMT Perfmon Monitoring pane, choose the system perfmon counter.
- Set up an e-mail or a message popup window for alert notification.
- Determine the threshold for the alert (for example, an alert activates when calls in progress exceed the threshold of over 100 calls or under 50 calls).
- Determine the frequency of the alert notification (for example, the alert occurs once or every hour).
- Determine the schedule for when the alert activates (for example, on a daily basis or at certain times of the day).

Zoom Counter

To get a closer look at performance monitors, zoom the monitor counter in the RTMT perfmon monitoring pane by highlighting the counter chart and choosing Zoom Chart in the Perfmon menu.

Counter Properties

Counter properties allow you to display a description of the counter and configure data-sampling parameters.

The Counter Property window contains the option to configure data samples for a counter. The performance counters that display in the RTMT performance monitoring pane contain green dots that represent samples of data over time. You can configure the number of data samples to collect and the

number of data points to show in the chart. After the data sample is configured, view the information by using the View All Data/View Current Data menu option to view all the data that a perfmon counter collected.

Understanding Perfmon Logs

The system logs the perfmon data whenever RTMT calls the LogPerfMon API. You can open the file log, which is compatible with the Windows Performance tool csv format, by using the Performance tool for analysis.

When you add new counters, RTMT changes the header to accommodate the new counters and logs the values correspondingly. When data is unavailable for an already existing counter (already added to header), RTMT inserts blank values in the file. If the character length of the new counters that are added is greater than 2000, the new file gets generated with all the counters.

The following file name format for the PerfMon Log applies:
PerfMonLog_<NodeName>_MM_DD_YYYY_hh_mm.csv.

The following lists comprises the perfmon counters that RTMT logs:

At System level

- Cisco Unified CallManager System Performance\QueueSignalsPresent 1-High
- Cisco Unified CallManager System Performance\QueueSignalsPresent 2-Normal
- Cisco Unified CallManager System Performance\QueueSignalsPresent 3-Low
- Cisco Unified CallManager System Performance\QueueSignalsPresent 4-Lowest
- Cisco Unified CallManager System Performance\QueueSignalsProcessed 1-High
- Cisco Unified CallManager System Performance\QueueSignalsProcessed 2-Normal
- Cisco Unified CallManager System Performance\QueueSignalsProcessed 3-Low
- Cisco Unified CallManager System Performance\QueueSignalsProcessed 4-Lowest

For each process that is running on the system

- Process\% Processor Time
- Process\ID Process
- Process\Private Bytes
- Process\Virtual Bytes

Additional Cisco Documentation

Troubleshooting Guide for Cisco Unified CallManager, Release 5.0(4)

Where to Find More Information

Related Topics

- [Real-Time Monitoring Tool](#), *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*
- [Real-Time Monitoring Configuration](#), *Cisco Unified CallManager New and Changed Information Guide, Release 5.1(1)*
- Trace Collection and Log Central in RTMT, *Cisco CallManager Serviceability Administration Guide, Release 5.0(4)*



PART 7

Cisco Unified CallManager CDR Analysis and Reporting Administration Guide





CDR Analysis and Reporting Overview

Cisco Unified CallManager Serviceability supports CDR Analysis and Reporting (CAR) under the Tools menu. CAR generates reports for Quality of Service, traffic, and billing information.



Note

CAR does not handle iDivert calls (feature that diverts calls to voice-messaging system) and treats them as normal calls. The part of the call after iDivert feature gets activated may not get charged to the correct party.

This chapter contains the following topics:

- [Understanding CDR Data, page 24-1](#)
- [Understanding CDR Analysis and Reporting, page 24-2](#)
- [CAR Administrators, Managers, and Users, page 24-5](#)
- [CAR System Settings, page 24-6](#)
- [CAR Reports, page 24-6](#)
- [CDR Search, page 24-12](#)
- [Internationalization for CDR Analysis and Reporting, page 24-14](#)
- [Web Browsers, page 24-15](#)
- [CDR Analysis and Reporting Configuration Checklist, page 24-15](#)
- [Related Topics, page 24-16](#)

Understanding CDR Data

Call detail records (CDR) detail the called number, the number that placed the call, the date and time that the call was started, the time that it connected, and the time that it ended. Call management records (CMRs, or diagnostic records) detail the jitter, lost packets, the amount of data sent and received during the call, and latency. CDR data comprises CDRs and CMRs collectively. A single call can result in the generation of several CDRs and CMRs. Cisco Unified CallManager records information regarding each call in CDRs and CMRs. CDRs and CMRs, known collectively as CDR data, serve as the basic information source for CAR.

The Cisco CDR Agent service transfers CDR and CMR files that Cisco Unified CallManager generates from the local host to the CDR repository node, where the CDR Repository Manager service runs over a SFTP connection. If the SFTP connection fails, the Cisco CDR Agent services continue to make connection attempts to the CDR repository node until a connection is made. The Cisco CDR Agent

service sends any accumulated CDR files when the connection to the CDR Repository node resumes. The CDR Repository Manager service maintains the CDR and CMR files, allocates the amount of disk space for use by CMRs and CDRs, sends the files to up to three configured destinations, and tracks the delivery result for each destination. CDR Analysis and Reporting (CAR) accesses the CDR/CMR files in the directory structure that the CDR Repository Manager service creates.

The high and low water mark settings that you configure specify percentages of the total disk space that are allocated for the CDR repository. Although the preserved folder under the CDR repository folder contributes to the high and low water mark percentages, Log Partition Monitoring never deletes the folder if the high water mark gets reached. If the high water mark gets reached, the CDR Repository Manager deletes processed CDR files until the low water mark is reached or all processed files are deleted, whichever comes first. If all processed CDR files are deleted but the low water mark has not been reached, the deletion stops. The CDRHighWaterMarkExceeded alarm gets generated until the system reaches the maximum disk allocation. If the maximum disk allocation gets reached, the system deletes undelivered files and files within the preservation duration, starting with the oldest files, until disk utilization falls below the high water mark. If you receive the CDRMaximumDiskSpaceExceeded alarm repeatedly for this scenario, either increase the disk allocation or lower the number of preservation days.

For more information on CDR services and alarms, refer to the *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)*.



Note

If you upgrade from Cisco Unified CallManager 4.x, Cisco Unified CallManager saves the CDRs in the CAR database to CSV files. The Data Migration Tool uses these CSV files to upgrade the CAR database. The system stores the CSV files in /common/download/windows/car. The system stores the pregenerated reports in /common/download/windows/pregenerated.

Because Cisco Unified CallManager 5.x does not use a CDR database to store CDR records as in previous releases, the CDR data does not migrate to the Cisco Unified CallManager 5.x system.

Understanding CDR Analysis and Reporting

You access CAR from the Tools menu of Cisco Unified CallManager Serviceability after you activate the appropriate services as described in the “Activating CAR” section in the *Cisco Unified CallManager CDR Analysis and Reporting Administration Guide, Release 5.0(4)*.

All CAR reports use CDR data. CAR processes the CDRs from flat files that the CDR Repository service has placed in the CDR repository folder structure. CAR processes CDRs at the scheduled time and frequency. By default, CDR data loads from midnight to 5 a.m. on a daily basis; however, you can set the loading time, interval, and duration as needed.

CAR retrieves information that is required for various reports from the CDRs and CMRs as well as from the Cisco Unified CallManager database.

Scheduling Reports

You can schedule CAR reports to generate automatically at a regular time. Each report that can be scheduled has its own report generation interval. You can make the report generation interval be daily, weekly, or monthly. Scheduling the Daily reports would schedule all the reports that have report generation intervals as Daily. Similarly, scheduling Weekly or Monthly reports would schedule the reports that have report generation intervals as weekly or monthly. You can also specify the time to keep a report before it gets automatically deleted.

By default, CAR uses the following report generation and deletion schedule:

- Daily reports run at 1 a.m. every day. These reports get purged after two days.
- Weekly reports run at 4 a.m. every Sunday. These reports get purged after four weeks.
- Monthly bill reports run at 3 a.m. on the first day of every month. These reports get purged after two months.
- Other monthly reports run at 2 a.m. on the first day of every month. These reports get purged after two months.

**Note**

For a list of reports and the default generation schedule, see the [“CAR Reports General Information” section on page 24-6](#).

For system monitoring, automatically generate various reports, such as QoS reports, and review them at regular intervals, perhaps every day if you have a very large system, or every week or every two weeks for smaller systems. QoS reports help you determine the quality of calls that are running on your network and judge whether you need additional hardware to improve performance. You can use utilization reports for gateways, voice messaging, conference bridge, route groups, route lists, and route patterns to provide a picture of the usage to help with system handling.

You can also customize the report parameters and enable a mailing option, so reports get e-mailed when they are created. The Customize Parameters option allows you to customize the report parameters for particular reports in the Customize Parameters window. For each individual report, you can customize the parameters for that report.

Setting Up Alerts

CAR provides e-mail alerts for various events, including the following events:

- Charge Limit Notification indicates when the daily charge limit for a user exceeds the specified maximum. You can set the maximum in the **Report Config > Notification Limits** window.
- QoS Notification indicates when the percentage of good calls drops below a specified range or the percentage of poor calls exceeds a specified limit. You can set the range in the **Report Config > Notification Limits** window.

Enabling the system for e-mail alerts comprises a two-step process. First, you must specify the mail server configuration information (**System > System Parameters > Mail Parameters**). CAR uses the configuration information to successfully connect to the e-mail server. Next, you must enable the e-mail alerts on the Automatic Report Generation/Alert window (**Report Config > Automatic Generation/Alert**). By default, CAR enables e-mail alerts for some, but not all, reports.

Purging CAR data

This section contains information on the following topics:

- Automatic purging
- Manual purging
- Event log purging

CAR provides automatic and manual purging of the CAR database. By default, the system enables automatic purging. Before and after loading CDRs/CMRs, CAR checks the size of the CAR database and invokes automatic purging, if necessary, to control the CAR database size.

With automatic purging, CAR continuously monitors the number of days that the CDRs are kept in the CAR database; when the CDR age exceeds the maximum number of days as configured in the maximum age setting in the Configure Automatic Database Purge window, CAR deletes all CDRs that are older than the number of days that you configured.

In the Configure Automatic Database Purge window, you specify the percentages of the CAR database that you want to allot for CAR data; the system maintains the CAR database size between the high water mark and low water mark that you specify. When the CAR database size exceeds the low water mark, CAR sends an e-mail to all CAR administrators. When the database size exceeds the high water mark or the number of CDRs in the CAR database exceeds two million records, CAR deletes CDRs that are older than the number of days that you specified for the CDR minimum age in the Configure Automatic Database Purge window; then, an e-mail gets sent to all CAR administrators. If the high water mark gets breached again or if the CDRs exceed two million even after automatic purging completes, CAR triggers auto purging, does not load the CDRs/CMRs, and sends another e-mail.

**Tip**

To disable automatic purging to the minimum age when the high water mark gets breached or when the CDRs exceed two million records, configure the CDR minimum age to equal the CDR maximum age in the Configure Automatic Database Purge window.

Configure manual database purge when you want to delete records that are older than a particular date or that fall in a specific date range, but you do not want to change the automatic purging schedule. You can also reload the CAR database with CDR records by clicking the Reload button in the Manual Purge window. You may want to reload the database to reclassify calls after dial-plan updates, user-device association changes, call rate changes, and so on. After the system loads the new records, the system loads the records according to the schedule in the configured CDR load schedule. By default, CDR data loads every day from midnight to 5 a.m.

**Tip**

Schedule database purges or manual purging during off-peak hours to minimize any degradation of Cisco Unified CallManager performance.

Event log purging, which is a daily scheduled job that monitors the `tbl_event_log` table, automatically deletes the `tbl_event_log` records to keep the latest 3 days of daily jobs, the latest 3 weeks of weekly jobs, and the latest 3 months of monthly jobs; that is, if more than 1500 rows exist in the `tbl_event_log` table. CAR automatically enables event log purging and does not send an e-mail when event log purging occurs.

Call Costs

You can use CAR to set a base monetary rate for the cost of calls on the basis of a time increment. Then, you can further qualify the cost by applying the time-of-day and voice-quality factors. Service providers who must account for service to subscribers use this feature. Some organizations also use this information to establish billing costs for users and departments in the organization for accounting or budgeting purposes.

Reports that use these rating parameters include individual bill, department bill, top N by charge, top N by number, and top N by duration.

**Note**

If you do not change the default value for charge base/block, the cost will always remain zero because the default base charge per block equals zero.

**Note**

If you do not want to increase call cost by voice quality, you can use the default values. The default multiplication factor specifies 1.00, so no increase in call cost for voice quality occurs.

For more information on setting call rates, see the [“Configuring the Rating Engine” section on page 26-1](#).

Tracking Activity

CAR provides logs that can track the status of the various activities. The event log tracks events that the CAR Scheduler triggers, such as automatically generated reports, loading of CDRs, notifications, report deletions, and database purging.

CAR Administrators, Managers, and Users

CAR provides reporting capabilities for three levels of users.

- Administrators use all the features of CDR Analysis and Reporting; for example, they can generate system reports to help with load balancing, system performance, and troubleshooting.
- Managers can generate reports for users, departments, and QoS to help with call monitoring for budgeting or security purposes and for determining the voice quality of the calls.
- Individual users can generate a billing report for calls.

Any user can act as a CAR administrator. Users who have been identified as CAR administrators have full control over the CAR system. The administrator can modify all the parameters that relate to the system and the reports.

CAR requires a minimum of one administrator.

You set up administrators, managers, and users in Cisco Unified CallManager Administration. For more information, see the “Configuring CAR Administrators, Managers, and Users” section in the *Cisco Unified CallManager CDR Analysis and Reporting Administration Guide, Release 5.0(4)*.

CAR System Settings

CDR Analysis and Reporting sets default values for all system parameters. Before you generate any reports in CAR, Cisco recommends that you customize a number of system parameters. Because default values are provided for all system parameters, Cisco recommends customizing but does not require it.

CAR allows you to set the following parameters:

- The mail server criteria—CAR uses this information to successfully connect to the e-mail server to send alerts and reports by e-mail. If you do not want to send alerts or reports by e-mail, you do not need to specify this information.
- Dial plan—The default dial plan in CAR specifies the North American numbering plan (NANP). Ensure the dial plan is properly configured, so call classifications are correct in the reports. If you have modified the default NANP that Cisco Unified CallManager Administration provides, or if you are outside the NANP, be sure to configure the dial plan according to your Cisco Unified CallManager dial plan.
- Gateways—To utilize the gateway reports, you need to configure gateways in CAR. You should do this after installation for any existing gateways in your Cisco IP telephony system and when you add gateways to the system. If the system deletes any gateways, CAR gets the latest list of gateways, and any configuration that is specified in CAR for the deleted gateways gets deleted. CAR uses the area code information to determine whether calls are local or long distance. You must provide the Number of Ports information for each gateway to enable CAR to generate the Utilization reports.
- System preferences—You can set CAR system preferences for the Company Name parameter.

CAR Reports

From CAR, you can generate reports on demand, or if you are an administrator, you can schedule reports for automatic generation. You can view reports in comma separated values (CSV) format or portable document format (PDF). If you choose PDF, you must have Adobe Acrobat Reader installed on your PC.

The section describes the reports that are available with CDR Analysis and Reporting and contains the following topics:

- [CAR Reports General Information, page 24-6](#)
- [User Reports, page 24-7](#)
- [System Reports, page 24-8](#)
- [Device Reports, page 24-10](#)
- [Automatically Generated Reports Schedule, page 24-11](#)

CAR Reports General Information

For all the CAR reports that show the pattern for Hour of Day, Day of Week, and Day of Month, the charts and tables get shown according to the following conditions:

- When no records match the time range specified (hour of day, day of week, or day of month) in the search criteria, the report displays a value of 0.00 for all of the days/hours.
- If all records that are returned have a value of 0.00, CAR does not display the charts. CAR displays the charts if any record contains a non-zero value.

- When records get generated (for at least one day in the chosen date range) and the number of days chosen is more than the number of days that the report can show (more than seven for weekly and more than 31 for monthly), the chart displays all the days (with 0 value for the days that do not generate records). A table displays for all the days with relevant value and 0.00 for the days that do not contain data.
- When records generate (for at least one day in the chosen date range) and the number of days chosen is less than the number of days that the report can show (less than seven for weekly and less than 31 for monthly), the chart displays all the days (with 0 value for the days that do not generate records). A table displays all the days with relevant value and 0.00 for the days that do not contain data.

In all the CAR reports that display username, userid displays if CAR cannot retrieve the username. This can happen when the report gets generated for the past data and if the user that was involved in a call at that time no longer exists in the system (Cisco Unified CallManager database).

Additional Information

See the [“Related Topics” section on page 24-16](#).

User Reports

Users, managers, and CAR administrators can generate user reports. CAR includes the following user reports:

- **Individual Bills**—Available for users, managers, and CAR administrators. Individual bills provide your call information for the date range that you specify. You can generate, view, or mail summary or detail information about your individual phone bills.
- **Department Bills**—Available for managers and CAR administrators. Department bills provide call information and quality of service (QoS) ratings. If you are a manager, you can generate a summary or detailed report of the calls that are made by all users who report to you, or only those users that you choose. If you are a CAR administrator, you can generate a summary or detailed report of the calls that some or all users in the system make. This report helps you to keep track of all calls on a user-level basis for the entire system.
- **Top N by Charge**—Available for managers and CAR administrators. Top N by Charge reports that individual users generate list the top number of users that incurred a maximum charge for calls during a period that you specify. Reports generated by destinations list the destinations that incurred the maximum charges. Reports generated by all calls list the calls that incurred the maximum charges. If you are a manager, the report includes the top charges for all calls that are made by users who report to you during the specified period. If you are a CAR administrator, the report includes the top charges for all calls that are made by all users on the system for the specified period.
- **Top N by Duration**—Available for managers and CAR administrators. Top N by Duration reports that individual users generate list the top number of users that incurred a maximum time on calls during a period that you specify. Reports generated by destinations list the destinations that incurred the maximum duration. Reports generated by all calls list the calls that incurred the maximum duration. If you are a manager, the report lists the top number of users who report to you who incurred a maximum time for calls that are made during the chosen date range, starting with the longest. If you are a CAR administrator, the report lists the top number of users that incurred a maximum time for calls that were made during the chosen date range, starting with the longest.
- **Top N by Number of Calls**—Available for managers and CAR administrators. Top N by Number of Calls reports that individual users generate lists the users who incurred the maximum number of calls. Reports that extensions generate list the extensions that placed or received the greatest number of calls during a period that you specify. If you are a manager, the report lists the top number of calls

by user or extension, among the users who report to you, for the chosen date range. If you are a CAR administrator, the report lists the top number of calls for each user or extension in the system. Reports generated By Individual Users lists the Users who incurred the maximum number of calls. Reports generated By Extensions lists the extensions that have placed or received the greatest number of calls in the group (for a Manager) or in the System (for the CAR Administrator).

- Cisco CallManager Assistant Call Completion Usage Reports—Available for CAR administrators. The Cisco IPMA summary and detail reports provide call completion usage details for both IPMA managers and assistants. The manager reports can include calls that managers handle for themselves only, calls that assistants handle for managers only, or calls that both managers and assistants handle for managers. The assistant reports can include calls that assistants handle for themselves only, calls that assistants handle for managers, calls that both assistants handle for themselves and for managers.
- Cisco IP Phone Services—Available for CAR administrators. The Cisco IP Phone Services report shows selected Cisco Unified IP Phone services, the number of users that are subscribed to each of the selected services, and the utilization percentage for each of the selected services. You can create services for a wide variety of business and entertainment uses. If you have revenue tied to a service, such as for advertising, you can use this report to determine the number of users who have subscribed to the service. You can also use this report to indicate the popularity of selected services.

Additional Information

See the [“Related Topics”](#) section on page 24-16.

System Reports

CDR Analysis and Reporting provides system reports for managers and CAR administrators. Managers or CAR administrators can access the QoS summary report. Only CAR administrators can access all other reports. This section describes the following reports:

- QoS Detail—Available for CAR administrators. The QoS detail report provides the QoS ratings that are attributed to inbound and outbound calls on the Cisco Unified CallManager network for the period that you specify. Use this report to help monitor the voice quality of all calls on a user-level basis for the entire system. The call details in CDRs and CMRs and the QoS parameters that you choose provide the basis for assigning a particular voice-quality category to a call.
- QoS Summary—Available for managers and CAR administrators. This report provides a two-dimensional pie chart that shows the distribution of QoS grades that are achieved for the specified call classifications and period. The report also provides a table that summarizes the calls for each QoS. The call details in CDRs and CMRs and the QoS parameters that you choose provide the basis for assigning a call to a particular voice-quality category. Use this report to monitor the voice quality of all calls through the network.
- QoS By Gateway—Available for CAR administrators. This report shows the percentage of the calls for each of the chosen gateways that meet the QoS criteria that the user chooses. You can generate this report on an hourly, daily, or weekly basis.
- QoS By Call Types—Available for CAR administrators. This report shows the percentage of the calls for each chosen call type that meet the QoS criteria that the user chooses. You can generate this report on an hourly, daily, or weekly basis.

- **Traffic Summary**—Available for CAR administrators. This report provides information about the call volume for a period that you specify. Include only those call types and QoS voice-quality categories that you chose. Use this report to determine the number of calls that are being made on an hourly, weekly, or daily basis. This report helps you identify high- and low-traffic patterns for capacity planning.
- **Traffic Summary by Extensions**—Available for CAR administrators. This report provides information about the call volume for a period and set of extensions that you specify. Include only those call types and extensions that you chose. You can generate the report on an hourly, weekly, or daily basis. This report helps you determine high-usage users or groups by aggregating the usage level across the users that you specify.
- **Authorization Code Name**—Available for CAR administrators. This report allows administrators to view the originating and destination numbers, the date and time that the call originated, the call duration in seconds, the call classification, and the authorization level for calls that relate to each chosen authorization code name.
- **Authorization Level**—Available for CAR administrators. This report allows administrators to view the originating and destination numbers, the date and time that the call originated, the call duration in seconds, the authorization code name, and the call classification for calls that relate to each chosen authorization level.
- **Client Matter Code**—Available for CAR administrators. This report allows administrators to view the originating and destination numbers, the date and time that the call originated, the call duration in seconds, and the call classification for calls that relate to each chosen client matter code.
- **Malicious Call Details**—Available for CAR administrators. The Cisco CallManager Malicious Call Identification (MCID) service tracks malicious calls. The Malicious Call Details report displays the details of malicious calls for a given date range.
- **Precedence Call Summary**—Available for CAR administrators. The Cisco CallManager Call Precedence service allows authenticated users to preempt lower priority phone calls. The PDF version of the CAR Precedence Call Summary report displays the Call Summary for the precedence values in the form of a bar chart, on an hour of day, day of week, or day of month basis, for each of the precedence levels that you choose. CAR generates one chart for each precedence level, a table for each precedence level that lists the number of call legs, and a subtable that summarizes the percentage distribution for each of the precedence levels. CAR makes the report available on-demand; the report does not get autogenerated.
- **System Overview**—Available for CAR administrators. This report provides a list of reports that you can select to generate. You can choose a list of reports that you want to appear on the report. Use this report to see a high-level picture of the Cisco Unified CallManager network.
- **CDR Error**—Available for CAR administrators. This report provides statistics for the number of error records in the CAR Billing_Error table and the reason for the errors. Use this report to determine whether CAR incurred any errors with CDR data while loading the CDR data. This report lists the percentage of CDRs that are invalid and the reason these CDRs have been classified as invalid.

Additional Information

See the [“Related Topics”](#) section on page 24-16.

Device Reports

Device reports help CAR administrators track the load and performance of Cisco Unified CallManager-related devices, such as conference bridges, voice-messaging server, and gateways. This section describes the device reports:

- **Gateway Detail**—Available for CAR administrators. Use the gateway detail report to track issues with specific gateways. The report provides a list of calls that used the specified gateways. Use this report to review detailed information about chosen gateways. You can specify gateways by type, such as all or some of the VG200 gateways in your system, or by only those gateways that use a particular route pattern. You can also specify search criteria based on call types and QoS values.
- **Gateway Summary**—Available for CAR administrators. This report provides a summary of all the calls that went through the gateways. It also provides the total number of calls and duration for each of the categories, namely Incoming, Tandem, and Outgoing (Long Distance, Local, International, Others, OnNet) and also, the total calls for each QoS value for each gateway in the system. Use this report to track the functionality of the system on a daily basis. If you discover issues that need to be studied further, use the gateway detail report.
- **Gateway Utilization**—Available for CAR administrators. The report provides an estimate of the utilization percentage of the gateway(s). You can examine the usage on the basis of each hour of a day or by a specified number of days of the week or month. Reports generate for each gateway that is chosen. Use this report for load balancing or capacity planning (to evaluate the need for adding or removing gateways, depending on their utilization). You can specify gateways by type, such as all or some of the VG200 gateways in your system, or by only those gateways that use a particular route pattern.
- **Route and Line Group Utilization**—Only CAR administrators can generate the route and line group utilization report. This report provides an estimated utilization percentage of the chosen route and line group(s). You can examine the usage on the basis of each hour of a day or by a specified number of days of the week or month. Reports generate for each chosen route and line group. Use the report to analyze whether the route and line group capacity is sufficient to meet the usage requirements. Based on the results, you can decide whether additions are required. If you are load balancing gateways by using different route and line groups or route patterns and hunt lists that are assigned to the gateways, you can use this report to see the load for the whole grouping. This report also provides a convenient way of generating utilization information for a grouping of gateways by a particular route and line group; the group will also include any H.323 fallback gateways that are using the specified route and line group.
- **Route/Hunt List Utilization**—Available for CAR administrators. The route/hunt list utilization report provides an estimated utilization percentage of the chosen route/hunt list(s). You can examine the usage on the basis of each hour of a day or by a specified number of days of the week or month. Reports generate for each chosen route/hunt list. Use the report to analyze whether the route and line group capacity is sufficient to meet the usage requirements. Based on the results, you can decide whether additions are required. If you are load balancing gateways by using different route/hunt lists that are assigned to the gateways, you can use this report to see the load for the whole grouping. This report also provides a convenient way of generating utilization information for a grouping of gateways by a particular route/hunt list; the group will also include any H.323 fallback gateways that are using the chosen route/hunt list.
- **Route Pattern/Hunt Pilot Utilization**—Available for CAR administrators. The route pattern/hunt pilot utilization report provides an estimated utilization percentage of the chosen route pattern(s)/hunt pilot(s). You can examine the usage on the basis of each hour of a day or by a specified number of days of the week or month. Reports generate for each chosen route pattern/hunt pilot. Use the report to analyze system usage on the chosen route pattern/hunt pilot.

- **Conference Call Details**—Available for CAR administrators. The Conference Call Details reports allows you to generate and view details about conference calls. The Summary Report displays the summary information of conference calls within a chosen date/time range but does not contain information about each individual conference participant call leg. The Detailed Report displays the detailed information about the conference calls within a chosen date/time range and includes information about each individual conference participant call leg.
- **Conference Bridge Utilization**—Available for CAR administrators. The report provides an estimate of the utilization percentage of the conference bridge(s). You can examine the usage on the basis of each hour of a day or by a specified number of days of the week or month. Generate reports for all the conference bridges in the system. Use this report to determine the activity on the conference bridge(s) and whether you need to add additional resources. This report helps you identify usage patterns, so you can plan capacity when you discover recurring peaks in the usage pattern.
- **Voice Messaging Utilization**—Available for CAR administrators. The report provides an estimate of the utilization percentage of the voice-messaging device(s). You can examine the usage on the basis of each hour of a day or by a specified number of days of the week or month. Reports generate for each voice-messaging device. Use this report to determine the activity on the voice messaging device(s) and whether you need to add additional resources. This report helps you to identify usage patterns, so you can plan capacity when you discover recurring peaks in the usage pattern.

Additional Information

See the [“Related Topics”](#) section on page 24-16.

Automatically Generated Reports Schedule

Automatically generating reports comprises a two-step process. First, you must enable the reports that you want to have generated, unless they are enabled by default. Second, you must schedule the reports for the day and time that you want them to generate. CAR provides a default schedule, so if the default schedule is acceptable, you need only enable the reports that you want to automatically generate.

The system enables or disables the following reports for automatic generation by default. The words Daily, Weekly, or Monthly in the square brackets next to the report name specify the report generation interval of the particular report.

- Traffic Summary-Hour of Day[Daily] - Enabled
- Conference-Summary [Monthly] - Disabled
- Conference-Detail [Daily] - Disabled
- Conference Bridge Util-Day of Week[Weekly] - Enabled
- Gateway Util-Day of Week[Weekly] - Enabled
- Line Group Util-Day of Week[Weekly] - Disabled
- Route Group Util-Day of Week[Weekly] - Disabled
- Route/Hunt List Util-Day of Week[Weekly] - Disabled
- Route Pattern/Hunt Pilot Util-Day of Week[Weekly] - Disabled
- Traffic Summary-Day of Week[Weekly] - Enabled
- Traffic Summary-Day of Month [Monthly] - Enabled
- Voice Messaging Util-Day of Week[Weekly] - Enabled
- Gateway Summary [Monthly] - Enabled

- QOS Summary [Monthly] - Enabled
- System Overview [Monthly] - Enabled
- Department Bill Summary [Monthly] - Disabled
- Individual Bill Summary [Monthly] - Disabled
- Top N Calls [Daily] - Disabled
- Top N Calls [Monthly] - Disabled
- Top N Charge [Daily] - Disabled
- Top N Charge [Monthly] - Disabled
- Top N Duration [Daily] - Disabled
- Top N Duration [Monthly] - Disabled

To enable or disable report generation, see the [“Enabling or Customizing Reports for Automatic Generation”](#) section on page 26-7.

To change the specific time each day, week, or month that reports get generated and get purged from the system see the [“System Scheduler Configuration”](#) section on page 25-7.

Additional Information

See the [“Related Topics”](#) section on page 24-16.

CDR Search

Call detail records (CDR) provide details about the called number, the number that placed the call, the date and time that the call was started, the time that it connected, the time that it ended, and the cause for the termination of a call. Call management records (CMRs, or diagnostic records) detail the jitter, lost packets, the amount of data that was sent and received during the call, and latency. CDR data comprises CDRs and CMRs collectively. A single call can result in the generation of several CDRs and CMRs as Cisco Unified CallManager tracks the progress of the call through each part of the call: sending digits, receiving digits, hold, transfer, engaging a transcoder for conferencing, and disengaging the transcoder.

You must enable the CDR Enabled Flag, CDR Log Calls with Zero Duration, and Call Diagnostics service parameters in Cisco Unified CallManager for CDR data to be generated. You must enable the CDR Enabled Flag parameter on each node in the cluster. For more information about configuring these service parameters, see the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

All CAR reports use CDR data. Make sure that you have the most current CDR data from which to build your reports. By default, CDR data loads from midnight to 5 a.m. on a daily basis; however, you can set the loading time, interval, and duration as needed.



Tip

When you configure the time range, use Coordinated Universal Time (UTC). When you configure the date and time range, configure the settings, so the number of CDR results does not exceed 15,000. If the results exceed 15,000, CDR search cannot occur, and a message displays to inform you that you must revise the date and time range.

In all CDR Search reports, the system only displays the oldest 100 records that fall into the time and date range that you configure.

You can configure CDR searches to verify the details of a call. The search forms groups of all the related legs of a call, which can be useful if the call involves a conference or transfer. This method helps you track the progress and quality of each part of an entire call.

This section describes the following features:

- **CDR Search by User Extension**—Available for CAR administrators. You can search CDRs by user or directory number (calling, original called, or final called) to analyze call details for the first 100 records that satisfy the search criteria. You can search for calls by using specific numbers for the period that you specify, which helps you trace calls that are placed from or to any specific numbers for diagnostic or informational purposes. All associated records, such as transfer and conference calls, appear together as a logical group. If you do not specify an extension, the system returns the first 100 CDR records that match the date range that you specify.
- **CDR Search by Gateway**—Available for CAR administrators. You can search CDRs by gateways to analyze the call details of calls that are using specific gateways. This method helps you trace issues on calls through specific gateways.
- **CDR Search by Cause for Call Termination**—Available for CAR administrators. You can search CDRs by cause for call termination to get information about the cause for the termination of a call. You can choose from a list of causes for call termination and can generate the report for a particular date range. The generated report contains the report criteria, along with the total number of calls that were placed in the given time. In addition, a table displays with the fields Call Termination Cause Value and description, the total number of calls, and the percentage of calls for each Call Termination Cause, and an option to choose the CDRs.
- **CDR Search by Call Precedence Level**—Available for CAR administrators. You can search CDRs by call precedence level. The report that generates allows you to view the CDRs on the basis of precedence. You can choose the precedence level and date range for which to generate a report. The report displays the number of calls and the percentage of these calls for each precedence level that you chose. Report criteria display the precedence levels and date range for which the report generated information in the Call Precedence Details window. You can view the media information and the CDR-CMR dump from the CDR Search by Precedence Levels Result window. The media information and CDR-CMR dump information display in separate windows.
- **CDR Search for Malicious Calls**—Available for CAR administrators. You can search CDRs to get information about malicious calls. You can choose extensions and the date range for which to generate a report. The report displays the CDRs for all the malicious calls for a chosen extension and date range. Report criteria display the extensions and the date range for which the report generated information. You can view the media information and CDR-CMR dump from the CDR-CMR search results window. The media information and CDR-CMR dump information display in separate windows.
- **Export CDR/CMR**—Available for CAR administrators. With this feature, you can export CDR/CMR dump information, for a given date range in the CSV format, to a location that you choose on your computer. You can also view the file size of the dump information and delete CDR/CMR files.

Internationalization for CDR Analysis and Reporting

CAR, designed to be internationalized to handle any locale (or language), includes a database that can also handle any locale.

**Note**

CAR supports all Latin-1 language and Unicode language locales as the Cisco Unified CallManager help pages specify. Latin-1 languages include English and Western European languages. Unicode languages include Japanese and Chinese.

Two types of locale exists: user and network. Each locale comprises a set of locale files. The following definitions describe the two types of files:

- User—Files that relate to user-related functions, such as phone display text, user applications, and user web pages.
- Network—Files that relate to network-related functions, such as phone and gateway tones. Country names designate network locales.

CAR supports the locales only if the Locale Installer has installed locales.

**Note**

Make sure that you have first installed the Cisco Unified CallManager Locale Installer on every server in the cluster. Installing the locale installer ensures that you have the latest translated text available for the CAR web pages. For more information on the Cisco Unified CallManager Locale Installer, refer to the *Cisco Unified Communications Operating System Administration Guide, Release 5.0(4)*.

Only User and Manager windows support multiple locales. Administrator pages display in English.

In the Cisco Unified CallManager Administration, set the user-preferred locale in the Cisco Unified CallManager database. You do this when you create a user from the End User Configuration window. Specify the preferred locale along with the user name, user ID, and so on. The Cisco Unified CallManager database stores this information. Refer to the *Cisco Unified CallManager Administration Guide, Release 5.0(4)* for more detailed information.

This section describes the elements that make up the internationalization of CAR.

Logon Page

When the client (browser) requests the logon information, the logon window header includes the client's most preferred locale. The CAR system checks whether the CAR UI supports this locale. If the CAR UI does not support the locale, or if the locale is not installed in the system, the logon window displays in the Cisco Unified CallManager system default locale that is set in the Cisco CallManager Enterprise parameter. If CAR does not also support this locale, or the locale is not installed in the system, the locale gets set to English_United_States.

Authenticate and Show CAR Pages for Post Logon Windows

User credentials (in any language) get authenticated through the Cisco Unified CallManager database, and then CAR windows for non-administrative users (users or managers) display the user's preferred locale. If the CAR UI does not support this locale, or if the locale is not installed in the system, the Cisco Unified CallManager system default locale gets used. If this locale is not supported by CAR, or is not installed in the system, pages display in the most preferred locale of the browser. When the browser-preferred locale is also not supported or not installed, the locale gets set to English_United_States. All information on the UI pages, including labels, number formats, and so on., displays based on the locale. The administrator windows always display in English.

Reports

Reports, which are generated in both CSV and PDF formats, display in the user's preferred locale for non-administrative users (users or managers). However, the dynamic data (like the Company Name shown in the report header) displays in the same language as was used to enter it in the database. The locale provides the basis for the header, footers, number formats, and some static data (like call classification). Reports for administrators display in English.

Web Browsers

The CAR program supports the following web browsers:

- Netscape Communicator 7.1 (or later)
- Microsoft Internet Explorer 6.0 (or later)

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 web page performance to suffer. Try to limit the number of users and administrators that are logged on simultaneously.

CDR Analysis and Reporting Configuration Checklist

Table 24-1 provides an overview of the steps for configuring CDR Analysis and Reporting.

Table 24-1 CAR Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Activate the CDR services on the appropriate servers.	Activating CAR, <i>Cisco Unified CallManager CDR Analysis and Reporting Administration Guide, Release 5.0(4)</i>
Step 2	To ensure that the CDR records write to flat files, you must enable the Cisco CallManager service parameters, CDREnabled and CallDiagnosticsEnabled.	<i>Cisco Unified CallManager Administration Guide, Release 5.0(4)</i>
Step 3	Set up CAR administrators, managers, and users in Cisco Unified CallManager Administration.	Configuring CAR Administrators, Managers, and Users, <i>Cisco Unified CallManager CDR Analysis and Reporting Administration Guide, Release 5.0(4)</i>
Step 4	Configure CAR system parameters for report generation: • Configure mail server. • Configure dial plan. • Configure gateway. • Set system preferences.	System Parameters Configuration, page 25-1
Step 5	Specify the value ranges that you consider good, acceptable, fair, and poor for jitter, latency, and lost packets.	Defining the Quality of Service (QoS) Values, page 26-5

Table 24-1 CAR Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 6	If desired, set a base monetary rate for the cost of calls on the basis of a time increment. You can further qualify the cost by applying the time-of-day and voice-quality factors.	Configuring the Rating Engine, page 26-1
Step 7	Enable the reports that you want to automatically generate by using the Automatic Generation/Alert Option window.	Configuring Automatic Report Generation/Alert, page 26-6 Automatically Generated Reports Schedule, page 24-11
Step 8	Configure the system scheduler to schedule when CAR loads CDRs as well as daily, weekly, and monthly reports.	System Scheduler Configuration, page 25-7
Step 9	Set the parameters for automatic purging of the CAR database. You can set the percentage of the CAR database that you want the system to use for CAR data and the age of CAR data that you want to delete when the CAR data exceeds the database size limit. You can disable automatic database purging, but the system enables purging by default.	Configuring Automatic Database Purge, page 25-14
Step 10	Set the charge limit notification that indicates when the daily charge limit for a user exceeds the specified maximum and the QoS notification that indicates when the percentage of good calls drops below a specified range or the percentage of poor calls exceeds a specified limit.	Configuring Notification Limits, page 26-8
Step 11	If your users want to view localized user and manager reports, install the proper locales.	<i>Cisco Unified Communications Operating System Administration Guide, Release 5.0(4)</i>
Step 12	To back up CAR, including the database and the pregenerated reports, make sure that you configure the CAR target in the backup utility.	<i>Disaster Recovery Administration Guide, Release 5.0(4)</i>

Additional Information

See the [“Related Topics”](#) section on page 24-16.

Related Topics

- [CAR Reports General Information, page 24-6](#)
- [User Reports, page 24-7](#)
- [System Reports, page 24-8](#)
- [Device Reports, page 24-10](#)
- [Automatically Generated Reports Schedule, page 24-11](#)
- [Getting Started with CDR Analysis and Reporting, Cisco Unified CallManager CDR Analysis and Reporting Administration Guide, Release 5.0\(4\)](#)
- [CAR System Configuration, page 25-1](#)
- [CAR Report Configuration, page 26-1](#)

- CAR User Reports Configuration, *Cisco Unified CallManager CDR Analysis and Reporting Administration Guide, Release 5.0(4)*
- CAR System Reports Configuration, *Cisco Unified CallManager CDR Analysis and Reporting Administration Guide, Release 5.0(4)*
- CAR Device Reports Configuration, *Cisco Unified CallManager CDR Analysis and Reporting Administration Guide, Release 5.0(4)*
- [CDR Search Configuration, page 27-1](#)
- Export CDR/CMR Records Configuration, *Cisco Unified CallManager CDR Analysis and Reporting Administration Guide, Release 5.0(4)*
- [CAR Report Results, page 28-1](#)

Additional Cisco Documentation

- *Cisco Unified Communications Operating System Administration Guide, Release 5.0(4)*
- *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)*
- *Cisco Unified CallManager Serviceability System Guide, Release 5.0(4)*



CAR System Configuration

Before you start generating reports with CAR, configure the system. In most cases, CAR provides default values; however, review the topics that this chapter provides to learn more about customizing CAR.

This chapter contains the following topics:

- [System Parameters Configuration, page 25-1](#)
- [System Scheduler Configuration, page 25-7](#)
- [System Database Configuration, page 25-12](#)
- [System Log Screens, page 25-15](#)
- [Related Topics, page 25-16](#)

System Parameters Configuration

Unless you want to use the default values, you should customize a number of system parameters before you generate any reports. This section describes the system parameters. Because default values are provided for all system parameters, Cisco recommends customizing but does not require it.

This section contains the following topics:

- [Configuring Mail Server Parameters, page 25-2](#)
- [Configuring the Dial Plan, page 25-2](#)
- [Restoring the Default Values for the CAR Dial Plan, page 25-4](#)
- [Gateway Configuration, page 25-5](#)
- [Configuring System Preferences, page 25-6](#)

Configuring Mail Server Parameters

To send e-mail alerts and reports by e-mail, you must specify the mail server configuration information. CAR uses the configuration information to successfully connect to the e-mail server.

This section describes how to specify e-mail server information.

Procedure

-
- Step 1** Choose **System > System Parameters > Mail Parameters**.
The Mail Parameters window displays.
- Step 2** In the Mail ID field, enter the e-mail identifier that will be used in the From field when e-mails are sent.
- Step 3** In the Password field, enter the password that is used to access the server that is running the e-mail system.
-  **Note** CAR does not authenticate the user ID and password. You must disable authentication on the mail server or enter a valid user ID and password.
-
- Step 4** In the Confirm Password field, enter the same password from [Step 3](#) to confirm.
- Step 5** In the Mail Domain field, enter the domain name for the server that is running the e-mail system.
- Step 6** In the Mail Server Name field, enter the name or IP address of the server that is running the e-mail system.
- Step 7** To make the changes, click the **Update** button.
-

Additional Information

See the [“Related Topics” section on page 25-16](#).

Configuring the Dial Plan

The default dial plan in CAR specifies the North American numbering plan (NANP). Make sure that the dial plan is properly configured, so call classifications display correctly in the reports.



Note

If you have modified the default NANP that is provided in Cisco Unified CallManager Administration, or if you are outside the NANP, be sure to configure the dial plan in CAR according to your Cisco Unified CallManager dial plan. At least one condition must exist to configure the Dial Plan. Refer to the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*, and the *Cisco Unified CallManager System Guide, Release 5.0(4)*, for dial plan information.

To configure the dial plan, define the parameters for the outgoing call classifications. Call classifications include international, local, long distance, on net, and so on. For example, if local calls in your area equal six digits in length, you would specify a row in the dial plan as follows:

Condition	No of Digits	Pattern	Call Type
=	6	!	Local

This section describes how to update the CAR dial plan configuration.

Procedure

-
- Step 1** Choose **System > System Parameters > Dial Plan Configuration**.
- The Dial Plan Configuration window displays.
- Step 2** In the Toll Free Numbers field, enter the numbers in your dial plan that can be placed without a charge.
- Step 3** Update the values in the table by using the following fields:
- **Condition**—Select the condition of the rule where > represents greater than; < represents less than, and = represents a value that is equal to the specified value in the No of Digits field.
 - **No Of Digits**—Choose the number of digits in the directory number to which this rule should be applied. If the number of digits does not impact the rule, specify NA.
 - **Pattern**—Enter the pattern that is used for the call classification, where
 - G—Signifies classified as specified in the rule (G equals a wildcard for the gateway area code that is specified in the [“Gateway Configuration” section on page 25-5.](#))
 - T—Retrieves the toll-free numbers that are configured in CAR.
 - !—Signifies multiple digits (any number that is more than 1 digit in length, such as 1234 or 5551234).
 - X—Signifies a single-digit number (such as 0, 1, or 9).
 - **Call Type**—Choose the call type if the condition is satisfied.
- Step 4** To add more rows, check the check box in the row below where you want to add rows and click the **Add Rows** link. The system adds a row above the row that you chose. To delete a row, check the check box by the row that you want to delete and click the **Delete Rows** link.
-  **Note** CAR classifies calls on the basis of the dialed number as stored in the CDRs. If the dialed digits differ from the digits that are written in CDRs (due to number transformations), configure the Dial Plan in CAR on the basis of how the digits show up in CDRs.
-
- Step 5** To make the changes, click the **Update** button.
-

Additional Information

See the [“Related Topics” section on page 25-16.](#)

Restoring the Default Values for the CAR Dial Plan

If you have modified the default dial plan in CAR, you can restore the default values that are based on the North American numbering plan (NANP).

[Table 25-1](#) provides the default NANP values.

Table 25-1 *Default Values for CAR Dial Plan*

Condition	No of Digits	Pattern	Call Type
=	5	!	OnNet
=	7	!	Local
=	10	T!	Others
=	10	G!	Local
=	10	!	Long Distance
=	11	T!	Others
=	11	XG!	Local
=	11	!	Long Distance
>	3	011!	International

The following information explains the default table values in [Table 25-1](#):

- Row 1—If the number of digits dialed equals 5 and the pattern is ! (more than one digit, in this case, 5 digits), the call gets classified as OnNet.
- Row 2—If the number of digits dialed equals 7 and the pattern is ! (more than one digit, in this case, 7 digits), the call gets classified as Local.
- Row 3—If the number of digits dialed equals 10 and the pattern is T! (more than one digit, in this case a 10-digit number that starts with a Toll Free number code), the call gets classified as Others.
- Row 4—If the number of digits dialed equals 10 and the pattern is G! (more than one digit, in this case a 10-digit number that starts with a gateway code), the call gets classified as Local.
- Row 5—If the number of digits dialed equals 10 and the pattern is ! (more than one digit, in this case an 10-digit number), the call gets classified as Long Distance.
- Row 6—If the number of digits dialed equals 11 and the pattern is T! (more than one digit, in this case an 11-digit number that starts with a toll-free number code), the call gets classified as Others.
- Row 7—If the number of digits dialed equals 11 and the pattern is XG! (more than one digit, in this case an 11-digit number that starts with any single digit followed by a gateway code), the call gets classified as Local.
- Row 8—If the number of digits dialed equals 11 and the pattern is ! (more than one digit, in this case an 11-digit number), the call gets classified as Long Distance.
- Row 9—If the number of digits dialed is greater than three and that starts with 011, the call gets classified as International.

If none of the conditions gets satisfied, the call gets classified as Others. This section describes how to restore the NANP dial plan values in CAR.

Procedure

-
- Step 1** Choose **System > System Parameters > Dial Plan Configuration**.
The Dial Plan Configuration window displays.
- Step 2** Click the **Restore Defaults** button.
The restoration takes effect at midnight. To make changes take effect immediately, restart the Cisco CAR Scheduler service. For information on restarting services, refer to the *Cisco Unified CallManager Serviceability Administration Guide, Release 5.0(4)*.
-

Additional Information

See the [“Related Topics” section on page 25-16](#).

Gateway Configuration



Tip

Configure the gateways in CAR for existing Cisco Unified CallManager system gateways. Also, after you add gateways to Cisco Unified CallManager Administration, configure the new gateways in CAR. When gateways are deleted from the Cisco Unified CallManager system, the system automatically removes the gateways (and any configuration settings that you specified) from CAR.

CAR uses the area code information to determine whether calls are local or long distance. You must provide the Number of Ports information for each gateway to enable CAR to generate the Utilization reports.



Note

“G” acts as a wildcard for the gateway area codes that are used in Dial Plan configuration.

This section describes how to configure gateways in CAR.

Procedure

-
- Step 1** Choose **System > System Parameters > Gateway Configuration**.
The Gateway Configuration window displays.
- Note** If you have not configured gateways in Cisco Unified CallManager Administration, a message displays that indicates that you have not configured gateways for the system.
-
- Step 2** Perform one of the following tasks:
- To update the area code for all gateways, enter the area code in the Area Code field and click the **Set Area Code** button.
A message displays that indicates that you must click Update to save changes. Click **OK**.
 - To update the area code for specific gateways, enter the area code for each gateway that you want to configure in the area code field for that gateway.

- Step 3** In the Max No. of Ports field, enter the number of ports for each gateway that you want to configure. The Max No of Ports range goes from 1 to 1000.



Note CAR uses the values that were provided for the gateway when it was added in Cisco Unified CallManager Administration. Therefore, some gateways will already have an area code setting or have a zero for maximum number of ports, depending on the details that were specified when the gateway was added in Cisco Unified CallManager Administration. CAR does not accept 0 as a value for the maximum number of ports; you may be prompted to change the maximum number of ports for all gateways with a value of zero.

- Step 4** To make the changes, click the **Update** button.
You can run reports in CAR on any or all of the configured gateways.

Additional Information

See the [“Related Topics” section on page 25-16](#).

Configuring System Preferences

CAR provides default system preferences; however, you may customize the system by specifying values for the system parameters.

This section describes how to specify values for system parameters.

Procedure

- Step 1** Choose **System > System Parameters > System Preferences**.
The System Preferences window displays. The list of available system parameters displays in the Parameter Name list.
- Step 2** In the Parameter Value field, enter the desired value for the parameter as described in [Table 25-2](#).

Table 25-2 *System Preferences Parameter*

Parameter	Description
COMPANY_NAME	Enter the company name that is used as header information in reports.

- Step 3** Click the **Update** button.

System Scheduler Configuration

The CAR System Scheduler provides the following functions:

- Loads the daily CDR schedule
- Disables the daily CDR schedule
- Schedules the daily report
- Schedules the weekly report
- Schedules the monthly report

**Note**

Loading CDR data can cause performance degradation on the Cisco Unified CallManager server. Cisco recommends that you use the default loading time or schedule the loading to occur at a time when Cisco Unified CallManager performance will be least affected.

Additional Information

See the [“Related Topics” section on page 25-16](#).

Configuring the CDR Load Schedule

By default, CDR data loads every day from midnight to 5 a.m. This section describes how to customize the loading schedule, how to restore the default loading schedule if it was customized, and how to disable CDR loading.

Disable CDR loading when you are installing or upgrading the system in the same off-hours during which CDR loading normally occurs. Because loading CDRs causes a resource drain on Cisco Unified CallManager resources, you can suspend CDR loads until other operations complete. Of course, the CDR data does not get updated when CDR loading is disabled. Be sure to enable CDR loading again as soon as possible. The CAR tool does not affect the CDR generation in Cisco Unified CallManager.

**Tip**

To manually delete the CAR data and reload the database with CDRs, see the [“Manually Purging or Reloading the CAR Database” section on page 25-12](#).

Procedure

Step 1 Choose **System > Scheduler > CDR Load**.

The CDR Load window displays.

Step 2 Perform one of the following steps:

- To restore the default loading schedule, so CDR data loads every day from midnight to 5 a.m., click the **Restore Defaults** button.

Changes take effect at midnight. For the change to take effect immediately, stop and restart the Cisco CAR Scheduler service in the Control Center—Feature Services window.

- To disable CDR data loading, check the **Disable Loader** check box and click the **Update** button. CDR data will not load into CAR until you enable CDR loading. Changes take effect at midnight. You can force the change to take effect immediately by stopping and restarting the CAR Scheduler service.
- To enable CDR data loading, uncheck the **Disable Loader** check box and continue with [Step 3](#) to configure the load parameters.

Step 3 In the Load CDR & CMR area, complete the fields as described in [Table 25-3](#).

Table 25-3 Load CDR & CMR Values

Field	Value
Time	Choose the hour and minute that you want CAR to begin loading CDR data from the CDR flat files.
Loading Interval	Choose the interval at which you want records loaded. The interval can range from every 15 minutes to every 24 hours.
Duration	Enter the number of minutes that you want to allow CDR data to load. Depending on the size of the CDR flat files, CAR performance may degrade when CDRs load. You can limit the time that is allowed for loading, but in doing so, the possibility exists that only a portion of the CDR data will be loaded in the time that you set. Be sure to reconcile the duration limit that you place with the interval. For example, if you load CDR data every 15 minutes, the duration of loading cannot exceed 15 minutes.

Uninhibited loading allows you to set a time during which CDR data will load continuously. It will not load CDR data automatically in the duration specified; it will load CDR data uninhibited in the specified duration only if loading starts at that duration per settings done in load CDR and CMR area. So, if loading starts at uninhibited loading interval, it will continue to the end of uninhibited loading interval, plus the duration field set in the load CDR and CMR area.

Uninhibited loading take precedence over any values that are set for scheduled loading. If you do not want uninhibited loading of CDR data, set the From and To values at 00:00.

Step 4 In the Uninhibited Loading of CDR area, complete the fields as described in [Table 25-4](#):

Table 25-4 Uninhibited Loading of CDR Values

Field	Value
From	Choose the hour and minute that you want continuous loading of CDR data to begin.
To	Choose the hour and minute that you want continuous loading of CDR data to end.

Step 5 Click the **Update** button.

CAR will load CDR data based on the time, interval, and duration that you have specified. Changes take effect at midnight. You can force the change to take effect immediately by stopping and restarting the CAR Scheduler service.

Additional Information

See the [“Related Topics” section on page 25-16](#).

Scheduling Daily Reports

The Daily Report Scheduler schedules the time and duration of CAR daily reports.



Note

Report generation can degrade Cisco Unified CallManager performance; schedule reports when performance will be least affected.

Before You Begin

Specify the reports to be generated by using the Automatic Generation/Alert Option. See the [“Configuring Automatic Report Generation/Alert” section on page 26-6](#), for more information.

This section describes how to schedule the time and duration of the automatic daily reports.

Procedure

Step 1 Choose **System > Scheduler > Daily**.

The Daily Scheduler window displays.

Step 2 From the Time drop-down list box, choose the hour and minute that you want daily reports to be generated.

A 24-hour clock represents time, where 0 equals midnight, and 1 through 11 represent a.m. hours, and 12 through 23 represent the p.m. hours of 1 p.m. through 11 p.m., respectively.

Step 3 From the Life drop-down list box, choose the duration of the report from the range of 0 to 12 days.



Tip

If you set the life of the report to 00, the report does not generate.

Step 4 Click the **Update** button.

Reports with report generation interval as Daily in Automatic Generation/Alert Option, and enabled, automatically generate every day at the time that you specified and get deleted after the number of days that you specified.

Changes take effect at midnight. You can force the change to take effect immediately by stopping and restarting the CAR Scheduler service.



Tip

To restore the defaults, click the **Restore Defaults** button. By default, the daily reports run at 1 a.m. every day and get purged after two days.

Additional Information

See the [“Related Topics”](#) section on page 25-16.

Scheduling Weekly Reports

The Weekly Report Scheduler schedules the day, time, and duration of the automatic weekly reports.

**Note**

Report generation can degrade Cisco Unified CallManager performance; schedule reports when performance will be least affected.

Before You Begin

Use the Automatic Generation/Alert Option to specify the reports to be generated. See the [“Configuring Automatic Report Generation/Alert”](#) section on page 26-6, for more information.

This section describes how to schedule the day, time, and duration of the automatic weekly reports.

Procedure

Step 1 Choose **System > Scheduler > Weekly**.

The Weekly Scheduler window displays.

Step 2 From the Day of Week drop-down list box, choose the day that you want reports to be generated.

Step 3 From the Time drop-down list box, choose the hour and minute that you want reports to be generated.

A 24-hour clock represents time, where 0 equals midnight, and 1 through 11 represent a.m. hours, and 12 through 23 represent the p.m. hours of 1 p.m. through 11 p.m., respectively.

Step 4 From the Life drop-down list box, choose the duration of the report from the range of 00 to 12 weeks. The option that you choose indicates how many weeks the report remains on the disk before the report gets deleted.

**Tip**

If you choose 00 for the life of the report, the report does not generate.

Step 5 Click the **Update** button.

Reports with report generation interval as Weekly in Automatic Generation/Alert Option, and enabled, automatically generate every week at the time that you specified and get deleted after the number of weeks that you specified.

Changes take effect at midnight. For the changes to take effect immediately, stop and restart the CAR Scheduler service in the Control Center—Feature Services window.

**Tip**

To restore the defaults, click the **Restore Defaults** button. By default, weekly reports run at 4 a.m. every Sunday and get purged after four weeks.

Additional Information

See the [“Related Topics”](#) section on page 25-16.

Scheduling Monthly Reports

The Monthly Report Scheduler schedules the day, time, and duration of CAR monthly reports.



Note

Report generation can degrade Cisco Unified CallManager performance; schedule reports when performance will be least affected.

Before You Begin

Use the Automatic Generation/Alert Option to specify the reports to be generated. See the [“Configuring Automatic Report Generation/Alert” section on page 26-6](#) for more information.

This section describes how to schedule the day, time, and duration of the automatic monthly reports.

Procedure

- Step 1** Choose **System > Scheduler > Monthly**.

The Monthly Scheduler window displays.

- Step 2** From the Day of Month drop-down list box in the Monthly Bill Generation row, choose the day of the month on which you want the report to be generated.

If you set the value to a day that does not occur in a given month (such as 29, 30, or 31), the report generates on the last day of that month.

- Step 3** From the Time drop-down list box in the Monthly Bill Generation row, choose the hour and minute that you want the report to be generated.

A 24-hour clock represents time, where 0 equals midnight, and 1 through 11 represent a.m. hours, and 12 through 23 represent the p.m. hours of 1 p.m. through 11 p.m., respectively.

- Step 4** From the Life drop-down list box in the Monthly Bill Generation row, choose the duration of the report from the range of 00 to 12 months. The option that you choose indicates how many months the report remains on the disk before the report gets deleted.



Tip

If you choose 00, the reports do not generate.

- Step 5** From the Day of Month drop-down list box in the Other Monthly Reports row, choose the day of the month on which you want the reports generated.

If you set this value to a day that does not occur in a given month (such as 29, 30, or 31), the report generates on the last day of that month.

- Step 6** From the Time drop-down list box in the Other Monthly Reports row, choose the hour and minute that you want reports to be generated.

A 24-hour clock represents time, where 0 equals midnight, and 1 through 11 represent a.m. hours, and 12 through 23 represent the p.m. hours of 1 p.m. through 11 p.m., respectively.

- Step 7** From the Life drop-down list box in the Other Monthly Reports row, choose the life of the report from the range of 00 to 12 months. The option that you choose indicates how many months the report remains on the disk before the report gets deleted.



Tip

If you choose 00, the reports do not generate.

Step 8 Click the **Update** button.

Reports with report generation interval as Monthly in Automatic Generation/Alert Option, and enabled, automatically generate every month at the time that you specified and get deleted after the number of months that you specified.

Changes take effect at midnight. For the changes to take effect immediately, stop and restart the CAR Scheduler service in the Control Center—Feature Services window.

**Tip**

To restore the defaults, click the **Restore Defaults** button. By default, monthly bill reports run at 3 a.m. on the first day of every month and get purged after two months, and other monthly reports run at 2 a.m. on the first day of every month and get purged after two months.

Additional Information

See the [“Related Topics”](#) section on page 25-16.

System Database Configuration

You can configure CAR to notify you when the CAR database size exceeds a percentage of the maximum number of records. You can set the message and the maximum number of records and specify the alert percentage.

You can configure the system to maintain the CAR database size between the low water mark and the high water mark values that you configure through the Configure Automatic Database Purge window. When the database size reaches the low water mark, CAR sends an alert to the user. When the database size reaches the high water mark, the system deletes records based on the deletion age and sends an Email.

See the following sections to configure system database information:

- [Manually Purging or Reloading the CAR Database, page 25-12](#)
- [Configuring Automatic Database Purge, page 25-14](#)
- [System Log Screens, page 25-15](#)

Manually Purging or Reloading the CAR Database

This section describes how to manually purge selected records from the CAR database and how to delete all of the CAR data and reload the database with new CDR data. You may want to reload the database to reclassify calls after dial-plan updates, user-device association changes, call rate changes, and so on.

Procedure

Step 1 Choose **System > Database > Manual Purge**.

The Manual Database Purge window displays.

Step 2 Choose one of the following actions:

- To delete the existing CAR data and reload the CAR database, click the **Reload All Call Detail Records** button.

The system displays a message that indicates that deleting the records may impact system performance. To continue the reload process, click **OK**.

The system begins loading the CDRs into the CAR database within 5 minutes and continues uninterrupted for up to 6 hours. To monitor the progress of the reload, generate the CDR Load event log, as described in the [“Generating the Event Log” section on page 25-15](#).

After the system loads the new records, the system loads the records according to the schedule that is configured in the [“Configuring the CDR Load Schedule” section on page 25-7](#). By default, CDR data loads every day from midnight to 5 a.m.

- To manually purge selected CAR records, continue with [Step 3](#).

Step 3 In the Select Table field, choose the table in the database that you want purged.

To view the tables for which manual purge is permitted, the total number of records in the table, and the latest record and oldest record in the table, click the **Table Information** button.

The Table Information window displays. To return to the Manual Database Purge window, click the **Close** button.

Step 4 In the Delete records field, choose a date that will determine which records will be purged by clicking one of the following radio buttons:

- Older than
- Between

Choose the date range of the CAR records that you want to delete.

Step 5 To delete all records older than or between the dates that you specified, click the **Purge** button.

A prompt advises you that you are about to permanently delete the specified records.

Step 6 To purge the records, click the **OK** button or click the **Cancel** button to abort the purge operation.

If you click **OK**, the records get purged from the selected table. After successful deletion of records, the status message shows the number of records that were deleted from the table.

Additional Information

See the [“Related Topics” section on page 25-16](#).

Configuring Automatic Database Purge

This section describes how to schedule and disable automatic purging of the CAR database. By default, the system enables automatic database purge.

Procedure

Step 1 Choose **System > Database > Configure Automatic Purge**.

The Configure Automatic Database Purge window displays.



Note To restore the default values for the fields in this window, click the **Restore Defaults** button.

Step 2 From the Low Water Mark drop-down list box, choose the minimum percentage of the 6-gigabyte CAR database that you want the system to use for CAR data.



Tip The system notifies you when the CAR database size reaches the low or the high water mark; it also notifies you when the CAR database size exceeds two million records. For information on configuring an Email alert, see the [“Enabling or Disabling Alerts by Mail”](#) section on page 26-8, for instructions.

Step 3 From the High Water Mark drop-down list box, choose the maximum percentage of the 6-gigabyte CAR database that you want the system to use for CAR data.

Step 4 In the Min Age of Call Detail Records field, enter the minimum number of days that you want CAR to use when it purges CDRs from the CAR database. Enter a number between 1 and 180.

When the database size exceeds the high water mark or the number of CDRs in the CAR database exceeds two million records, CAR deletes the CDRs that are older than the number of days that you specified in this field.

Step 5 In the Max Age of Call Detail Records field, enter the maximum number of days that you want to keep the CDRs in the CAR database. Enter a number between 1 and 180.

CAR deletes all CDRs that are older than the specified number of days.

Step 6 Click the **Update** button.

The changes take effect at midnight. To make changes take effect immediately, restart the Cisco CAR Scheduler service.



Tip When CAR loads the CDRs into the CAR database, the CAR Scheduler checks the low and high water marks and the two million record limit. If any threshold is breached, CAR immediately deletes records that are older than the number of days that you specify in [Step 4](#).

Additional Information

See the [“Related Topics”](#) section on page 25-16.

System Log Screens

CAR provides logs that you can use to track the status of the various activities. The event log tracks events that the CAR Scheduler triggers, such as automatically generated reports, loading of CDRs, report deletions, and database purging.

Additional Information

See the [“Related Topics” section on page 25-16](#).

Generating the Event Log

The event log provides a report on the status of the activities that the CAR scheduler controls. The event log report shows whether the tasks have started, completed successfully, or are in progress.

This section describes how to generate the event log report.

Procedure

- Step 1** Choose **System > Log Screens > Event Log**.
The Event Log window displays.
- Step 2** Click the **Daily** radio button to choose daily jobs, the **Weekly** radio button to choose weekly jobs, or the **Monthly** radio button to choose monthly jobs.
- Step 3** In the List of Jobs area, choose the tasks for which you want information.
- Step 4** To add the chosen task to the Selected Jobs area, click the right arrow icon.
- Step 5** To remove tasks from the Selected Jobs area, choose the task that you want removed and click the left arrow icon.
- Step 6** To add tasks with a different frequency, repeat [Step 2](#) through [Step 4](#). For example, you can have daily reports and reports that include monthly or weekly tasks.
- Step 7** Choose the status to include in the report. You must choose at least one status as described in [Table 25-5](#).



Note The system chooses all the job statuses by default.

Table 25-5 Event Log Report Status

Status	Description
Completed	If this check box is checked, the event log report includes tasks that have completed.
In Progress	If this check box is checked, the event log report includes tasks that are currently in progress.
Unsuccessful	If this check box is checked, the event log report includes tasks that have failed.

- Step 8** Choose a date range by choosing From and To values.
- Step 9** To generate the event log report, click the **OK** button.

The event log displays information about the chosen tasks.

[Table 25-6](#) describes the event log report output.

Table 25-6 Event Log Report Output Parameters

Parameter	Description
SI No	Serial number
Jobs	Name of the task
Start Time	Time the task started
End Time	Time the task ended
Status	Unsuccessful, in progress, completed
Date	Date the task was scheduled

Step 10 Print the log by right-clicking on the screen and choosing **Print**.

Additional Information

See the [“Related Topics”](#) section on page 25-16.

Related Topics

- [Configuring Mail Server Parameters, page 25-2](#)
- [Configuring the Dial Plan, page 25-2](#)
- [Restoring the Default Values for the CAR Dial Plan, page 25-4](#)
- [Configuring the CDR Load Schedule, page 25-7](#)
- [Scheduling Daily Reports, page 25-9](#)
- [Scheduling Weekly Reports, page 25-10](#)
- [Scheduling Monthly Reports, page 25-11](#)
- [System Database Configuration, page 25-12](#)
- [Configuring Automatic Database Purge, page 25-14](#)
- [System Log Screens, page 25-15](#)
- [Generating the Event Log, page 25-15](#)
- [Configuring Automatic Report Generation/Alert, page 26-6](#)
- [Configuring Notification Limits, page 26-8](#)
- [QoS by Gateway Configuration, Cisco Unified CallManager CDR Analysis and Reporting Guide, Release 5.0\(4\)](#)
- [Gateway Detail Report Configuration, Cisco Unified CallManager CDR Analysis and Reporting Guide, Release 5.0\(4\)](#)

- Gateway Summary Report Configuration, *Cisco Unified CallManager CDR Analysis and Reporting Guide, Release 5.0(4)*
- Gateway Utilization Reports Configuration, *Cisco Unified CallManager CDR Analysis and Reporting Guide, Release 5.0(4)*



CAR Report Configuration

Use report configuration to define the following parameters:

- Rating parameters for calls—Duration, time of day, voice quality



Note

Rating parameters for calls get used during CAR loading. If you want old CDR records in the CAR database to use new values for these parameters, you must reload all the CDRs in the CAR database.

- Quality of service
- Automatic generation of reports with alerts
- Notification limits

This chapter contains the following topics:

- [Configuring the Rating Engine, page 26-1](#)
- [Defining the Quality of Service \(QoS\) Values, page 26-5](#)
- [Configuring Automatic Report Generation/Alert, page 26-6](#)
- [Configuring Notification Limits, page 26-8](#)
- [Related Topics, page 26-9](#)

Before You Begin

Before you start generating reports with CAR, configure the system. See the “[CAR System Configuration](#)” section on page 25-1.

Configuring the Rating Engine

You can use CAR to set a base monetary rate for the cost of calls based on a time increment. You can further qualify the cost by applying the time-of-day and voice-quality factors. Service providers who must account for service to subscribers commonly use this feature. Some organizations also use this information to establish billing costs for users and departments in the organization for accounting or budgeting purposes.

Reports that use these rating parameters include individual bill, department bill, top N by charge, top N by duration, and top N by number of calls.

**Note**

If you do not change the default value for charge base/block, the cost will always equal zero because the default base charge per block equals zero.

The charge of any call comprises the multiplication of the basic charge of the call, multiplication factor for time of day, and multiplication factor for voice quality. You can set the basic charge for a call through the **Report Config > Rating Engine > Duration** window. Refer to the following list:

- Basic charge = cost, or number of units, applied to the duration block that is specified in the Number of Blocks section
- Number of blocks = total duration of call, in seconds, for which you want the base charge to be applied

You can set the multiplication factor for time of day through the **Report Config > Rating Engine > Time of Day** window. The basis of the settings provides the connect time of the call.

You can set the multiplication factor for voice quality through the **Report Config > Rating Engine > Voice Quality** window.

Setting the Base Rate and Duration

To establish a cost basis for calls, you must specify a base rate for all calls. For example, if your service provider charges you 6 cents for each minute, billed in 10-second increments, you can set the base rate at which all calls are charged at 1 cent for each 10-second increment.

This section describes how to establish the base charge and duration values.

**Note**

If you use the default base charge value, reports do not provide any costs. The system provides default values, but if left to the defaults, the Rating Engine stays disabled and does not provide costs.

Procedure

Step 1 Choose **Report Config > Rating Engine > Duration**.

The Call Duration window displays.

Step 2 In the To (seconds) field, enter the seconds for which you want the base charge to be applied. For example, if you are billed in 6-second increments, enter 6 in this field. If you are billed a flat rate for each minute regardless of call duration, enter 60 in this field, so the charge is based on whole minutes.

Step 3 In the Base Charge/Block field, enter the cost basis for the seconds that are shown in the To (seconds) field. For example, if you are billed 6 cents for each minute in 6-second increments, enter 0.006 in this field. If you are billed 7 cents for each minute in whole minutes (no incremental billing), enter 0.07 in this field.

In the preceding examples, if you are billed in 6-second increments and the cost is 0.006 for each 6-second increment, a call that lasts 7 seconds would cost 0.012. Rationale: Each 6-second increment costs 0.006, and two blocks from 0 to 6 seconds occurred.

Likewise, if you are billed in whole minutes and the cost is 7 cents for each minute, a call that lasted 3 minutes would cost 21 cents. Rationale: Each 60-second increment costs 7 cents, and three blocks of 1 minute occurred.

Step 4 Click the **Update** button.

**Tip**

To restore the default setting, click the **Restore Defaults** button. By restoring the default value of 0 for the call charge/block, you effectively disable the other factors that are used in determining call cost.

Additional Information

See the [“Related Topics”](#) section on page 26-9.

Factoring Time of Day into Call Cost

To further define the cost of calls, you can specify a multiplication factor for certain times of day. For example, if you want to charge subscribers a premium for daytime calls, you can apply a multiplication factor to the base charge/block that you specified in the Call Duration window.

This section describes how to establish certain times of day when calls cost more.

**Note**

If you do not want to increase call cost by time of day, you can use the default values. The default multiplication factor specifies 1, so no increase in call cost for time of day occurs.

Procedure

Step 1 Choose **Report Config > Rating Engine > Time of Day**.

The Time of Day window displays.

Step 2 To add rows, click the **Add Rows** link.

The system adds a row between 00:00:00 and 23:59:59.

Step 3 To add additional rows, check the check box for the row above which you want to add a new row and click the **Add Rows** link.

**Note**

To delete rows, check the check box for the row that you want to delete and click the **Delete Rows** link.

Step 4 Enter the From and To time ranges in 24-hour, minute, and second format. A 24-hour period, from 00:00:00 to 23:59:59, represents the default time range. If you want to set one time-of-day range from 8 am to 5 pm, you will need to establish three time-of-day ranges: the first from 00:00:00 to 07:59:59, the second from 08:00:00 to 16:59:59, and the third from 17:00:00.

**Note**

You must use military time, rather than a 12-hour clock when factoring Time of Day into Call Cost.

- Step 5** Enter the Multiplication Factor that designates a number by which you want the base charge/block to be multiplied when a call occurs in the specified time range. For example, if you charge a premium of double the price for calls that are placed between 8 a.m. and 5 p.m., the multiplication factor would be 2.00. A multiplication factor of 1.00 does not affect the cost of the call.
- Step 6** To add the time-of-day and multiplication factors, click the **Update** button.



Tip To restore the default setting, click the **Restore Defaults** button.

Additional Information

See the [“Related Topics” section on page 26-9](#).

Factoring Voice Quality into Call Cost

To further define the cost of calls, you can specify a multiplication factor for the voice quality of a call. For example, if subscribers are paying a premium price to ensure the highest voice quality on calls, you can apply various multiplication factors to the base charge/block that you specified in the Call Duration window depending on the voice quality. Using a multiplication factor other than 1.00 helps differentiate between the various voice quality calls as well.

This section describes how to establish call cost when calls that have a certain voice quality cost more.



Note If you do not want to increase call cost by voice quality, you can use the default values. The default multiplication factor equals 1.00, so no increase in call cost occurs for voice quality.

Procedure

- Step 1** Choose **Report Config > Rating Engine > Voice Quality**.
The Voice Quality window displays.
- Step 2** In the Multiplication Factor field, enter the number by which you want the base charge/block to be multiplied when a call occurs in the specified voice-quality category. The [“Defining the Quality of Service \(QoS\) Values” section on page 26-5](#), defines the voice-quality categories: Good, Acceptable, Fair, and Poor.

Example

Voice Quality Good; Factor 1.2

Voice Quality Acceptable; Factor 1.0

Voice Quality Fair; Factor 1.0

Voice Quality Poor; Factor 0.8

A good call gets charged 1.2 times that of an acceptable or fair call. A poor call gets charged 0.8 times that of an acceptable or fair call.



Note Multiplication factor for a good call $\geq$ the multiplication factor for acceptable $\geq$ multiplication factor for fair $\geq$ multiplication factor for poor.

Step 3 To set the voice quality multiplication factors, click the **Update** button.



Tip

To restore the default setting, click the **Restore Defaults** button.

Additional Information

See the [“Related Topics”](#) section on page 26-9.

Defining the Quality of Service (QoS) Values

CAR generates Quality of Service reports. To qualify the data that is presented in those reports, CAR uses predefined values that are set about voice quality. Specify the value ranges that are good, acceptable, fair, and poor for jitter, latency, and lost packets. If a call does not satisfy any of the criteria that are set for any of the four voice-quality categories, it receives a classification of NA (not applicable); likewise, if the system is not configured to generate CMR data (or if the CMR is bad), the CMR receives a classification of NA (not applicable).

Enter NA to ignore the values of a parameter. For example, a QoS parameter such as jitter, has NA, and the QoS is defined as good, which means that the QoS depends only on the values of latency and lost packets. All three parameters cannot have NA as values. Infinity designates the maximum value that is available for any parameter. If you specify a rule where a jitter value from 500 to Infinity is considered poor, a call with jitter greater than 500 receives a classification of poor.



Note

Be aware that the classifications of “NA” and “Infinity” are case-sensitive.

This section describes how to define the quality-of-service values.

Procedure

Step 1 Choose **Report Config > Define QoS**.

The Define Quality of Service window displays. [Table 26-1](#) describes the QoS default values.

Table 26-1 QoS Default Values

QoS Parameter	Default
Lost Packets	Good—0.00 to 15.00 Acceptable—15.01 to 30.00 Fair—30.01 to 45.00 Poor—45.01 to infinity
Jitter	Good—0 to 20 Acceptable—21 to 100 Fair—101 to 150 Poor—151 to infinity
Latency	No default values apply.

Step 2 To add rows, check the check box for the row above which you want to add a new row and click the **Add Rows** link.

The new row gets added above the row that you checked, and the check box is cleared.

The rows represent the values that CAR uses to quantify the conditions good, acceptable, fair, and poor in the QoS reports. For each value set, enter the upper and lower limits in the From and To columns.



Note To delete rows, check the check box for the row that you want to delete and click the **Delete Rows** link.

Step 3 For each value that you have set, choose the Quality of Service.

Step 4 Click the **Update** button.



Tip To restore the default QoS values, click the **Restore Defaults** button.

Additional Information

See the [“Related Topics”](#) section on page 26-9.

Configuring Automatic Report Generation/Alert

CAR automatically generates reports based on a schedule. Report generation can include a daily, weekly, or monthly summary report, QoS reports, traffic reports, Device/Route Plan utilization reports, and so on, that you may want to view on a regular basis.



Note In large setups, with a large number of gateways, route groups, route lists, and route patterns, enabling all the Utilization reports (Gateway Utilization, Line Group Utilization, Route Group Utilization, Route List Utilization, and Route Pattern Utilization) increases the CPU usage of the system, therefore increasing the time in which reports are generated. This also affects system performance. Cisco recommends that you enable only Gateway Utilization reports for automatic generation, due to the number of gateways that are typically found in a large system. You can generate all Utilization reports on demand by selecting 15 or less gateways, route groups, route lists, or route groups.

Automatically generating reports involves a two-step process:

- First, enable the reports that you want to generate unless they are enabled by default. See the [“Enabling or Customizing Reports for Automatic Generation”](#) section on page 26-7.
- Second, schedule the reports for the day and time that you want them to generate. (CAR provides a default schedule. If the default schedule is acceptable, only enable the reports that you want to generate automatically.) See the [“System Scheduler Configuration”](#) section on page 25-7.

CAR provides e-mail alerts for various events. Enabling the system for e-mail alerts involves a two-step process:

- First, enable the e-mail alerts. Default enables some, but not all, reports. See the [“Enabling or Disabling Alerts by Mail”](#) section on page 26-8.
- Second, configure the e-mail that is sent when the alert criteria are met.

Additional Information

See the [“Related Topics”](#) section on page 26-9.

Enabling or Customizing Reports for Automatic Generation

This section describes how to enable or disable one or all reports for automatic generation. You can also customize the report parameters and enable a mailing option, so reports get e-mailed when they are created. When the report gets mailed, CAR generates the e-mail address by using the mail ID for the CAR administrator(s) and the mail domain that is configured in the Mail Parameters window; that is, CAR uses <mail ID for the CAR administrator> @ <domain that is configured in the mail parameters window>.

The [“Automatically Generated Reports Schedule”](#) section on page 24-11 describes reports that are enabled by default.

Procedure

Step 1 Choose **Report Config > Automatic Generation/Alert**.

The Automatic Report Generation/Alert Option window displays.

Step 2 In the Reports [Report Generation Interval] box, choose the report that you want to automatically generate based on the schedule that you defined in the System Scheduler. See the [“System Scheduler Configuration”](#) section on page 25-7.

Step 3 In the Status field, choose **Enabled** or **Disabled**.

Step 4 To customize the report or have the report e-mailed when it is generated, click the **Customize Parameters** button.

The Customize Parameters window displays.



Note Each report provides different customization options, depending on the type of report.

Step 5 Choose the CSV or PDF radio button, depending on the type of report that you want the system to mail.

Step 6 To have the report mailed to all CAR administrators, check the **Mailing Option** check box.

Step 7 To save the values that you specified, click the **Update** button.

The Customize Parameters window closes.

Step 8 To enable or customize other reports, repeat [Step 4](#) through [Step 7](#).

Step 9 Click the **Update** button.

Changes take effect at midnight. You can force the change to take effect immediately by stopping and restarting the CAR Scheduler service.

Additional Information

See the [“Related Topics”](#) section on page 26-9.

Enabling or Disabling Alerts by Mail

This section describes how to enable alerts to be mailed to users.

**Note**

For the QoS and Charge Limit Notifications, see the [“Configuring Notification Limits”](#) section on page 26-8.

Procedure

-
- Step 1** Choose **Report Config > Automatic Generation/Alert**.
The Automatic Report Generation/Alert window displays.
- Step 2** In the Alerts by Mail box, choose the alert that you want to enable or disable.
- Step 3** In the Status field, choose **Enabled** or **Disabled**.
- Step 4** Click the **Update** button.
- Step 5** To enable or disable alerts by mail, repeat [Step 2](#) and [Step 4](#).
Changes take effect at midnight. You can force the change to take effect immediately by stopping and restarting the CAR Scheduler service.
-

Additional Information

See the [“Related Topics”](#) section on page 26-9.

Configuring Notification Limits

You can specify limits for QoS and daily charges, so the administrator gets alerted by e-mail when these limits are exceeded. The alerts go to all users that are designated as CAR Administrators through Cisco Unified CallManager Administration. See the “Configuring CAR Administrators, Managers, and Users” section in the *Cisco Unified CallManager CDR Analysis and Reporting Administration Guide, Release 5.0(4)*.

This section describes how to specify the notification limits for QoS and daily charges.

Procedure

-
- Step 1** Choose **Report Config > Notification Limits**.
The Set Limits for Notification window displays.
- Step 2** In the Daily QoS Parameters area, enter a threshold for good and poor calls.
The threshold applies in the form of a percentage of all calls that must be exceeded to trigger an e-mail alert to the administrator. The default for good calls specifies less than 20 percent, meaning that when good calls represent less than 20 percent of all calls per day, an alert gets sent. The default for poor calls specifies greater than 30 percent, meaning that when poor calls represent more than 30 percent of all calls per day, an alert gets sent.
- Step 3** In the Daily Charge Limit area, enter the number of monetary units (such as dollars, francs, or pounds) that, when exceeded by any user in the system, will trigger sending of an e-mail alert to the administrator.

Step 4 Click the **Update** button.

Changes take effect immediately. The new values get used whenever the next alert is sent.

Additional Information

See the [“Related Topics”](#) section on page 26-9.

Related Topics

- [System Parameters Configuration, page 25-1](#)
- [Enabling or Customizing Reports for Automatic Generation, page 26-7](#)
- [Configuring Mail Server Parameters, page 25-2](#)
- [Enabling or Disabling Alerts by Mail, page 26-8](#)
- [Configuring Mail Server Parameters, page 25-2](#)
- [System Scheduler Configuration, page 25-7](#)
- [Configuring the Rating Engine, page 26-1](#)
- [Defining the Quality of Service \(QoS\) Values, page 26-5](#)
- [System Database Configuration, page 25-12](#)
- [Setting the Base Rate and Duration, page 26-2](#)
- [Factoring Time of Day into Call Cost, page 26-3](#)
- [Factoring Voice Quality into Call Cost, page 26-4](#)



CDR Search Configuration

CAR provides reporting capabilities for three levels of users: administrators, managers, and individual users. Only CAR administrators can use CDR Search.

This chapter contains the following topics:

- [Configuring CDR Search by User Extension, page 27-1](#)
- [Configuring CDR Search by Gateway, page 27-3](#)
- [Configuring CDR Search by Cause for Call Termination, page 27-4](#)
- [Viewing Call Termination Details, page 27-5](#)
- [Configuring CDR Search By Call Precedence Levels, page 27-5](#)
- [Configuring CDR Search for Malicious Calls, page 27-7](#)
- [Related Topics, page 27-8](#)

Before You Begin

Make sure that you set the Cisco CallManager service parameters CDR Enabled Flag and Call Diagnostics Enabled to true (enabled), so the system can generate CDR/CMR data. By default, the system disables these service parameters. For more information about these service parameters, refer to the *Cisco Unified CallManager Administration Guide, Release 5.0(4)*.

All CAR reports use CDR data. Be sure to have the most current CDR data from which your reports are built. By default, CDR data loads daily from midnight to 5 a.m. However, you can set the loading time, interval, and duration as needed. See the [“System Scheduler Configuration” section on page 25-7](#) for more information.

Configuring CDR Search by User Extension

Only CAR administrators use the CDR search by user extension feature.

This section describes how to show the details of CDR data based on a user or extension. You can search CDR data by user name and extension. You can narrow the search by specifying both users and extensions in the same search.



Caution

Use CAR only during off-peak hours. Otherwise, data collection and report generation could cause performance degradation on the Cisco Unified CallManager system.

Procedure

Step 1 Choose **CDR > Search > By User/Extension**.

The CDR Search by User Extension window displays.



Note You can enter a wildcard pattern like “!” or “X” to search on extensions. The “!” represents any n digit that has 0-9 as each of its digits, and the “X” represents a single digit in the range 0-9.

Step 2 Perform one of the following tasks:

- To search CDRs based on extensions, enter the extension number in the Extension field and click the **Add Extension** button.
- To search CDRs based on user, click the **Search Extension(s) based on User(s)** link, enter the first few letters of the first and/or last name in the First Name and/or Last Name fields, and click the **Search** button. When the results display, click the **Select** link next to the result that you want to include. Click the **Close** button.

The extension displays in the Selected Extension(s) box.



Note To delete an item from the Report Criteria box, click the **Remove Extension(s)** button. You can delete all items from the Report Criteria box by clicking the **Remove All Extensions** button.

Step 3 Choose the date range of the period for which you want to see CDR data for the specified user or extension.

Tip When you configure the date range, configure the setting, so the number of CDR results does not exceed 15,000. If the results exceed 15,000, CDR search cannot occur, and a message displays to inform you that you must revise the setting.

Step 4 Click the **OK** button.

The CDR-CMR Search Results window displays. The system only displays the oldest 100 records that fall into the date range that you configured in [Step 3](#).

Step 5 To view the CMR data, click the **Others** button. To view both the CDR and CMR data fields, click the **View** button.**Step 6** To mail the report to e-mail recipient(s), follow the steps in the “Mailing a Report” section in the *Cisco Unified CallManager CDR Analysis and Reporting Administration Guide, Release 5.0(4)*.

Additional Information

See the [“Related Topics”](#) section on page 27-8.

Configuring CDR Search by Gateway

Only CAR administrators use the CDR search by gateway feature.

This section describes how to search CDR data based on a specific gateway type or on those gateways that use a chosen route pattern.

**Caution**

Use CAR only during off-peak hours. Otherwise, data collection and report generation could cause performance degradation on the Cisco Unified CallManager system.

Procedure

Step 1 Choose **CDR > Search > By Gateway**.

The CDR Search by Gateway window displays.

Step 2 Perform one of the following tasks:

- To display all the gateways that are configured in the system, click **Gateway Types** in the column on the left side of the window.
- To expand the tree structure and display the type of gateway from which you can choose, click the icon next to Gateway types.
- To choose a gateway that uses a particular route pattern/hunt pilot, rather than a gateway type, click **Route Patterns/Hunt Pilots** in the column on the left side of the window. The gateways that are associated to the configured Route Patterns/Hunt Pilots display.
- To expand the tree structure and display route pattern/hunt pilot for you to choose, click the icon next to Route Patterns/Hunt Pilots.

**Note**

You can also search for specific route patterns/hunt lists by entering part of the name of the route pattern(s)/hunt pilot(s) in the Route Patterns/Hunt Pilots box in the column on the left side of the window. CAR searches for the route pattern(s)/hunt list(s) that matches the search string.

Step 3 Choose a gateway type from the list.

The gateway name displays in the List of Gateways box.

**Note**

The List of Gateways box will display up to 200 gateways that are configured for the chosen gateway type.

Step 4 In the List of Gateways box, choose the gateways that you want to include in the report.

**Note**

You can generate a report for up to 15 gateways at a time.

Step 5 To move the chosen gateway to the list of Selected Gateways box, click the down arrow.

The gateway that you chose displays in the Selected Gateways box.

Step 6 Choose the date and time range of the period during which you want to search CDR data.

**Tip**

When you configure the time range, use Coordinated Universal Time (UTC).

When you configure the date and time ranges, configure the setting, so the number of CDR results does not exceed 15,000. If the results exceed 15,000, CDR search cannot occur, and a message displays to inform you that you must revise the settings.

Step 7 Click the **OK** button.

The CDR-CMR Results window displays. The system only displays the oldest 100 records that fall into the date and time range that you configured in [Step 6](#).

Step 8 To view the CMR data, click the **Others** button. To view both the CDR and CMR data fields, click the **View** button.

Step 9 To mail the report to e-mail recipient(s), follow the steps in the “Mailing a Report” section in the *Cisco Unified CallManager CDR Analysis and Reporting Administration Guide, Release 5.0(4)*.

Additional Information

See the [“Related Topics”](#) section on page 27-8.

Configuring CDR Search by Cause for Call Termination

Only CAR administrators use the CDR Search by Cause for Call Termination feature.

This section describes how to search for information about the cause for termination of a call.

Procedure

Step 1 Choose **CDR > Search > By Cause for Call Termination**.

The Cause for Call Termination window displays.

Step 2 To search for the cause(s) of the termination of a call, highlight the cause(s) in the list of call termination causes.

**Tip**

You can select more than one cause by clicking the causes that you want while holding down the Ctrl key on your keyboard. You can also select all causes in the list by holding down the Shift key while clicking all causes.

Step 3 With the desired cause(s) highlighted, click the down arrow above the Selected Call Termination Causes box.

The cause(s) that you chose displays in the Selected Call Termination Causes list box.

Step 4 Choose the date and time range of the period during which you want to search CDR data.

**Tip**

When you configure the time range, use Coordinated Universal Time (UTC).

Step 5 Click **OK**.

The Call Termination Details window displays the report criteria for which the report has been generated, along with the total number of calls that have been placed during the given time range as well as how many call legs and the percentage of call legs for each cause code that is selected.

- Step 6** To view CDRs, see the [“Viewing Call Termination Details” section on page 27-5](#).
-

Additional Information

See the [“Related Topics” section on page 27-8](#).

Viewing Call Termination Details

This section describes how to view the call termination details.

Before You Begin

Follow the steps in the [“Configuring CDR Search by Cause for Call Termination” section on page 27-4](#) to display the Call Termination Details window.

Procedure

- Step 1** In the Select CDRs field, check the check box beside the individual CDRs that you want to view or, if you want to view all CDRs in the list, check the **Select CDRs** check box.
- Step 2** After you have chosen the CDRs that you want to view, click **View CDRs**.
The CDR-CMR Search Results window displays.
To view the media information and the CDR-CMR dump records, click the **Others** and **View** links. See the [“Understanding the CDR Search Results” section on page 28-23](#) for information on how to read CDR search results reports.
- Step 3** To mail the report in an e-mail, click **Send Report** and follow the procedure described in the “Mailing a Report” section in the *Cisco Unified CallManager CDR Analysis and Reporting Administration Guide, Release 5.0(4)*.
-

Additional Information

See the [“Related Topics” section on page 27-8](#).

Configuring CDR Search By Call Precedence Levels

Only CAR administrators use the CDR Search by Call Precedence Levels feature.

This section describes how to search for calls according to call precedence.

Procedure

- Step 1** Choose **CDR > Search > By Call Precedence Level**.
The CDR Search by Precedence Levels window displays.

- Step 2** In Select Precedence Levels, check the check box(es) for the call precedence level(s) on which you want to search as described in [Table 27-1](#).

Table 27-1 Call Precedence Levels

Voice Quality	Description
Flash Override	Highest precedence setting for MLPP calls.
Flash	Second highest precedence setting for MLPP calls.
Immediate	Third highest precedence setting for MLPP calls.
Priority	Forth highest precedence setting for MLPP calls.
Routine	Lowest precedence setting for MLPP calls.



Note To check the check boxes of every precedence level, click **Select All**. To clear the check boxes, click **Clear All**.

- Step 3** In the From Date field, choose the date and time from which you want CDRs searched.



Tip When you configure the time range, use Coordinated Universat Time (UTC).

When you configure the date and time ranges, configure the setting, so the number of CDR results does not exceed 15,000. If the results exceed 15,000, CDR search cannot occur, and a message displays to inform you that you must revise the settings.

- Step 4** In the To Date field, choose the date and time to which you want CDRs searched.

- Step 5** Click **OK**.

The Call Precedence Details window displays and shows the call precedence levels and values, number of call legs, and percentage of call legs.

- Step 6** In the Select CDRs column, check the check box(es) of the CDR(s) at which you want to look.

- Step 7** Click **View CDRs**.

The CDR-CMR Search by Precedence Levels - CDR-CMR Search Results window displays. The system displays only the oldest 100 records that fall into the date and time ranges that you configured in [Step 3](#) and [Step 4](#).

- Step 8** To view the CMR data, click the **Others** button. To view both the CDR and CMR data fields, click the **View** button.

- Step 9** To mail the report to e-mail recipient(s), click **Send Report** and follow the steps in the “Mailing a Report” section in the *Cisco Unified CallManager CDR Analysis and Reporting Administration Guide, Release 5.0(4)*.

Additional Information

See the [“Related Topics”](#) section on page 27-8.

Configuring CDR Search for Malicious Calls

Only CAR administrators use the CDR Search for Malicious Calls feature.

This section describes how to search for malicious calls.

Procedure

Step 1 Choose **CDR > Search > Malicious Calls**.

The CDR Search for Malicious calls window displays.

Step 2 Perform one of the following tasks:

- In the Select Extension(s) box, enter an extension in the Extension field and click **Add Extension**. The extension of the user displays in the Selected Extension(s) box.
- To search for a user extension, click the **Search Extension(s) based on User(s)** link, enter the first few letters of the first and/or last name in the First Name and/or Last Name fields, and click the **Search** button. When the results display, click the **Select** link next to the result that you want to include. The extension number that is associated with the user appears in the Selected Extension(s) box. Click the **Close** button.



Note To remove an extension, highlight the extension(s) that you want removed and click **Remove Extension(s)**. To remove all extensions, click **Remove All Extensions**.

Step 3 Choose the date and time range of the period when you want to search CDR data.



Tip When you configure the time range, use Coordinated Universal Time (UTC).

When you configure the date and time ranges, configure the setting, so the number of CDR results does not exceed 15,000. If the results exceed 15,000, CDR search cannot occur, and a message displays to inform you that you must revise the settings.

Step 4 Click **OK**.

The CDR-CMR Search Results window displays. The system only displays the oldest 100 records that fall into the date and time ranges that you configured in [Step 3](#).

Step 5 To view the CMR data, click the **Others** button. To view both the CDR and CMR data fields, click the **View** button.

Step 6 To mail the report to e-mail recipient(s), follow the steps in the “Mailing a Report” section in the *Cisco Unified CallManager CDR Analysis and Reporting Administration Guide, Release 5.0(4)*.

Additional Information

See the [“Related Topics” section on page 27-8](#).

Related Topics

- [Understanding the CDR Search Results, page 28-23](#)
- [Media Information, page 28-25](#)
- [CDR and CMR Dump Tables, page 28-25](#)
- [Mailing a Report, *Cisco Unified CallManager CDR Analysis and Reporting Administration Guide, Release 5.0\(4\)*.](#)
- [Configuring CDR Search by User Extension, page 27-1](#)
- [Configuring CDR Search by Gateway, page 27-3](#)
- [Configuring CDR Search by Cause for Call Termination, page 27-4](#)
- [Viewing Call Termination Details, page 27-5](#)
- [Configuring CDR Search By Call Precedence Levels, page 27-5](#)
- [Configuring CDR Search for Malicious Calls, page 27-7](#)



CAR Report Results



Tip

When a logged-in Cisco Extension Mobility user makes a call, CAR uses the user ID that is configured for the Cisco Extension Mobility user in all reports that display a user ID. When the call is made by a non-Cisco Extension Mobility user (or logged-out Cisco Extension Mobility user) and when the call is made with a device that does not have a configured Owner User ID, CAR uses the default user ID, `_unspecifieduser`, in the report.

This chapter describes report output information for each CAR report type:

- [Bill Summary Report Results, page 28-2](#)
- [Bill Detail Report Results, page 28-3](#)
- [Top N By Charge or Duration Report Results, page 28-4](#)
- [Top N By Number of Calls Report Results, page 28-5](#)
- [Call Usage for Cisco IPMA Assistant—Detail, page 28-6](#)
- [Call Usage for Cisco IPMA Assistant—Summary, page 28-7](#)
- [Call Usage for Cisco IPMA Manager—Detail, page 28-8](#)
- [Call Usage for Cisco IPMA Manager—Summary, page 28-8](#)
- [Cisco IP Phone Services Report Results, page 28-9](#)
- [QoS Detail Report Results, page 28-9](#)
- [QoS Summary Report Results, page 28-11](#)
- [QoS by Gateways Report Results, page 28-11](#)
- [QoS by Call Types Report Results, page 28-11](#)
- [Traffic Summary Report Results, page 28-12](#)
- [Authorization Code Name Call Details, page 28-14](#)
- [Authorization Level Call Details, page 28-14](#)
- [Client Matter Code Details, page 28-15](#)
- [Malicious Call Details Report Results, page 28-15](#)
- [Precedence Call Summary Report Results, page 28-15](#)
- [System Overview Report Results, page 28-16](#)
- [CDR Error Report Results, page 28-17](#)

- [Gateway Detail Report Results, page 28-18](#)
- [Gateway Summary Report Results, page 28-19](#)
- [Gateway and Route Utilization Report Results, page 28-21](#)
- [Conference Call Detail Report Results, page 28-21](#)
- [Conference Bridge Utilization Report Results, page 28-22](#)
- [Voice Messaging Utilization Report Results, page 28-23](#)
- [Understanding the CDR Search Results, page 28-23](#)
- [Media Information, page 28-25](#)
- [CDR and CMR Dump Tables, page 28-25](#)

Bill Summary Report Results

The report groups information by the user name in ascending order. The summary report includes the following fields (see [Table 28-1](#)).

Table 28-1 **Summary Report Fields**

Field	Description
Call Classification—Call categories specify classes.	
Internal	Intracuster calls that originated in the Cisco Unified CallManager network and ended in the same Cisco Unified CallManager network (no gateways are used).
Local	Local calls that are routed through the public switched telephone network (PSTN) to numbers without an area code or that include one of the local area codes.
Long Distance	Long-distance calls that originate in the Cisco Unified CallManager network that go out through the PSTN.
International	International calls that originate in the Cisco Unified CallManager network that go out through the PSTN.
On Net	Outgoing, intercluster calls that originate on one Cisco Unified CallManager cluster and terminate on a different cluster.
Others	All other outgoing calls, such as toll-free numbers or emergency calls such as 911.
QOS—The number of calls for each Quality of Service category. Parameters that the CAR administrator sets provided basis for QoS categories; see “Defining the Quality of Service (QoS) Values” and “Configuring QoS Parameters” in the <i>Cisco Unified CallManager CDR Analysis and Reporting Guide, Release 5.0(4)</i> .	
Good	QoS for these calls designates the highest possible quality.

Table 28-1 Summary Report Fields (continued)

Field	Description
Acceptable	QoS for these calls shows them slightly degraded but still falls within an acceptable range.
Fair	QoS for these calls, although degraded, still fall within a usable range.
Poor	QoS for these calls was unsatisfactory.
NA	These calls did not match any criteria for the established QoS categories.
Calls—Indicates the number of calls for each call classification.	
Charge—Indicates the charge that is associated with each call. Call charge information that the CAR administrator provides for the CAR rating engine provides basis for charges. See “Configuring the Rating Engine” in the <i>Cisco Unified CallManager CDR Analysis and Reporting Guide, Release 5.0(4)</i> .	

Bill Detail Report Results

The report groups information by the user name in ascending order. The detail report includes the following fields (see [Table 28-2](#)).

Table 28-2 Detail Report Fields

Field	Description
Date and Orig. Time	The date and time that the call originated.
Orig.	The originating number from which the call was placed.
Dest.	The destination number to which the call was directed.
Call Classification—Call categories specify classes.	
Internal	Intracluster calls that originated in the Cisco Unified CallManager network and ended in the same Cisco Unified CallManager network (no gateways are used).
Local	Local calls that are routed through the public switched telephone network (PSTN) to numbers without an area code or that include one of the local area codes.
Long Distance	Long-distance calls that originate in the Cisco Unified CallManager network that go out through the PSTN.
International	International calls that originate in the Cisco Unified CallManager network that go out through the PSTN.
On Net	Outgoing, intercluster calls that originate on one Cisco Unified CallManager cluster and terminate on a different cluster.

Table 28-2 *Detail Report Fields (continued)*

Field	Description
Others	All other outgoing calls, such as toll-free numbers or emergency calls such as 911.
QoS—The number of calls for each Quality of Service category. Parameters that the CAR administrator sets provided basis for QoS categories; see “Defining the Quality of Service (QoS) Values” and “Configuring QoS Parameters” in the <i>Cisco Unified CallManager CDR Analysis and Reporting Guide, Release 5.0(4)</i> .	
Good	QoS for these calls designates the highest possible quality.
Acceptable	QoS for calls that are slightly degraded but still within an acceptable range.
Fair	QoS for calls, that although degraded, still within a usable range.
Poor	QoS for calls that are unsatisfactory.
NA	Calls that did not match any criteria for the established QoS categories.
Duration(s)	The time, in seconds, that the call remained connected.
Charge	The charge that is associated with each call. Call charge information that the CAR administrator provided for the CAR rating engine provides basis for charges. See “Configuring the Rating Engine” in the <i>Cisco Unified CallManager CDR Analysis and Reporting Guide, Release 5.0(4)</i> .

Top N By Charge or Duration Report Results

The fields for the Top N by Charge and the Top N by Duration vary depending on the report type. The reports show only outgoing calls. See [Table 28-3](#).

Table 28-3 *Top N by Charge and by Duration Report Fields*

Field	Description
By Individual Users	
User	User names.
Calls	Total number of calls.
Duration(s)	The time, in seconds, that the call was connected.
Charge	The charge that is associated with each call. Call charge information that the CAR administrator provided for the CAR rating engine provides basis for charges. See “Configuring the Rating Engine” in the <i>Cisco Unified CallManager CDR Analysis and Reporting Guide, Release 5.0(4)</i> .
By Destinations	

Table 28-3 Top N by Charge and by Duration Report Fields (continued)

Field	Description
Dest	The destination of the calls.
Call Classification	The total number of calls for each call classification.
Calls	Total number of calls.
Duration	The time, in seconds, that the call was connected.
Charge	The charge that is associated with each call. Call charge information that the CAR administrator provided for the CAR rating engine provides basis for charges. See “Configuring the Rating Engine” in the <i>Cisco Unified CallManager CDR Analysis and Reporting Guide, Release 5.0(4)</i> .
By Number of Calls	
User	User names.
Date	Date that the call occurred.
Orig Time	Time that the calls originated.
Orig	Origin of the calls.
Dest	Destination of the calls.
Call Classification	The total number of calls for each call classification.
Duration	The time, in seconds, that the call was connected.
Charge	The charge that is associated with each call. Call charge information that the CAR administrator provided for the CAR rating engine provides basis for charges. See “Configuring the Rating Engine” in the <i>Cisco Unified CallManager CDR Analysis and Reporting Guide, Release 5.0(4)</i> .

Top N By Number of Calls Report Results

The fields for the Top N by Number of Calls report vary depending on the report type. The report shows both incoming and outgoing calls. See [Table 28-4](#).

Table 28-4 Top N by Number of Calls Report Fields

Field	Description
By Individual Users	
Users	User names.
Duration(s)	The time, in seconds, that the call connected.

Table 28-4 Top N by Number of Calls Report Fields (continued)

Field	Description
Charge	The total amount of billing charges for all calls to that user. Call charge information that the CAR administrator provided for the CAR rating engine provides basis for charges. See “Configuring the Rating Engine” in the <i>Cisco Unified CallManager CDR Analysis and Reporting Guide, Release 5.0(4)</i> .
Calls Made	The total number of calls that the user placed.
Calls Received	The total number of calls that the user received.
Total Calls	The total number of incoming and outgoing calls.
By Extensions	
Extension No	The extension that originated/placed and received the call.
Charge	The total amount of billing charges for all calls to that user. Call charge information that the CAR administrator provided for the CAR rating engine provides basis for charges. See “Configuring the Rating Engine” in the <i>Cisco Unified CallManager CDR Analysis and Reporting Guide, Release 5.0(4)</i> .
Duration	The time, in seconds, that the call was connected.
Calls Made	The total number of calls that the user placed.
Calls Received	The total number of calls that the user received.
Total Calls	The total number of incoming and outgoing calls.

Call Usage for Cisco IPMA Assistant—Detail

The report shows the number of calls that assistants handled for themselves, that the assistant handled for each manager, and the total number of calls that the assistant handled. The report groups information about calls that the assistant handled and calls that the assistant handled for the manager. The detail report includes the following fields (see [Table 28-5](#)).

Table 28-5 Detail Report Fields

Field	Description
Date	The date that the call originated.
Orig. Time	The time that the call originated.
Orig.	The originating number from which the call was placed.
Dest.	The destination number to which the call was directed.

Table 28-5 *Detail Report Fields (continued)*

Field	Description
Call Classification	The type of call (internal, incoming, and so on.)
Duration (sec)	The time, in seconds, that the call connected.

Call Usage for Cisco IPMA Assistant—Summary

The report shows information about calls that the assistant handled for themselves and that the assistant handled for the manager. The reports groups call information by attendant name. The summary report includes the following fields (see [Table 28-6](#)).

Table 28-6 *Summary Report Fields*

Field	Description
Assistant-Extn/Manager	Shows the assistant name and directory number. If the assistant handles a call for a manager, the manager name displays.
Call Classification—Call categories specify classes.	
Internal	Intracuster calls that originated in the Cisco Unified CallManager network and ended in the same Cisco Unified CallManager network (no gateways are used).
Local	Local calls that are routed through the public switched telephone network (PSTN) to numbers without an area code or that include one of the local area codes.
Long Distance	Long-distance calls that originate in the Cisco Unified CallManager network that go out through the PSTN.
International	International calls that originate in the Cisco Unified CallManager network that go out through the PSTN.
Incoming	Inbound calls that originated outside the Cisco Unified CallManager network, entered through a gateway, and went into the Cisco Unified CallManager network.
On Net	Outgoing, intercluster calls that originate on one Cisco Unified CallManager cluster and terminate on a different cluster.
Others	All other outgoing calls, such as toll-free numbers or emergency calls such as 911.
Calls	The number of calls that the assistant handled or the assistant handled for the manager.
Duration (sec)	The total duration for all the calls for the particular call classification.

Call Usage for Cisco IPMA Manager—Detail

The report provides information about calls that managers handle for themselves and that assistants handle for managers. The report groups information by the assistant name and shows the total number of calls that the manager handles and that the assistant handles for the manager. The detail report includes the following fields (see [Table 28-7](#)).

Table 28-7 **Detail Report Fields**

Field	Description
Date	The date that the call originated.
Orig. Time	The time that the call originated.
Orig.	The originating number from which the call was placed.
Dest.	The destination number to which the call was directed.
Call Classification	The type of call (internal, incoming, and so on.)
Duration (sec)	The time, in seconds, that the call connected.

Call Usage for Cisco IPMA Manager—Summary

The report shows information about calls that the managers handle for themselves and that the assistants handle for the managers. The report groups information by the manager name and shows the total number of calls that are handled for each manager. The report includes the following fields (see [Table 28-8](#)).

Table 28-8 **Summary Report Fields**

Field	Description
Manager-Extn/Assistant	Shows the manager name and directory number. If the assistant handles a call for a manager, the assistant name displays.
Call Classification—Call categories specify classes.	
Internal	Intracuster calls that originated in the Cisco Unified CallManager network and ended in the same Cisco Unified CallManager network (no gateways are used).
Local	Local calls that are routed through the public switched telephone network (PSTN) to numbers without an area code or which include one of the local area codes.
Long Distance	Long-distance calls that originate in the Cisco Unified CallManager network that go out through the PSTN.

Table 28-8 *Summary Report Fields (continued)*

Field	Description
International	International calls that originate in the Cisco Unified CallManager network that go out through the PSTN.
Incoming	Inbound calls that originated outside the Cisco Unified CallManager network, entered through a gateway, and went into the Cisco Unified CallManager network.
On Net	Outgoing, intercluster calls that originate on one Cisco Unified CallManager cluster and terminate on a different cluster.
Others	All other outgoing calls, such as toll-free numbers or emergency calls such as 911.
Calls	The number of calls that the assistant or the manager handles.
Duration	The total duration for all the calls for the particular call classification.

Cisco IP Phone Services Report Results

The Cisco Unified IP Phone Services report includes the following fields. See [Table 28-9](#).

Table 28-9 *Cisco Unified IP Phone Services Report Fields*

Field	Description
Cisco IP Phone Services	The name of the selected service.
Number of Subscribers	The total number of subscribers for a given service.
% Subscription	The percentage of users who have subscribed to a given service, out of the total number of subscriptions for all services.

QoS Detail Report Results

The QoS detail report includes the following fields. See [Table 28-10](#).

Table 28-10 *QoS Detail Report Fields*

Field	Description
Orig. Time	The time that the call was placed, in 24-hour, minute, and second format.
Term. Time	The time that the call disconnected, in 24-hour, minute, and second format.

Table 28-10 QoS Detail Report Fields (continued)

Field	Description
Duration(s)	The amount of time, in seconds, that the call was connected.
Orig.	The originating number from which the call was placed.
Dest.	The destination number to which the call was directed.
Call Classification—Call categories specify classes.	
Internal	Intracenter calls that originated in the Cisco Unified CallManager network and ended in the same Cisco Unified CallManager network (no gateways are used).
Local	Local calls that are routed through the public switched telephone network (PSTN) to numbers without an area code or that include one of the local area codes.
Long Distance	Long-distance calls that originate in the Cisco Unified CallManager network that go out through the PSTN.
International	International calls that originate in the Cisco Unified CallManager network that go out through the PSTN.
On Net	Outgoing, intercluster calls that originate on one Cisco Unified CallManager cluster and terminate on a different cluster.
Incoming	Inbound calls that originated outside the Cisco Unified CallManager network, entered through a gateway, and went into the Cisco Unified CallManager network.
Tandem	Inbound calls that originated outside the Cisco Unified CallManager network, entered the Cisco Unified CallManager network through a gateway, and were transferred outbound from the Cisco Unified CallManager network through a gateway.
Others	All other outgoing calls, such as toll-free numbers or emergency calls such as 911.
Orig. Codec	The codec that the originating device uses.
Dest. Codec	The codec that the destination device uses.
Orig. Device	The name of the device that placed the call.
Dest. Device	The name of the device that received the call.

Table 28-10 QoS Detail Report Fields (continued)

Field	Description
Orig. QoS	The voice quality that the device that placed the call experienced.
Dest. QoS	The voice quality that the device that received the call experienced.

QoS Summary Report Results

The QoS summary report includes the following fields. See [Table 28-11](#).

Table 28-11 QoS Summary Report Fields

Field	Description
Quality of Service	The quality of service of the calls.
Call Legs	Number of call legs with the quality of service that the Quality of Service field specified.

QoS by Gateways Report Results

The QoS by gateways report provides the following information. See [Table 28-12](#).

Table 28-12 QoS Gateway Report Fields

Field	Description
Time/Day	Indicates the cumulative hours of the day(s), the days of the week, or the days of the month for the selected date range.
% of Call Legs	Displays the percentage of calls for each gateway for the hours of the day, the days of the week, or the days of the month for the selected date range.

QoS by Call Types Report Results

The QoS by call types report provides the following information. See [Table 28-13](#).

Table 28-13 QoS Call Type Report Fields

Field	Description
Time/Day	The cumulative hours of the day(s), the days of the week, or the days of the month for the selected date range.
% of Call Legs	The percentage of calls for each gateway for the hours of the day, the days of the week, or the days of the month for the selected date range.
Internal	Intracuster calls that originated in the Cisco Unified CallManager network and ended in the same Cisco Unified CallManager network (no gateways are used).
Local	Local calls that are routed through the public switched telephone network (PSTN) to numbers without an area code or that include one of the local area codes.
Long Distance	Long-distance calls that originate in the Cisco Unified CallManager network that go out through the PSTN.
International	International calls that originate in the Cisco Unified CallManager network that go out through the PSTN.
On Net	Outgoing, intercluster calls that originate on one Cisco Unified CallManager cluster and terminate on a different cluster.
Incoming	Inbound calls that originated outside the Cisco Unified CallManager network, entered through a gateway, and went into the Cisco Unified CallManager network.
Tandem	Inbound calls that originated outside the Cisco Unified CallManager network, entered the Cisco Unified CallManager network through a gateway, and were transferred outbound from the Cisco Unified CallManager network through a gateway.
Others	All other outgoing calls, such as toll-free numbers or emergency calls such as 911.

Traffic Summary Report Results

The traffic summary and traffic summary by extension reports contain the same information and include some or all the following fields. See [Table 28-14](#).

Table 28-14 **Traffic Summary Report Fields**

Field	Description
Time/Day	The cumulative hours of the day(s), the days of the week, or the days of the month for the selected date range.
Average Number of Calls	The percentage of calls for each gateway for the hours of the day, the days of the week, or the days of the month for the selected date range.
Internal	Intracenter calls that originated in the Cisco Unified CallManager network and ended in the same Cisco Unified CallManager network (no gateways are used).
Local	Local calls that are routed through the public switched telephone network (PSTN) to numbers without an area code or that include one of the local area codes.
Long Distance	Long-distance calls that originate in the Cisco Unified CallManager network that go out through the PSTN.
International	International calls that originate in the Cisco Unified CallManager network that go out through the PSTN.
On Net	Outgoing, intercluster calls that originate on one Cisco Unified CallManager cluster and terminate on a different cluster.
Incoming	Inbound calls that originated outside the Cisco Unified CallManager network, entered through a gateway, and went into the Cisco Unified CallManager network.
Tandem	Inbound calls that originated outside the Cisco Unified CallManager network, entered the Cisco Unified CallManager network through a gateway, and were transferred outbound from the Cisco Unified CallManager network through a gateway.
Others	All other outgoing calls, such as toll-free numbers or emergency calls such as 911.
Total	The total number of calls for each hour or day.

Authorization Code Name Call Details

This report shows the usage of specific authorization code names. For security purposes, the authorization code name (description) displays and not the authorization code. The detail report includes the following fields (see [Table 28-15](#)).

Table 28-15 *Detail Report Fields*

Field	Description
Orig.	The originating number from which the call was placed.
Dest.	The destination number to which the call was directed.
Orig. Date Time	The date and time that the call originated.
Duration (sec)	The time, in seconds, that the call connected.
Call Classification	The type of call (internal, incoming, on so on.)
Authorization Level	The authorization level for calls for each chosen authorization code name.

Authorization Level Call Details

This report shows the usage of specific authorization levels. The detail report includes the following fields (see [Table 28-16](#)).

Table 28-16 *Detail Report Fields*

Field	Description
Orig.	The originating number from which the call was placed.
Dest.	The destination number to which the call was directed.
Orig. Date Time	The date and time that the call originated.
Duration (sec)	The time, in seconds, that the call connected.
Call Classification	The type of call (internal, incoming, and so on.)
Authorization Code Name	The authorization code name for each authorization level that you chose.

Client Matter Code Details

The report shows the usage of specific client matter codes. The detail report includes the following fields (see [Table 28-17](#)).

Table 28-17 *Detail Report Fields*

Field	Description
Orig.	The originating number from which the call was placed.
Dest.	The destination number to which the call was directed.
Orig. Date Time	The date and time that the call originated.
Duration (sec)	The time, in seconds, that the call connected.
Call Classification	The type of call (internal, incoming, and so on.)

Malicious Call Details Report Results

The Malicious Call Details report provides information about malicious calls. The report provides the following fields. See [Table 28-18](#).

Table 28-18 *Malicious Call Details Report Fields*

Field	Description
Orig. Time	Time at which the malicious call originated.
Term. Time	Time at which the malicious call terminated.
Duration	Total time of malicious call in seconds.
Orig.	Originating DN.
Dest.	Destination DN.
Orig. Device	Name of the originating device.
Dest. Device	Name of the destination device.
Call Classification	Classification of the malicious call.

Precedence Call Summary Report Results

The Precedence Call Summary report provides information about calls based on precedence levels. The report displays the call summary for the precedence values in the form of a bar chart on an “Hour of Day,” “Day of Week,” or “Day of Month” basis for each precedence level that you choose. Two tables, one reflecting the bar chart, and the other listing the “Number of Calls” and “Percentage” for each precedence level that was chosen, display in the report. See [Table 28-19](#).

Table 28-19 **Precedence Call Summary Report Fields**

Field	Description
Time/Day	Indicates the cumulative hours of the day(s), the days of the week, or the days of the month for the selected date range.
Call Legs	Number of calls for each precedence level by time/day.
Precedence Level	Precedence level value of the call.
No. of Call Legs	Number of call legs per each precedence level.
Percentage	Percentage of calls per each precedence level.

System Overview Report Results

The system overview provides information about all parts of the Cisco Unified CallManager network. The report provides the following sections. See [Table 28-20](#).

Table 28-20 **System Overview Report**

Field	Description
Top 5 Users based on Charge	Details the five users who have incurred the highest charges for calls that occurred during the specified date range. See “Top N By Charge or Duration Report Results” section on page 28-4.
Top 5 Destinations based on Charge	Details the five called numbers that have incurred the highest charges for calls during the specified date range. See the “Top N By Charge or Duration Report Results” section on page 28-4.
Top 5 Calls based on Charge	Details the five calls that have incurred the highest charges for calls during the specified date range. See the “Top N By Charge or Duration Report Results” section on page 28-4 for details about this section of the system overview report.
Top 5 Users based on Duration	Details the five users who have spent the most time on calls during the specified date range. See “Top N By Charge or Duration Report Results” section on page 28-4 for details about this section of the system overview report.
Top 5 Destinations based on Duration	Details the five called numbers that have been engaged in calls for the longest time during the specified date range. See the “Top N By Charge or Duration Report Results” section on page 28-4 for details about this section of the system overview report.

Table 28-20 **System Overview Report (continued)**

Field	Description
Top 5 Calls based on Duration	Details the five longest calls for the specified date range. See the “Top N By Charge or Duration Report Results” section on page 28-4 for details about this section of the system overview report.
Traffic Summary Report - Hour of Day	Shows the volume of calls during the specified date range based on each hour of the day. See the “Traffic Summary Report Results” section on page 28-12 for details about this section of the system overview report.
Traffic Summary Report - Day of Week	Shows the volume of calls during the specified date range based on each day of the week. See the “Traffic Summary Report Results” section on page 28-12 for details about this section of the system overview report.
Traffic Summary Report - Day of Month	Shows the volume of calls during the specified date range based on each day of the month. See the “Traffic Summary Report Results” section on page 28-12 for details about this section of the system overview report.
Quality of Service Report - Summary	Shows the number of calls that fell within each voice-quality category during the specified date range. See the “QoS Summary Report Results” section on page 28-11 for details about this section of the system overview report.
Gateway Summary Report	Shows the summary of the call classification for each gateway along with the QoS, the number of calls, and the duration for each classification for the gateway during the specified date range. See the “QoS by Gateways Report Results” section on page 28-11 for details about this section of the system overview report.

CDR Error Report Results

The CDR error report provides the following information. See [Table 28-21](#).

Table 28-21 **CDR Error Report Fields**

Field	Description
Time	The hour for the specified day that the error occurred.
No of Error CDRs	The total number of CDR data records that were not processed during loading into CAR due to an error.

Table 28-21 CDR Error Report Fields (continued)

Field	Description
No of Valid CDRs	The total number of CDR data records that were successfully loaded to CAR.
% of Error CDRs	The percentage of failed CDR data records out of all the CDR data records to be loaded.
Error Description	An error that occurred when the system was trying to load the CDR data records.
% of Error CDRs	The percentage of CDR data records that failed due to the corresponding error description.

Gateway Detail Report Results

The gateway detail report includes the following fields. See [Table 28-22](#).

Table 28-22 Gateway Detail Report Fields

Field	Description
Date	The date when the call went through the gateway.
Orig. Time	The time when the call went through the gateway.
Term. Time	The time that the call terminated.
Duration(s)	The duration, in seconds, that the call was connected. The duration specifies the difference between the Dest Connect and the Dest Disconnect times.
Orig	The directory number from which the call was placed.
Dest	The directory number to which the call was originally placed. If the call was not forwarded, this directory number should match the Final Destination number. If the call was forwarded, this field contains the original destination number of the call before it was forwarded.
Orig. Codec	The codec code (compression or payload code) that the call originator used on its sending side during this call. This code may differ from the codec code that was used on its receiving side.
Dest. Codec	The codec code (compression or payload code) that the destination used on its sending side during this call. This code may differ from the codec code that was used on its receiving side.
Orig. Device	The device name of the device that placed the call. For incoming and tandem calls, this field specifies the device name of the gateway.

Table 28-22 Gateway Detail Report Fields (continued)

Field	Description
Dest Device	The device name of the device that received the call. For outgoing and tandem calls, this field specifies the device name of a gateway. For conference calls, this field specifies the device name of the conference bridge.
Orig QoS	Quality of service shows the voice-quality grade that was achieved for the calls.
Dest QoS	The QoS category that was experienced by the receiver of the call.

Gateway Summary Report Results

The gateway summary report includes the following fields. See [Table 28-23](#).



Note

The gateway summary report segregates calls for each call classification that the user selects and divides the calls based on QoS type.

Table 28-23 Gateway Summary Report Fields

Field	Description
Call Classification	Shows the type of call (internal, incoming, and tandem.)
Quality of Service	Shows a summary of the performance of the various gateways with the total number of calls for each voice-quality category. The parameters set in “Defining the Quality of Service (QoS) Values” in the <i>Cisco Unified CallManager CDR Reporting and Analysis Guide, Release 5.0(4)</i> , provide the basis for all voice-quality categories. • Good—QoS for these calls specifies the highest possible quality. • Acceptable—QoS for these calls, although slightly degraded, still falls within an acceptable range. • Fair—QoS for these calls, although degraded, still falls within a usable range. • Poor—QoS for these calls was unsatisfactory. • NA—These calls did not match any criteria for the established QoS categories.
Calls	Shows the total calls for the particular call classification.

Table 28-23 *Gateway Summary Report Fields (continued)*

Field	Description
Duration(s)	Shows the total duration for all the calls for the particular call classification.

Gateway and Route Utilization Report Results

The gateway, route group, route list, and route pattern utilization reports provide similar output. If you generate these reports in CSV format, the report displays in a table. If you chose PDF, the report shows the utilization as a bar chart. A graph displays for each selected gateway or route group. See [Table 28-24](#).

Table 28-24 Gateway and Route Utilization Report Fields

Field	Description
Time/Day	Time in one-hour blocks if you chose Hourly or one-day blocks if you chose weekly or monthly. The results show the utilization for each hour or day for the entire period that is shown in the from and to dates.
% of Calls	Gateway, route group, route list, or route pattern utilization percentage. This field gives the cumulative utilization percentage of the gateways or route groups or route lists or route patterns relative to the total number of calls that all the gateways put together can support at any one time.

Conference Call Detail Report Results

You can choose to generate Conference Call information in either a summary or a detailed report. The reports display the call details in a table whether you chose to generate the report in the CSV or PDF format. The following tables show the fields in the Conference Call Detail and Summary reports. See [Table 28-25](#) and [Table 28-26](#).



Note

The report criteria include the type of conference (ad hoc and/or meet-me) and the From and To date range.

Table 28-25 Conference Call Detail Summary Report Fields

Field	Description
Orig. Time	Time that the first participant enters the conference.
Term. Time	Time that the last participant leaves the conference.
No. of Participants	Number of participants in the conference.
Duration	Sum of the duration of individual participants in the conference in seconds.
Device Name	Names of the conference devices that were used.

Table 28-26 Conference Call Detail Report Fields

Field	Description
Conference Start Time	Time at which conference started.
Conference End Time	Time at which conference ended.
Connect Time	Time at which conference participants connected to conference.
Disconnect Time	Time at which conference participants disconnected from conference.
Duration	Total time of conference.
Directory Number	Directory number of participants.
Call Classification	Call types of conference (internal, incoming, and so on.)
Device Name	Names of the conference devices that were used.
QoS	Quality of service.

Conference Bridge Utilization Report Results

The report provides the following fields. If you chose CSV output, the report displays the utilization in a table. If you chose PDF, the report shows the utilization as a bar chart. See [Table 28-27](#).

Table 28-27 Conference Bridge Utilization Report Fields

Field	Description
Time/Day	Time in one-hour blocks if you chose Hourly or one-day blocks if you chose day of week or daily.
% Usage	Conference bridge utilization percentage.
Conf. Bridge	The conference bridge device that is used to hold conference calls.
Type	Either hardware or software conference bridge.
Max Streams	The number of conferences that can be held at a time along with the number of people per conference.

Voice Messaging Utilization Report Results

The report provides the following fields. If you chose CSV output, the report displays the utilization in a table. If you chose PDF, the report shows the utilization as a bar chart. See [Table 28-28](#).

Table 28-28 Voice-Messaging Utilization Report Fields

Field	Description
% Usage	Voice-messaging percentage.
Time/Day	Time in one-hour blocks if you chose Hourly or one-day blocks if you chose day of week or daily.
Voice Messaging Ports	The sum of the maximum number of ports for all the gateways under the route patterns that are configured for Octel voice-messaging system and the entries in the Device table of Cisco Unified CallManager that have type Class as 8.
Voice Messaging Gateways	The originating or destination device name as the gateways under the route patterns that are configured for Octel system.
Number of Ports	The number of ports that the voice-messaging gateway supports.

Understanding the CDR Search Results

The following sections describe CDR search results: the “[Understanding the Results for CDR Search](#)” section on page 28-23, the “[Media Information](#)” section on page 28-25, and the “[CDR and CMR Dump Tables](#)” section on page 28-25.

Understanding the Results for CDR Search

The CDR search allows users to view the CDR/CMR fields as described in “[CDR and CMR Dump Tables](#)” section on page 28-25. The CDR search retrieves the CDR/CMR files from the tbl_billing_data and tbl_billing_error tables of the CAR database.

See [Table 28-29](#).

Table 28-29 CDR Search Results

Field	Description
Sl No	This field specifies the serial or record number.
Call Type	This field specifies the type of call: simple, transfer, forward, pickup, conference, refer, replaces, or redirection.
GCID_CMId GCID_CallId	This field specifies the call identifiers that are associated with all the records for the entire call.

Table 28-29 CDR Search Results (continued)

Field	Description
Orig Node Id Dest Node Id	This field specifies the node within the Cisco Unified CallManager cluster where the call originator/destination was registered at the time of the call.
Orig Leg Id Dest Leg Id	This field specifies the unique identifiers (within a cluster) to the originating/destination leg of a call.
Calling No Calling Partition	The calling number specifies the directory number where the call originated. The calling partition specifies the partition that is associated with the calling party.
Called No Called Partition	The called number specifies the directory number from which the call was initially placed and is the same as the Dest No when the call is not transferred or forwarded. The called partition specifies the partition that is associated with the called party.
Dest No Dest No Partition	The destination number specifies the directory number where the call finally terminated and is the same as the called number when the call is not transferred or forwarded. The destination number partition specifies the partition that is associated with the destination number.
Last Rd. No Last Rd. No Partition	The last redirected number specifies the directory number from which the call was finally redirected. The last redirected number partition specifies the partition that is associated with the last redirected number.
Media Info Orig Pkts Rcd Dest Pkts Rcd Orig Pkts Lost Dest Pkts Lost	This field specifies the packets that were received or lost for the origination or destination leg of a call and a link to the media information. See the “CDR and CMR Dump Tables” section on page 28-25 for information about the CDR and CMR Dump tables.
CDR - CMR Dump	This field specifies a link to the CDR and CDR dump tables. This link allows the users to view the values in the CDR/CMR fields. See the “CDR and CMR Dump Tables” section on page 28-25 for information about the CDR and CMR Dump tables.

Media Information

The media information table provides following information. See [Table 28-30](#).

Table 28-30 CDR Media Information

Field	Description
Origination Leg	A unique identifier (within a cluster) for the originating leg of a call.
Destination Leg	A unique identifier (within a cluster) for the destination leg of a call.
Parameter	The media parameters MediaTransportAdd_IP, PayLoadCapability, MediaCap_g723BitRate, packets sent, octets sent, packets received, octets received, packets lost, jitter, latency, VideoCap_Codec, VideoCap_Bandwidth, VideoCap_Resolution, VideoTransportAddress_IP, VideoTransportAddress_Port, and QoS.
Origination	The value for all the preceding parameters for the origination leg of the call.
Destination	The value for all the preceding parameters for the destination leg of the call.

CDR and CMR Dump Tables

The CDR and CMR dump tables provide the following information. See [Table 28-31](#).



Note

You can view the content of the voice quality metrics field, varVQMetrics, in the Origination CMR and Destination CMR fields.

Table 28-31 CDR and CMR Dump Tables

Field	Description
CDR	This field specifies the call detail record fields.
Origination CMR	Only a single set of fields for origination and destination exists. You can find the origination or destination CMR by using the leg IDs. If the leg IDs of the CMR match the Orig/Dest leg ID of the CDR, the following record represents Orig/Dest CMR.
Destination CMR	Only a single set of fields for origination and destination exists. You can find the origination or destination CMR by using the leg IDs. If the leg IDs of the CMR match the Orig/Dest leg ID of the CDR, the following record represents Orig/Dest CMR.



PART 8

Cisco Unified CallManager Call Detail Record Definitions





Call Detail Record Definitions

This document describes the changes to the call detail records (CDRs) and call management records (CMRs) for Cisco Unified CallManager Release 5.1(1).

The only change for Cisco Unified CallManager Release 5.1(1) is the addition of a single new codec type, Media_Payload_AAC = 42, as noted in the following table.

Codec Types

[Table 29-1](#) contains the compression and payload types that may appear in the codec fields.

Table 29-1 **Codec Types**

Value	Description
1	NonStandard
2	G711Alaw 64k
3	G711Alaw 56k
4	G711mu-law 64k
5	G711mu-law 56k
6	G722 64k
7	G722 56k
8	G722 48k
9	G7231
10	G728
11	G729
12	G729AnnexA
13	Is11172AudioCap
14	Is13818AudioCap
15	G.729AnnexB
16	G.729 Annex AwAnnexB
18	GSM Full Rate
19	GSM Half Rate

Table 29-1 *Codec Types (continued)*

Value	Description
20	GSM Enhanced Full Rate
25	Wideband 256K
32	Data 64k
33	Data 56k
40	G7221 32K
41	G7221 24K
42	Media_Payload_AAC
80	GSM
81	ActiveVoice
82	G726_32K
83	G726_24K
84	G726_16K
100	H261
101	H263
102	Vieo
103	H264
106	H224



PART 9

Cisco Unified CallManager Security Guide





Security Overview

Implementing security mechanisms in the Cisco Unified CallManager system prevents identity theft of the phone/Cisco Unified CallManager server, data tampering, and call-signaling/media-stream tampering.

The Cisco IP telephony network establishes and maintains authenticated communication streams, digitally signs files before transferring the file to the phone, and encrypts media streams and call signaling between Cisco Unified IP Phones.

This chapter provides information on the following topics:

- [Authentication and Encryption Terminology, page 30-2](#)
- [System Requirements, page 30-4](#)
- [Features List, page 30-4](#)
- [Security Icons, page 30-5](#)
- [Interactions and Restrictions, page 30-5](#)
- [Best Practices, page 30-10](#)
- [Installation, page 30-12](#)
- [TLS and IPSec, page 30-12](#)
- [Certificates, page 30-12](#)
- [Authentication, Integrity, and Authorization Overview, page 30-15](#)
- [Encryption Overview, page 30-19](#)
- [Configuration Checklist Overview, page 30-21](#)
- [Where to Find More Information, page 30-25](#)

Authentication and Encryption Terminology

The definitions in [Table 30-1](#) apply when you configure authentication and encryption for your Cisco IP telephony network:

Table 30-1 Terminology

Term	Definition
Access control list (ACL)	List that defines rights and permissions to access system functions and resources. See Method List.
Authentication	Process that verifies the identity of an entity.
Authorization	Process that specifies whether an authenticated user, service, or application has the necessary permissions to perform a requested action; in Cisco Unified CallManager, security process that restricts SUBSCRIBE requests and certain trunk-side SIP requests to authorized users.
Authorization Header	A SIP user agent response to a challenge.
Certificate Authority (CA)	Entity that issues certificates; may be a Cisco or third-party entity.
Certificate Authority Proxy Function (CAPF)	Process by which supported devices can request locally significant certificates by using Cisco Unified CallManager Administration.
Certificate Trust List (CTL)	A file that contains a list of certificates that the phone is to trust. The Cisco Site Administrator Security Token (security token) signs the CTL file. The CTL file gets created automatically when the Cisco CTL client is used to transition the cluster to secure/mixed-mode.
Challenge	In digest authentication, a request to a SIP user agent to authenticate its identity.
Cisco Site Administrator Security Token (security token; etoken)	A portable hardware security module that contains a private key and an X.509v3 certificate that the Cisco Certificate Authority signs; used for file authentication, it signs the CTL file.
Device Authentication	Process that validates the identity of the device and ensures that the entity is what it claims to be before making a connection.
Digest Authentication	A form of device authentication where an MD5 hash of a shared password (among other things) gets used to establish the identity of a SIP User agent.
Digest User	User name that is included in the authorization request that SIP phones or SIP trunks send.
Encryption	Process that ensures that only the intended recipient receives and reads the data; process that ensures the confidentiality of the information; process that translates data into ciphertext, which appears random and meaningless. Requires an encryption algorithm and encryption key.
File Authentication	Process that validates digitally signed files that the phone downloads. The phone validates the signature to make sure that file tampering did not occur after the file creation.
Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)	An IETF-defined protocol that ensures (at a minimum) the identity of the HTTPS server; by using encryption, ensures the confidentiality of the information that is exchanged between the Tomcat server and the browser client.

Table 30-1 Terminology (continued)

Term	Definition
Image Authentication	Process that prevents tampering with the binary image prior to loading it on the phone; process whereby a phone validates the integrity and source of an image.
Integrity	Process that ensures that data tampering did not occur between entities.
IPSec	Transport that provides secure H.225, H.245, and RAS signaling channels for end-to-end security.
Locally Significant Certificate (LSC)	A digital X.509v3 certificate that is installed on the phone or JTAPI/TAPI/CTI application; issued by a third-party certificate authority or CAPF.
Manufacture Installed Certificate (MIC)	A digital X.509v3 certificate that is signed by the Cisco Certificate Authority and installed in supported phones by Cisco Manufacturing.
Man-in-the-Middle Attacks	Process that allows an attacker to observe and modify the information flow between Cisco Unified CallManager and the phone.
Media Encryption	Process whereby the confidentiality of the media is protected by use of cryptographic procedures. Media encryption uses Secure Real-Time Protocol (SRTP) as defined in IETF RFC 3711.
Message/Data Tampering	Event when an attacker attempts to alter messages in transit, including ending a call prematurely.
Method List	Tool to restrict certain categories of messages that can come in on a SIP trunk during the authorization process; defines which SIP nonINVITE methods are allowed for a trunk-side application or device. Also Method ACL.
Mixed Mode	Mode within a cluster that you configured for security; includes authenticated and nonauthenticated devices that connect to the Cisco Unified CallManager.
Nonce	A unique, random number that the server generates for each digest authentication request.
Nonsecure Call	Call in which at least one device is not authenticated or encrypted.
PKI	Public key infrastructure; the set of elements that is needed for public key encryption, including certificates and certificate authorities.
Replay Attack	Event when an attacker captures information that identifies a phone or proxy server and replays information while pretending to be the actual device; for example, by impersonating the proxy server private key.
System Administrator Security Token (SAST)	In CTI/JTAPI/TAPI applications, a token that is used to sign the CTL file for CTL download.
Simple Certificate Enrollment Protocol (SCEP)	A protocol that is used to communicate with a certificate authority that issues X.509 certificates.
Secure Call	Call in which all devices are authenticated and the media stream is encrypted.
Signaling Authentication	Process that validates that no tampering occurred to signaling packets during transmission; uses the Transport Layer Security protocol.

Table 30-1 Terminology (continued)

Term	Definition
Signaling Encryption	Process that uses cryptographic methods to protect the confidentiality of all signaling messages that are sent between the device and the Cisco Unified CallManager server.
SIP Realm	A string (name) that specifies protected space in digest authentication; identifies the line- or trunk-side user agent for the SIP request.
SSL	A cryptographic protocol that secures data communications such as e-mail on the Internet. Consider SSL as equivalent to TLS, its successor.
Transport Layer Security (TLS)	A cryptographic protocol that secures data communications such as e-mail on the Internet. Consider TLS as functionally equivalent to SSL.
Trust List	Certificate list without digital signatures.
Trust Store	A repository of X.509 certificates that are explicitly trusted by an application, such as Cisco Unified CallManager.
X.509	An ITU-T cryptographic standard for importing PKI certificates, which includes certificate formats.

System Requirements

The following system requirements exist for authentication or encryption:

- Cisco Unified CallManager Release 5.1(1) serves as the minimum requirement for the security features that this document describes.
- The Administrator password can differ on every server in the cluster.
- The username and password that are used at the Cisco CTL client (to log in to the Cisco Unified CallManager server) matches Cisco Unified CallManager Administration username and password (the username and password that are used to log in to the Cisco Unified CallManager Administration).
- For Certificate Authority Proxy Function (CAPF) information, see “CAPF System Interactions and Requirements” in the Using the Certificate Authority Proxy Function chapter in the *Cisco Unified CallManager Security Guide, Release 5.0(4)*.
- Before you configure voice mail ports for security, verify that you installed a version of Cisco Unity that supports Cisco Unified CallManager Release 5.1.

Features List

Cisco Unified CallManager system uses a multilayered approach to call security, from the transport layer to the application layer.

Transport layer security includes TLS and IPSec for signaling authentication and encryption to control and prevent access to the voice domain. SRTP adds media authentication and encryption to secure privacy and confidentiality for voice conversation and other media.

[Table 30-2](#) provides a summary of security features that Cisco Unified CallManager can implement during a SIP or SCCP call, depending on the features that are supported and configured.

Table 30-2 **Call Processing Security Features List**

Security Feature	Line Side	Trunk Side
Transport/Connection/Integrity	Secure TLS port	IPSec associations Secure TLS port (SIP trunk only)
Device Authentication	TLS certificate exchange w/Cisco Unified CallManager and/or CAPF	IPSec certificate exchange or pre-shared key
Digest Authentication	SIP phone users only	SIP trunk users and SIP trunk application users
Signaling Authentication/Encryption	TLS Mode: authenticated or encrypted	IPSec [authentication header, encryption (ESP), or both] TLS Mode: authenticated or encrypted mode (SIP trunk only)
Media Encryption	SRTP	SRTP
Authorization	Presence requests	Presence requests Method list

Note: The features that are supported on a device vary by device type and protocol.

Security Icons

Phones that support security icons display the Cisco Unified CallManager security level that is associated with a call.

- The phone displays a shield icon for calls with a signaling security level of authenticated. A shield identifies a secured connection between Cisco IP devices.
- The phone displays a lock icon for calls with encrypted media, meaning the media stream between the Cisco IP devices is encrypted.

Refer to [“Phone Icons and Encryption” section on page 30-9](#) for restrictions that are associated with security icons.

Interactions and Restrictions

This section contains information on the following topics:

- [Interactions, page 30-5](#)
- [Restrictions, page 30-6](#)

Interactions

This section describes how Cisco security features interact with Cisco Unified CallManager applications.

To add presence group authorization for SIP phones and trunks, configure presence groups to restrict presence requests to authorized users.

**Note**

Refer to the *Cisco Unified CallManager Features and Services Guide* for more information about configuring presence groups.

To allow presence requests on SIP trunks, you must authorize Cisco Unified CallManager to accept presence requests on the SIP trunk and, if required, configure end user clients in Cisco Unified CallManager Administration to allow Cisco Unified CallManager to accept and authenticate incoming presence requests from the remote device and application.

To use SIP-initiated transfer features and other advanced transfer-related features on SIP trunks, such as Web Transfer and Click to Dial, you must authorize Cisco Unified CallManager to accept incoming Out of Dialog REFER requests.

To provide support for event reporting (such as MWI support) and to reduce per-call MTP allocations (from a voice-messaging server for example), you must authorize Cisco Unified CallManager to accept Unsolicited Notification SIP requests.

To allow Cisco Unified CallManager to transfer an external call on a SIP trunk to an external device or party (in attended transfer, for example) you must authorize Cisco Unified CallManager to accept SIP requests with replaces header in REFERS and INVITES.

For extension mobility, the SIP digest credentials change when a user logs in and out because different credentials are configured for different end users.

Cisco Unified CallManager Assistant supports a secure connection to CTI (transport layer security connection); the administrator must configure a CAPF profile (one for each Cisco Unified CallManager Assistant node).

When multiple instance of a CTI/JTAPI/TAPI application are running, CTI TLS support requires administrators to configure a unique instanceID (IID) for every application instance to secure signaling and media communication streams between CTI Manager and JTAPI/TSP/CTI applications.

When the device security mode equals authenticated or encrypted, the Cisco Unity-CM TSP connects to Cisco Unified CallManager through the Cisco Unified CallManager TLS port. When the security mode equals nonsecure, the Cisco Unity TSP connects to Cisco Unified CallManager through the Cisco Unified CallManager port.

Restrictions

The following sections describe restrictions that apply to Cisco security features:

- [Authentication and Encryption, page 30-7](#)
- [Barge and Encryption, page 30-7](#)
- [Wideband Codecs and Encryption, page 30-8](#)
- [Media Resources and Encryption, page 30-8](#)
- [Device Support and Encryption, page 30-8](#)
- [Phone Icons and Encryption, page 30-9](#)
- [Cluster and Device Security Modes, page 30-9](#)
- [Packet Capturing and Encryption, page 30-9](#)

Authentication and Encryption

Consider the following restrictions before you install and configure authentication and encryption features:

- Auto-registration does not work when you configure the cluster for mixed mode.
- You cannot implement signaling or media encryption if device authentication does not exist in the cluster; that is, if you do not enable the Cisco CTL Provider service or install and configure the Cisco CTL client.
- Cisco does not support Network Address Translation (NAT) with Cisco Unified CallManager if you configure the cluster for mixed mode.

You can enable UDP in the firewall to allow media stream firewall traversal. Enabling UDP allows the media source on the trusted side of the firewall to open a bidirectional media flow through the firewall by sending the media packet through the firewall.

**Tip**

Hardware DSP resources cannot initiate this type of connection and, therefore, must exist outside of the firewall.

Signaling encryption does not support NAT traversal. Instead of using NAT, consider using LAN extension VPNs.

- SRTP encrypts voice packets only.

Barge and Encryption

The following restrictions apply to barge and encryption:

- A Cisco Unified IP Phone model 7960 (SCCP) and 7970 user cannot barge in to an encrypted call if the Cisco Unified IP Phone model 7970 that is used to barge is not configured for encryption. When barge fails in this case, a busy tone plays on the phone where the user initiated the barge.

If the initiator phone is configured for encryption, the barge initiator can barge in to an authenticated or nonsecure call from the encrypted phone. After the barge occurs, Cisco Unified CallManager classifies the call as nonsecure.

If the initiator phone is configured for encryption, the barge initiator can barge in to an encrypted call, and the phone indicates that the call state equals encrypted.

A user can barge in to an authenticated call, even if the phone that is used to barge is nonsecure. The authentication icon continues to display on the authenticated devices in the call, even if the initiator phone does not support security.

**Tip**

You can configure cbarge if you want barge functionality, but Cisco Unified CallManager automatically classifies the call as nonsecure.

- If you configure encryption for Cisco Unified IP Phone models 7960 and 7940, those encrypted devices cannot accept a barge request when they are participating in an encrypted call. When the call is encrypted, the barge attempt fails. A tone plays on the phone to indicate that the barge failed.

A message displays in Cisco Unified CallManager Administration when you attempt the following configuration:

- In the Phone Configuration window, you apply a security profile that supports encryption, you choose **On** for the Built In Bridge setting (or default setting equals On), and you click **Save** after you create this specific configuration.
- In the Service Parameter window, you update the Built In Bridge Enable parameter.

Wideband Codecs and Encryption

The following information applies for Cisco Unified IP Phone models 7960 or 7940 that are configured for encryption and associated with a wideband codec region. This only applies to Cisco Unified IP Phone models 7960 or 7940 that are configured for TLS/SRTP.

To establish an encrypted call, Cisco Unified CallManager ignores the wideband codec and chooses another supported codec from the codec list that the phone presents. If the other devices in the call are not configured for encryption, Cisco Unified CallManager may establish the authenticated/nonsecure call by using the wideband codec.

Media Resources and Encryption

Cisco Unified CallManager supports authenticated and encrypted calls between secure Cisco Unified IP Phones (SCCP or SIP), secure CTI devices/route points, secure Cisco MGCP IOS gateways, secure SIP trunks, secure H.323 gateways, and secure H.323/H.245/H.225 trunks where no media resources are used. For example, Cisco Unified CallManager Release 5.1 does not provide media encryption in the following cases:

- Calls that involve transcoders or media termination points
- Ad hoc or Meet-Me conferences
- Calls that involve music on hold

Device Support and Encryption

Some Cisco Unified IP Phone models, such as Cisco Unified IP Phone model 7912, do not support encrypted calls. Some phones support encryption but do not validate certificate signatures. Refer to the Cisco Unified IP Phone administration guides for Cisco Unified IP Phone models that support encryption and this version of Cisco Unified CallManager for more information.



Note

In this release, the following Cisco Unified SCCP IP Phone models support encryption: 7906, 7911, 7940, 7941, 7941G-GE, 7960, 7961, 7961G-GE, 7970, 7971. The following Cisco Unified SIP IP Phone models support encryption: 7906, 7911, 7941, 7941G-GE, 7961, 7961G-GE, 7970, 7971.

Cisco Unified SIP IP Phone models 7940/7960 do not support signaling encryption with TLS.

SIP trunks do not support SRTP encryption; Cisco Unified CallManager secures calls on SIP trunks with TLS.

**Note**

Cisco Unified CallManager supports SRTP primarily for IOS gateways and Cisco Unified CallManager H.323 trunks on gatekeeper-controlled and non-gatekeeper-controlled trunks. If SRTP cannot be engaged for a call, Cisco Unified CallManager engages RTP.

Not all phones support encrypted configuration files. Some phones support encrypted configuration files but do not validate file signatures. All phones that support encrypted configuration files require new firmware (except Cisco Unified IP Phone models 7905 and 7912) that is compatible with this release to receive full encrypted configuration files. Cisco Unified IP Phone models 7905 and 7912 use existing security mechanisms and do not require new firmware for this feature.

Refer to [Supported Phone Models, page 33-4](#) for phone support of encrypted configuration files.

Phone Icons and Encryption

The encryption lock icon indicates that the media stream between the Cisco IP devices is encrypted.

The encryption lock icon may not display on the phone when you perform tasks such as conferencing, transferring, or putting a call on hold; the status changes from encrypted to nonsecure if the media streams that are associated with these tasks are not encrypted.

Cisco Unified CallManager does not display the lock icon for calls that originate at or terminate to SIP trunk-side connections. Cisco Unified CallManager does not display the shield icon for calls that are transiting H.323 trunks.

Cluster and Device Security Modes

When the cluster security mode equals nonsecure, the device security mode equals nonsecure in the phone configuration file, even though Cisco Unified CallManager Administration may indicate that the device security mode is authenticated or encrypted. Under these circumstances, the phone attempts nonsecure connections with the SRST-enabled gateway and the Cisco Unified CallManager servers in the cluster.

When the cluster security mode equals nonsecure, the security-related configuration in Cisco Unified CallManager Administration gets ignored; for example, the device security mode, the SRST Allowed check box, and so on. The configuration does not get deleted in Cisco Unified CallManager Administration, but security does not get provided.

The phone attempts a secure connection to the SRST-enabled gateway only when the cluster security mode equals secure, the device security mode in the phone configuration file is set to authenticated or encrypted, the SRST Allowed? check box is checked in the Trunk Configuration window, and a valid SRST certificate exists in the phone configuration file.

Packet Capturing and Encryption

When SRTP encryption is implemented, third-party sniffing tools do not work. Authorized administrators with appropriate authentication can initiate packet capturing in Cisco Unified CallManager Administration with a configuration change in Cisco Unified CallManager Administration (for devices that support packet capturing).

Best Practices

Cisco strongly recommends the following best practices:

- Always perform installation and configuration tasks in a secure lab environment before you deploy to a wide-scale network.
- Use IPSec for gateways and other application servers at remote locations; for example, Cisco Unity or Cisco Unified Contact Center or other Cisco Unified CallManager servers.

**Caution**

Failure to use IPSec in these instances results in session encryption keys getting transmitted in the clear.

- To prevent toll fraud, configure conference enhancements that are described in the *Cisco Unified CallManager System Guide*. Likewise, you can perform configuration tasks to restrict external transferring of calls. For information on how to perform this task, refer to the *Cisco Unified CallManager Features and Services Guide*.

This section contains the following topics:

- [Resetting the Devices, Restarting Services, or Rebooting the Server/Cluster, page 30-10](#)
- [Configuring Media Encryption with Barge, page 30-11](#)

Resetting the Devices, Restarting Services, or Rebooting the Server/Cluster

This section describes when you need to reset the devices, to restart services in Cisco Unified CallManager Serviceability, or to reboot the server/cluster.

Consider the following guidelines:

- Reset a single device after you apply a different security profile in Cisco Unified CallManager Administration.
- Reset the devices if you perform phone-hardening tasks.
- Reset the devices after you change the clusterwide security mode from mixed to nonsecure mode (or vice versa).
- Restart all devices after you configure the Cisco CTL client or update the CTL file.
- Reset the devices after you update CAPF enterprise parameters.
- Restart the Cisco CTL Provider service after you update ports for the TLS connection.
- Restart the Cisco CallManager service after you change the clusterwide security mode from mixed to nonsecure mode (or vice versa).
- Restart the Cisco Certificate Authority Proxy Function service after you update associated CAPF service parameters.
- Restart all Cisco CallManager and Cisco TFTP services in Cisco Unified CallManager Serviceability after you configure the Cisco CTL client or update the CTL file. Perform this task on all servers that run these services.
- Restart all Cisco CallManager and Cisco TFTP services after you start or stop the CTL Provider service.
- Reset dependent devices after you configure secure SRST references.
- If you set the Smart Card service to Started and Automatic, reboot the PC where you installed the Cisco CTL client.

- Restart the Cisco CallManager IP Manager Assistant Service, Cisco WebDialer Web Service, and the Cisco Extended Functions service after you configure the security-related service parameters that are associated with the Application User CAPF Profile.

To restart the Cisco CallManager service, refer to the *Cisco Unified CallManager Serviceability Administration Guide*.

To reset a single device after updating the configuration, see the [“Applying a Phone Security Profile” section on page 32-9](#).

To reset all devices in the cluster, perform the following procedure:

Procedure

-
Step 1	In Cisco Unified CallManager Administration, choose System > Cisco Unified CallManager . The Find/List window displays.
Step 2	Click Find . A list of configured Cisco Unified CallManager servers displays.
Step 3	Choose the Cisco Unified CallManager on which you want to reset devices.
Step 4	Click Reset .
Step 5	Perform Step 2 and Step 4 for each server in the cluster.
-

Configuring Media Encryption with Barge

Use the following information with the [“Barge and Encryption” section on page 30-7](#).

When you attempt to configure barge for Cisco Unified IP Phone models 7960 and 7940 that are configured for encryption, the following message displays:

If you configure encryption for Cisco Unified IP Phone models 7960 and 7940, those encrypted devices cannot accept a barge request when they are participating in an encrypted call. When the call is encrypted, the barge attempt fails.

The message displays when you perform the following tasks in Cisco Unified CallManager Administration:

- In the Phone Configuration window, you choose **Encrypted** for the Device Security Mode (or System Default equals Encrypted) and **On** for the Built In Bridge setting (or default setting equals On), and you click **Insert** or **Update** after you create this specific configuration.
- In the Enterprise Parameter window, you update the Device Security Mode parameter.
- In the Service Parameter window, you update the Built In Bridge Enable parameter.



Tip

For changes to take effect, you must reset the dependent Cisco IP devices.

Installation

To obtain authentication support, you install a plug-in, the Cisco CTL client, from Cisco Unified CallManager Administration. To install the Cisco CTL client, you must obtain at least two security tokens.

Media and signaling encryption capabilities automatically install when you install Cisco Unified CallManager.

Cisco Unified CallManager automatically installs Secure Sockets Layer (SSL) for Cisco Unified CallManager virtual directories.

Cisco Certificate Authority Proxy Function (CAPF) installs automatically as a part of Cisco Unified CallManager Administration.

TLS and IPsec

Transport security handles the coding, packing, and sending of data. Cisco Unified CallManager provides the following secure transport protocols:

- Transport Layer Security (TLS) provides secure and reliable data transfer between two systems or devices by using secure ports and certificate exchange. TLS secures and controls connections between Cisco Unified CallManager-controlled systems, devices, and processes to prevent access to the voice domain. Cisco Unified CallManager uses TLS to secure SCCP calls to SCCP phones and SIP calls to SIP phones or trunks.
- IP Security (IPsec) provides secure and reliable data transfer between Cisco Unified CallManager and gateways. IPsec implements signaling authentication and encryption to Cisco IOS MGCP and H.323 gateways.

You can add secure RTP (SRTP) to TLS and IPsec transport services for the next level of security on devices that support SRTP. SRTP authenticates and encrypts the media stream (voice packets) to ensure that voice conversations that originate at or terminate to Cisco Unified IP Phones and either TDM or analog voice gateway ports are protected from eavesdroppers who may have gained access to the voice domain. SRTP adds protection against replay attacks.

Certificates

Certificates secure client and server identities. After root certificates are installed, certificates get added to the root trust stores to secure connections between users and hosts, including devices and application users.

Administrators can view the fingerprint of server certificates, regenerate self-signed certificates, and delete trust certificates at the Cisco Unified Communications Operating System GUI.

Administrators can also regenerate and view self-signed certificates at the command line interface (CLI).

For information on updating the Cisco Unified CallManager trust store and managing certificates, refer to the *Cisco Unified Communications Operating System Administration Guide, Release 5.0(4)*.

**Note**

Cisco Unified CallManager supports only PEM (.pem) and DER (.der) formatted certificates.

This section contains information on the following topics:

- [Phone Certificate Types, page 30-13](#)
- [Server Certificate Types, page 30-13](#)
- [Support for Certificates from External CAs, page 30-14](#)

Phone Certificate Types

Cisco uses the following certificate types in phones:

- **Manufacture-installed certificate (MIC)**—Cisco Manufacturing automatically installs this certificate in supported phone models. With certain phone models, one MIC and one locally significant certificate (LSC) can exist in the same phone, in which case, the LSC takes precedence over the MIC for authentication to the Cisco Unified CallManager after you configure the device security mode for authentication or encryption.

You cannot overwrite or delete the manufacture-installed certificate.

- **Locally significant certificate (LSC)**—This certificate type installs on supported phones after you perform the necessary tasks that are associated with the Cisco Certificate Authority Proxy Function (CAPF). With certain phone models, one LSC and one MIC can exist in the same phone, in which case, the LSC takes precedence over the MIC for authentication to the Cisco Unified CallManager after you configure the device security mode for authentication or encryption.



Tip

Cisco recommends using manufacturer-installed certificates (MICs) for LSC installation only. Cisco supports LSCs to authenticate the TLS connection with Cisco Unified CallManager. Because MIC root certificates can be compromised, customers who configure phones to use MICs for TLS authentication or for any other purpose do so at their own risk. Cisco assumes no liability if MICs are compromised.

Cisco recommends upgrading Cisco Unified IP Phone models 7906, 7911, 7941, 7961, 7970, and 7971 to use LSCs for TLS connection to Cisco Unified CallManager and removing MIC root certificates from the CallManager trust store to avoid possible future compatibility issues. Some phone models that use MICs for TLS connection to Cisco Unified CallManager may not be able to register.

Administrators should remove the following MIC root certificates from the CallManager trust store:

CAP-RTP-001

CAP-RTP-002

Cisco_Manufacturing_CA

Cisco_Root_CA_2048

MIC root certificates that stay in the CAPF trust store get used for certificate upgrades. For information on updating the Cisco Unified CallManager trust store and managing certificates, refer to the *Cisco Unified Communications Operating System Administration Guide, Release 5.0(4)*.

Server Certificate Types

Cisco uses the following self-signed (own) certificate types in Cisco Unified CallManager servers:

- **HTTPS certificate (tomcat_cert)**—This self-signed root certificate gets generated during the Cisco Unified CallManager installation for the HTTPS server.

- Cisco Unified CallManager node certificate—This self-signed root certificate automatically installs when you install Cisco Unified CallManager 5.1 for the Cisco Unified CallManager server. Cisco Unified CallManager certificates provide server identification, including the Cisco Unified CallManager server name and the Global Unique Identifier (GUID).
- CAPF certificate—The system copies this root certificate to all servers in the cluster after you complete the Cisco CTL client configuration.
- IPsec certificate (ipsec_cert)—This self-signed root certificate gets generated during Cisco Unified CallManager installation for IPsec connections with MGCP and H.323 gateways.
- SRST-enabled gateway certificate—When you configure a secure SRST reference in Cisco Unified CallManager Administration, Cisco Unified CallManager retrieves the SRST-enabled gateway certificate from the gateway and stores it in the Cisco Unified CallManager database. After you reset the devices, the certificate gets added to the phone configuration file. Because the certificate is stored in the database, this certificate does not get integrated into the certificate management tool.

Cisco Unified CallManager imports the following certificate types to the Cisco Unified CallManager trust store:

- Cisco Unity server certificate—Cisco Unity uses this self-signed root certificate to sign the Cisco Unity SCCP device certificates. The Cisco Unity Telephony Integration Manager manages this certificate.
- Cisco Unity SCCP device certificates—Cisco Unity SCCP devices use this signed certificate to establish a TLS connection with the Cisco Unified CallManager. Every Unity device (or port) gets issued a certificate that is rooted at the Unity root certificate. The Unity certificate name represents a hash of the certificate subject name, which is based on the Unity machine name.
- SIP Proxy server certificate—A SIP user agent that connects via a SIP trunk authenticates to Cisco Unified CallManager if the Cisco Unified CallManager trust store contains the SIP user agent certificate and if the SIP user agent contains the Cisco Unified CallManager certificate in its trust store.

Support for Certificates from External CAs

Cisco Unified CallManager supports integration with third-party certificate authorities (CAs) by using a PKCS#10 certificate signing request (CSR) mechanism, which is accessible at the Cisco Unified Communications Operating System Certificate Manager GUI. Customers who currently use third-party CAs should use the CSR mechanism to issue certificates for both CallManager and CAPF.



Note

This release of Cisco Unified CallManager does not provide SCEP interface support.

Cisco has verified the PKCS#10 CSR support mechanism with these CAs: Keon and Microsoft. Cisco has not verified certificate issuance with other external CAs that support PKCS#10 CSRs.

Be sure to run the CTL client after you upload a third-party, CA-signed certificate to the platform to update the CTL file. After running the CTL client, restart the appropriate service(s) for the update; for example, restart Cisco Call Manager and Cisco Tftp when updating the Cisco Unified CallManager certificate, restart CAPF when updating the CAPF certificate, and so on. See [“Configuring the Cisco CTL Client” section on page 31-1](#) for the update procedure.

For information on generating Certificate Signing Requests (CSRs) at the platform, refer to the *Cisco Unified Communications Operating System Administration Guide, Release 5.0(4)*

Authentication, Integrity, and Authorization Overview

Integrity and authentication protect against the following threats:

- TFTP file manipulation (integrity)
- Modification of call-processing signaling between the phone and Cisco Unified CallManager (authentication)
- Man-in-the-middle attacks (authentication), as defined in [Table 30-1](#)
- Phone and server identity theft (authentication)
- Replay attack (digest authentication)

Authorization specifies what an authenticated user, service, or application can do. You can implement multiple authentication and authorization methods in a single session.

See the following sections for information on authentication, integrity, and authorization:

- [Image Authentication, page 30-15](#)
- [Device Authentication, page 30-15](#)
- [File Authentication, page 30-16](#)
- [Signaling Authentication, page 30-16](#)
- [Digest Authentication, page 30-17](#)
- [Authorization, page 30-18](#)

Image Authentication

This process prevents tampering with the binary image, that is, the firmware load, prior to loading it on the phone. Tampering with the image causes the phone to fail the authentication process and reject the image. Image authentication occurs through signed binary files that are automatically installed when you install Cisco Unified CallManager. Likewise, firmware updates that you download from the web also provide signed binary images.

Device Authentication

This process validates the identity of the device and ensures that the entity is who it claims to be. For a list of devices that are supported, see “Supported Phone Models” in the Phones Security Overview chapter in the *Cisco Unified CallManager Security Guide, Release 5.0(4)*.

Device authentication occurs between the Cisco Unified CallManager server and supported Cisco Unified IP Phones, SIP trunks, or JTAPI/TAPI/CTI applications (when supported). An authenticated connection occurs between these entities only when each entity accepts the certificate of the other entity. This process of mutual certificate exchange is called mutual authentication.

Device authentication relies on the creation of the Cisco CTL file (for authenticating Cisco Unified CallManager server node and applications), as described in [Configuring the Cisco CTL Client, page 31-1](#), and the Certificate Authority Proxy Function (for authenticating phones and JTAPI/TAPI/CTI applications), as described in “Using the Certificate Authority Proxy Function” chapter in the *Cisco Unified CallManager Security Guide, Release 5.0(4)*.

**Tip**

A SIP user agent that connects via a SIP trunk authenticates to Cisco Unified CallManager if the Cisco Unified CallManager trust store contains the SIP user agent certificate and if the SIP user agent contains the Cisco Unified CallManager certificate in its trust store. For information on updating the Cisco Unified CallManager trust store, refer to the *Cisco Unified Communications Operating System Administration Guide, Release 5.0(4)*.

File Authentication

This process validates digitally signed files that the phone downloads; for example, the configuration, ring list, locale, and CTL files. The phone validates the signature to verify that file tampering did not occur after the file creation. For a list of devices that are supported, see “Supported Phone Models” in the Phone Security Overview chapter in the *Cisco Unified CallManager Security Guide, Release 5.0(4)*.

The TFTP server does not sign any files if you configure the cluster for nonsecure mode. If you configure the cluster for mixed mode, the TFTP server signs static files, such as ring list, localized, default.cnf.xml, and ring list wav files, in .sgn format. The TFTP server signs files in <device name>.cnf.xml format every time that the TFTP server verifies that a data change occurred for the file.

The TFTP server writes the signed files to disk if caching is disabled. If the TFTP server verifies that a saved file has changed, the TFTP server re-signs the file. The new file on the disk overwrites the saved file that gets deleted. Before the phone can download the new file, the administrator must restart affected devices in Cisco Unified CallManager Administration.

After the phone receives the files from the TFTP server, the phone verifies the integrity of the files by validating the signature on the file. For the phone to establish an authenticated connection, ensure that the following criteria are met:

- A certificate must exist in the phone.
- The CTL file must exist on the phone, and the Cisco Unified CallManager entry and certificate must exist in the file.
- You configured the device for authentication or encryption.

**Note**

File authentication relies on the creation of the Certificate Trust List (CTL) file, which the [“Configuring the Cisco CTL Client” section on page 31-1](#) describes.

Signaling Authentication

This process, also known as signaling integrity, uses the TLS protocol to validate that no tampering occurred to signaling packets during transmission.

Signaling authentication relies on the creation of the Certificate Trust List (CTL) file, which the [“Configuring the Cisco CTL Client” section on page 31-1](#) describes

Digest Authentication

This process for SIP trunks and phones allows Cisco Unified CallManager to challenge the identity of a SIP user agent (UA) when the UA sends a request to Cisco Unified CallManager. (A SIP user agent represents a device or application that originates a SIP message.)

Cisco Unified CallManager acts as a user agent server (UAS) for SIP calls that are originated by line-side phones or devices that are reached through the SIP trunk, as a user agent client (UAC) for SIP calls that it originates to the SIP trunk, or a back-to-back user agent (B2BUA) for line-to-line or trunk-to-trunk connections. In most environments, Cisco Unified CallManager acts primarily as B2BUA connecting SCCP and SIP endpoints.

Cisco Unified CallManager can challenge SIP phones or SIP devices that connect through a SIP trunk (as a UAS) and can respond to challenges that are received on its SIP trunk interface (as a UAC). When digest authentication is enabled for a phone, Cisco Unified CallManager challenges all SIP phone requests except keepalive messages.

**Note**

Cisco Unified CallManager does not respond to challenges from line-side phones.

Cisco Unified CallManager defines a SIP call as having two or more separate call legs. For a standard, two-party call between two SIP devices, two separate call legs exist: one leg between the originating SIP UA and Cisco Unified CallManager (the originating call leg) and the other leg between Cisco Unified CallManager and destination SIP UA (the terminating call leg). Each call leg represents a separate dialog. Because digest authentication is a point-to-point process, digest authentication on each call leg stays independent of the other call legs. SRTP capabilities can change for each call leg, depending on the capabilities that are negotiated between the user agents.

**Tip**

Digest authentication does not provide integrity or confidentiality. To ensure integrity and confidentiality for the device, configure the TLS protocol for the device, if the device supports TLS. If the device supports encryption, configure the device security mode as encrypted. If the device supports encrypted phone configuration files, configure encryption for the files.

Cisco Unified CallManager server uses a SIP 401 (Unauthorized) message to initiate a challenge, which includes the nonce and the realm in the header. (The nonce specifies a random number that gets used to calculate the MD5 hash.) When a SIP user agent challenges the identity of Cisco Unified CallManager, Cisco Unified CallManager responds to SIP 401 and SIP 407 (Proxy Authentication Required) messages.

After you enable digest authentication for a SIP phone or trunk and configure digest credentials, Cisco Unified CallManager calculates a credentials checksum that includes a hash of the username, password, and the realm. Cisco Unified CallManager encrypts the values and stores the username and the checksum in the database. Each digest user can have one set of digest credentials per realm.

**Tip**

SIP phones can only exist in the Cisco Unified CallManager realm. For SIP trunks, the realm represents the domain that connects through the SIP trunk, such as xyz.com, which helps to identify the source of the request.

When Cisco Unified CallManager challenges a user agent, Cisco Unified CallManager indicates the realm and nonce value for which the user agent must present its credentials. After receiving a response, Cisco Unified CallManager validates the checksum for the username that is stored in the database against the credentials that are received in the response header from the UA. If the credentials match, digest authentication succeeded, and Cisco Unified CallManager processes the SIP request.

When responding to a challenge from a user agent that is connected through the SIP trunk, Cisco Unified CallManager responds with the Cisco Unified CallManager username and password that are configured for the realm, which is specified in the challenge message header. When Cisco Unified CallManager gets challenged, the Cisco Unified CallManager looks up the username and encrypted password based on the realm that the challenge message specifies. Cisco Unified CallManager decrypts the password, calculates the digest, and presents it in the response message.

Administrators configure SIP digest credentials for a phone user or application user. For applications, you specify digest credentials in the Applications User Configuration window in Cisco Unified CallManager Administration. For SIP phones, you specify the digest authentication credentials, which are then applied to a phone, in the End User window in Cisco Unified CallManager Administration.

To associate the credentials with the phone after you configure the user, you choose a Digest User, an end user, in the Phone Configuration window. After you reset the phone, the credentials exist in the phone configuration file that the TFTP server offers to the phone.

If you enable digest authentication for an end user but do not configure the digest credentials, the phone will fail registration. If the cluster mode is nonsecure and you enable digest authentication and configure digest credentials, the digest credentials get sent to the phone, and Cisco Unified CallManager still initiates challenges.

Administrators configure the SIP realm for challenges to the phone and for challenges that are received through the SIP trunk. The SIP Realm GUI provides the trunk-side credentials for UAC mode. You configure the SIP realm for phones with the service parameter SIP Station Realm. You must configure a SIP realm and username and password in Cisco Unified CallManager Administration for each SIP trunk user agent that can challenge Cisco Unified CallManager.

Administrators configure the minutes for which the nonce value stays valid for the external device before Cisco Unified CallManager rejects the external device and generates a new number.

Authorization

Cisco Unified CallManager uses the authorization process to restrict certain categories of messages from SIP phones, from SIP trunks, and from SIP application requests on SIP trunks.

For SIP INVITE messages and in-dialog messages, and for SIP phones, Cisco Unified CallManager provides authorization through calling search spaces and partitions.

For SIP SUBSCRIBE requests from phones, Cisco Unified CallManager provides authorization for user access to presence groups.

For SIP trunks, Cisco Unified CallManager provides authorization of presence subscriptions and certain non-INVITE SIP messages; for example, out-of-dial REFER, unsolicited notification, and any SIP request with the replaces header. You specify authorization in the SIP Trunk Security Profile window when you check the related check boxes in the window.

Authorization occurs for the SIP trunk first (as configured in the SIP Trunk Security Profile) and then for the SIP application user agent on the SIP trunk (as configured in the Application User Configuration), when application-level authorization is configured. For the trunk, Cisco Unified CallManager downloads the trunk ACL information and caches it. The ACL information gets applied to the incoming SIP request. If the ACL does not allow the SIP request, the call fails with a 403 Forbidden message.

If the ACL allows the SIP request, Cisco Unified CallManager checks whether digest authentication is enabled in the SIP Trunk Security Profile. If digest authentication is not enabled and application-level authorization is not enabled, Cisco Unified CallManager processes the request. If digest authentication is enabled, Cisco Unified CallManager verifies that the authentication header exists in the incoming request and then uses digest authentication to identify the source application. If the header does not exist, Cisco Unified CallManager challenges the device with a 401 message.

To enable SIP application authorization on the SIP trunk, you must check the Enable Application Level Authorization check box in the SIP Trunk Security Profile window. Before an application-level ACL gets applied, Cisco Unified CallManager authenticates the SIP trunk user agent through digest authentication. Therefore, you must enable digest authentication in the SIP Trunk Security Profile for application-level authorization to occur.

Encryption Overview

**Tip**

Encryption installs automatically when you install Cisco Unified CallManager 5.1 on each server in the cluster.

Cisco Unified CallManager supports the following types of encryption:

- [Signaling Authentication, page 30-16](#)
- [Media Encryption, page 30-20](#)
- [Configuration File Encryption, page 30-21](#)

Signaling Encryption

Signaling encryption ensures that all SIP and SCCP signaling messages that are sent between the device and the Cisco Unified CallManager server are encrypted.

Signaling encryption ensures that the information that pertains to the parties, DTMF digits that are entered by the parties, call status, media encryption keys, and so on, are protected against unintended or unauthorized access.

Cisco does not support Network Address Translation (NAT) with Cisco Unified CallManager if you configure the cluster for mixed mode; NAT does not work with signaling encryption.

You can enable UDP ALG in the firewall to allow media stream firewall traversal. Enabling the UDP ALG allows the media source on the trusted side of the firewall to open a bidirectional media flow through the firewall by sending the media packet through the firewall.

**Tip**

Hardware DSP resources cannot initiate this type of connection and, therefore, must exist outside the firewall.

Signaling encryption does not support NAT traversal. Instead of using NAT, consider using LAN extension VPNs.

SIP trunks support signaling encryption but do not support media encryption.

Media Encryption

Media encryption, which uses SRTP, ensures that only the intended recipient can interpret the media streams between supported devices. Support includes audio streams only. Media encryption includes creating a media master key pair for the devices, delivering the keys to the devices, and securing the delivery of the keys while the keys are in transport.

**Note**

Cisco Unified CallManager handles media encryption keys differently for different devices and protocols. All SCCP phones get their media encryption keys from Cisco Unified CallManager, which secures the media encryption key downloads to phones with TLS encrypted signaling channels. SIP phones generate and store their own media encryption keys. Media encryption keys that are derived by Cisco Unified CallManager system securely get sent via encrypted signaling paths to gateways over IPSec-protected links.

If the devices support SRTP, the system uses a SRTP connection. If at least one device does not support SRTP, the system uses a RTP connection. SRTP-to-RTP fallback may occur for transfers from a secure device to a non-secure device, conferencing, transcoding, music on hold, and so on.

For most security-supported devices, authentication and signaling encryption serve as the minimum requirements for media encryption; that is, if the devices do not support signaling encryption and authentication, media encryption cannot occur. Cisco IOS gateways and trunks support media encryption without authentication. For Cisco IOS gateways and trunks, you must configure IPSec when you enable the SRTP capability (media encryption).

**Tip**

Before you configure SRTP or signaling encryption for gateways and trunks, Cisco strongly recommends that you configure IPSec because Cisco IOS MGCP gateways, H.323 gateways, H.323/H.245/H.225 trunks, and SIP trunks rely on IPSec configuration to ensure that security-related information does not get sent in the clear. Cisco Unified CallManager does not verify that you configured IPSec correctly. If you do not configure IPSec correctly, security-related information may get exposed.

Secure SIP trunks can support secure calls over TLS; be aware, though, that the trunk supports signaling encryption but does not support media encryption (SRTP). Because the trunk does not support media encryption, the shield icon may display on the phones during the call; that is, if all devices in the call support authentication or signaling encryption.

The following example demonstrates media encryption for SCCP and MGCP calls.

1. Device A and Device B, which support media encryption and authentication, register with Cisco Unified CallManager.
2. When Device A places a call to Device B, Cisco Unified CallManager requests two sets of media session master values from the key manager function.
3. Both devices receive the two sets: one set for the media stream, Device A—Device B, and the other set for the media stream, Device B—Device A.
4. Using the first set of master values, Device A derives the keys that encrypt and authenticate the media stream, Device A—Device B.
5. Using the second set of master values, Device A derives the keys that authenticate and decrypt the media stream, Device B—Device A.
6. Device B uses these sets in the inverse operational sequence.

7. After the devices receive the keys, the devices perform the required key derivation, and SRTP packet processing occurs.

**Note**

SIP phones and H.323 trunks/gateways generate their own cryptographic parameters and send them to Cisco Unified CallManager.

Configuration File Encryption

Cisco Unified CallManager pushes confidential data such as digest credentials and administrator passwords to phones in configuration file downloads from the TFTP server.

Cisco Unified CallManager uses reversible encryption to secure these credentials in the database. To secure this data during the download process, Cisco recommends that you configure encrypted configuration files for all Cisco Unified IP Phones that support this option (see [“Supported Phone Models” section on page 33-4](#)). When this option is enabled, only the device configuration file gets encrypted for download.

**Note**

In some circumstances, you may choose to download confidential data to phones in the clear; for example, to troubleshoot the phone or during auto-registration.

Cisco Unified CallManager encodes and stores encryption keys in the database. The TFTP server encrypts and decrypts configuration files by using symmetric encryption keys:

- If the phone has PKI capabilities, Cisco Unified CallManager can use the phone public key to encrypt the phone configuration file.
- If the phone does not have PKI capabilities, you must configure a unique symmetric key in Cisco Unified CallManager and in the phone.

You enable encrypted configuration file settings in the Phone Security Profile window in Cisco Unified CallManager Administration, which you then apply to a phone in the Phone Configuration window.

See [“Understanding Encryption of the Phone Configuration File” section on page 33-1](#) in this document for more information.

Configuration Checklist Overview

[Table 30-3](#) describes tasks that you must perform to implement authentication and encryption. Each chapter may also contain a checklist for the tasks that you must perform for the specified security feature.

Table 30-3 Configuration Checklist for Authentication and Encryption

Configuration Steps		Related Procedures and Topics
Step 1	On each server in the cluster, activate the Cisco CTL Provider service in Cisco Unified CallManager Serviceability. Tip If you activated this service prior to a Cisco Unified CallManager upgrade, you do not need to activate the service again. The service automatically activates after the upgrade.	Activating the Cisco CTL Provider Service, page 31-4
Step 2	On the first node, activate the Cisco Certificate Authority Proxy service in Cisco Unified CallManager Serviceability to install, upgrade, troubleshoot, or delete locally significant certificates. Timesaver Performing this task before you install and configure the Cisco CTL client ensures that you do not have to update the CTL file to use CAPE.	Activating the Certificate Authority Proxy Function Service, <i>Cisco Unified CallManager Security Guide, Release 5.0(4)</i>
Step 3	If you do not want to use the default port settings, configure ports for the TLS connection. Tip If you configured these settings prior to a Cisco Unified CallManager upgrade, the settings migrate automatically during the upgrade.	Configuring Ports for the TLS Connection, page 31-5
Step 4	Obtain at least two security tokens and the passwords, hostnames/IP addresses, and port numbers for the servers that you will configure for the Cisco CTL client.	Configuring the Cisco CTL Client, page 31-8
Step 5	Install the Cisco CTL client. Tip To update the Cisco CTL file after an upgrade to Cisco Unified CallManager 5.1(1), you must install the plug-in that is available in Cisco Unified CallManager Administration 5.1(1).	• System Requirements, page 30-4 • Installation, page 30-12 • Installing the Cisco CTL Client, page 31-6 • Upgrading the Cisco CTL Client and Migrating the Cisco CTL File, page 31-7
Step 6	Configure the Cisco CTL client. Tip If you created the Cisco CTL file prior to a Cisco Unified CallManager upgrade, the Cisco CTL file migrates automatically during the upgrade. To update the Cisco CTL file after an upgrade to Cisco Unified CallManager 5.1(1), you must install and configure the 5.1(1) version of the Cisco CTL client.	• Configuring the Cisco CTL Client, page 31-8 • Upgrading the Cisco CTL Client and Migrating the Cisco CTL File, page 31-7

Table 30-3 Configuration Checklist for Authentication and Encryption (continued)

Configuration Steps	Related Procedures and Topics
Step 7 Configure the phone security profiles. Perform the following tasks when you configure the profiles: • Configure the device security mode (for SCCP and SIP phones). The device security mode migrates automatically during the Cisco Unified CallManager upgrade. If you want to configure encryption for devices that only supported authentication in Cisco Unified CallManager 4.0, you must choose a security profile for encryption in the Phone Configuration window. • Configure CAPF settings (for some SCCP and SIP phones). Additional CAPF settings display in the Phone Configuration window. • If you plan to use digest authentication for SIP phones, check the Enable Digest Authentication check box. • To enable encrypted configuration files (for some SCCP and SIP phones), check the TFTP Encrypted Config check box. • To exclude digest credentials in configuration file downloads, check the TFTP Exclude Digest Credential in Configuration File check box.	Configuring a Phone Security Profile, page 32-3 Configuration Tips for Phone Security Profiles, page 32-1 Configuring Encrypted Phone Configuration Files, page 33-1 Configuration Tips for Encrypted Configuration Files, page 33-4
Step 8 Apply the phone security profiles to the phones.	Applying a Phone Security Profile, page 32-9
Step 9 Configure CAPF to issue certificates to the phones. If you performed certificate operations before the upgrade to Cisco Unified CallManager 5.1 and CAPF ran on a subscriber server, you must copy the CAPF data to the 4.0 publisher database server before you upgrade the cluster to Cisco Unified CallManager 5.1.  Caution The CAPF data on the Cisco Unified CallManager 4.0 subscriber server does not migrate to the Cisco Unified CallManager 5.1 database, and a loss of data occurs if you do not copy the data to the 5.1 database. If a loss of data occurs, the locally significant certificates that you issued with CAPF utility 1.0(1) remain in the phones, but CAPF 5.1 must reissue the certificates, which are no longer valid.	• System Requirements, page 30-4 • CAPF Configuration Checklist, <i>Cisco Unified CallManager Security Guide, Release 5.0(4)</i>
Step 10 Verify that the locally significant certificates are installed on supported Cisco Unified IP Phones.	• System Requirements, page 30-4 • Entering the Authentication String on the Phone, <i>Cisco Unified CallManager Security Guide, Release 5.0(4)</i>

Table 30-3 Configuration Checklist for Authentication and Encryption (continued)

Configuration Steps		Related Procedures and Topics
Step 11	Configure digest authentication for SIP phones.	Configuring Digest Authentication for the SIP Phone, <i>Cisco Unified CallManager Security Guide, Release 5.0(4)</i>
Step 12	Perform phone-hardening tasks. Tip If you configured phone-hardening settings prior to a Cisco Unified CallManager upgrade, the device configuration settings migrate automatically during the upgrade.	Phone Hardening, <i>Cisco Unified CallManager Security Guide, Release 5.0(4)</i>
Step 13	Configure voice mail ports for security.	- Configuring Voice Messaging Ports for Security, <i>Cisco Unified CallManager Security Guide, Release 5.0(4)</i> <i>Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x</i>
Step 14	Configure security settings for SRST references. Tip If you configured secure SRST references in a previous Cisco Unified CallManager release, the configuration automatically migrates during the Cisco Unified CallManager upgrade.	Configuring a Secure Survivable Remote Site Telephony (SRST) Reference, <i>Cisco Unified CallManager Security Guide, Release 5.0(4)</i>
Step 15	Configure IPSec.	- Configuring Encryption for Gateways and Trunks, <i>Cisco Unified CallManager Security Guide, Release 5.0(4)</i> - Considerations for Configuring IPSec in the Network Infrastructure, <i>Cisco Unified CallManager Security Guide, Release 5.0(4)</i> <i>Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways</i> <i>Cisco Unified Communications Operating System Administration Guide, Release 5.0(4)</i>.
Step 16	Configure the SIP trunk security profile. If you plan to use digest authentication, check the Enable Digest Authentication check box in the profile. For trunk-level authorization, check the authorization check boxes for the allowed SIP requests. If you want application-level authorization to occur after trunk-level authorization, check the Enable Application Level Authorization check box. You cannot check application-level authorization unless digest authentication is checked.	- Configuring the SIP Trunk Security Profile, <i>Cisco Unified CallManager Security Guide, Release 5.0(4)</i> - Configuring Digest Authentication Enterprise Parameters, <i>Cisco Unified CallManager Security Guide, Release 5.0(4)</i>

Table 30-3 Configuration Checklist for Authentication and Encryption (continued)

Configuration Steps		Related Procedures and Topics
Step 17	Apply the SIP trunk security profile to the trunk.	Applying a SIP Trunk Security Profile, <i>Cisco Unified CallManager Security Guide, Release 5.0(4)</i>
Step 18	Configure digest authentication for the trunk.	Configuring Digest Authentication for the SIP Trunk, <i>Cisco Unified CallManager Security Guide, Release 5.0(4)</i>
Step 19	If you checked the Enable Application Level Authorization check box in the SIP trunk security profile, configure the allowed SIP requests by checking the authorization check boxes in the Application User Configuration window.	- Configuring the SIP Trunk Security Profile, <i>Cisco Unified CallManager Security Guide, Release 5.0(4)</i> - See also application user authorization in the <i>Cisco Unified CallManager Administration Guide</i>
Step 20	Reset all phones in the cluster.	Resetting the Devices, Restarting Services, or Rebooting the Server/Cluster, page 30-10
Step 21	Reboot all servers in the cluster.	Resetting the Devices, Restarting Services, or Rebooting the Server/Cluster, page 30-10

Where to Find More Information

Related Cisco Documentation

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

- *Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager*
- *Cisco Unified Communications Operating System Administration Guide*
- *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*
- *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x*
- Cisco Unified Survivable Remote Site Telephony (SRST) administration documentation that supports the SRST-enabled gateway
- *Cisco IP Telephony Disaster Recovery Framework Administration Guide*
- *Cisco Unified CallManager Bulk Administration Guide*
- *Troubleshooting Guide for Cisco Unified CallManager*
- The firmware release notes that support your phone model



Configuring the Cisco CTL Client

This chapter contains information on the following topics:

- [Cisco CTL Client Overview, page 31-2](#)
- [Configuration Tips for Cisco CTL Client Configuration, page 31-2](#)
- [Cisco CTL Client Configuration Checklist, page 31-3](#)
- [Activating the Cisco CTL Provider Service, page 31-4](#)
- [Activating the Cisco CAPF Service, page 31-5](#)
- [Configuring Ports for the TLS Connection, page 31-5](#)
- [Installing the Cisco CTL Client, page 31-6](#)
- [Upgrading the Cisco CTL Client and Migrating the Cisco CTL File, page 31-7](#)
- [Configuring the Cisco CTL Client, page 31-8](#)
- [Updating the CTL File, page 31-10](#)
- [Deleting a CTL File Entry, page 31-12](#)
- [Updating the Clusterwide Security Mode, page 31-12](#)
- [Cisco CTL Client Configuration Settings, page 31-12](#)
- [Verifying the Security Mode for the Cisco Unified CallManager Cluster, page 31-15](#)
- [Setting the Smart Card Service to Started and Automatic, page 31-15](#)
- [Changing the Security Token Password \(Etoken\), page 31-16](#)
- [Deleting the CTL File on the Cisco Unified IP Phone, page 31-16](#)
- [Determining the Cisco CTL Client Version, page 31-17](#)
- [Verifying or Uninstalling the Cisco CTL Client, page 31-18](#)
- [Where to Find More Information, page 31-18](#)

Cisco CTL Client Overview

Device, file, and signaling authentication rely on the creation of the Certificate Trust List (CTL) file, which is created when you install and configure the Cisco Certificate Trust List (CTL) client on a single Windows workstation or server that has a USB port.

**Note**

Supported Windows versions for Cisco CTL client include Windows 2000 and Windows XP. Do not use Terminal Services to install the Cisco CTL client. Cisco installs Terminal Services, so Cisco Technical Assistance Center (TAC) can perform remote troubleshooting and configuration tasks.

The CTL file contains entries for the following servers or security tokens:

- Site Administrator Security Token (SAST)
- Cisco Unified CallManager and Cisco TFTP that are running on the same server
- Certificate Authority Proxy Function (CAPF)
- TLS proxy server such as a firewall

The CTL file contains a server certificate, public key, serial number, signature, issuer name, subject name, server function, DNS name, and IP address for each server.

After you create the CTL file, you must restart the Cisco CallManager and Cisco TFTP services in Cisco Unified CallManager Serviceability on all Cisco Unified CallManager servers that run these services and on all TFTP servers in the cluster. The next time that the phone initializes, it downloads the CTL file from the TFTP server. If the CTL file contains a TFTP server entry that has a self-signed certificate, the phone requests a signed configuration file in .sgn format. If no TFTP server contains a certificate, the phone requests an unsigned file.

After the Cisco CTL client adds a server certificate to the CTL file, you can display the certificate in the CTL client GUI.

When you configure a TLS proxy server in the CTL file, you can secure a Cisco PIX Firewall as part of a secure Cisco Unified CallManager system. The Cisco CTL client displays the firewall certificate as a “CCM” certificate.

Cisco Unified CallManager Administration uses an etoken to authenticate the TLS connection between the Cisco CTL client and provider.

Configuration Tips for Cisco CTL Client Configuration

Consider the following information when you configure the Cisco CTL client in Cisco Unified CallManager Administration:

- Ensure that Cisco Unified CallManager node hostnames are resolvable on the remote PC where the Cisco CTL client is installed, or the Cisco CTL client will not function correctly.
- You must activate the Cisco CTL Provider service on all servers in the cluster.
- When the Cisco CTL client contains entries for off-cluster servers, such as alternate or centralized TFTP server, you must also run the CTL Provider service on these servers.
- In the Alternate TFTP Server Tab Settings section of the CTL client GUI, alternate TFTP server designates a Cisco TFTP server that exists in a different cluster. Use these setting to configure alternate and centralized TFTP servers in the CTL client.

**Note**

See “[Cisco TFTP](#)” for information about configuring off-cluster (alternate and centralized) TFTP servers by using TFTP service parameters.

- For centralized TFTP configurations, all off-cluster TFTP servers that are operating in mixed mode must add the Master TFTP server or Master TFTP server IP address to the off-cluster CTL file. The master TFTP server serves configuration files from all alternate TFTP servers in the alternate file list that is configured for the master TFTP server. All clusters in a centralized TFTP configuration do not need to use the same security mode; each cluster can select its own mode.
- After you create or update the CTL file, you must restart the Cisco CallManager and Cisco TFTP services in Cisco Unified CallManager Serviceability on all Cisco Unified CallManager servers that run these services and on all TFTP servers in the cluster.

Cisco CTL Client Configuration Checklist

[Table 31-1](#) provides a list of configuration tasks that you perform to install and configure the Cisco CTL client for the first time. See [Upgrading the Cisco CTL Client and Migrating the Cisco CTL File](#), page 31-7, for more information about configuring the CTL file when you upgrade Cisco Unified CallManager.

Table 31-1 Cisco CTL Client Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	On each Cisco Unified CallManager in the cluster, activate the Cisco CTL Provider service in Cisco Unified CallManager Serviceability. Tip If you activated this service prior to a Cisco Unified CallManager upgrade, you do not need to activate the service again. The service automatically activates after the upgrade.	Activating the Cisco CTL Provider Service , page 31-4
Step 2	On the first node, activate the Cisco Certificate Authority Proxy service in Cisco Unified CallManager Serviceability. Timesaver Performing this task before you install and configure the Cisco CTL client ensures that you do not have to update the CTL file to use CAPF.	Activating the Certificate Authority Proxy Function Service , <i>Cisco Unified CallManager Security Guide, Release 5.0(4)</i>
Step 3	If you do not want to use the default settings, configure ports for the TLS connection. Tip If you configured these settings prior to a Cisco Unified CallManager upgrade, the settings migrate automatically.	Configuring Ports for the TLS Connection , page 31-5
Step 4	Obtain at least two security tokens and the passwords, hostnames/IP addresses, and port numbers for the servers that you will configure for the Cisco CTL client.	Configuring the Cisco CTL Client , page 31-8

Table 31-1 Cisco CTL Client Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 5	Install the Cisco CTL client.	• System Requirements, page 30-4 • Installation, page 30-12 • Installing the Cisco CTL Client, page 31-6
Step 6	Configure the Cisco CTL client.	Configuring the Cisco CTL Client, page 31-8

Activating the Cisco CTL Provider Service

After you configure the Cisco CTL client, this service changes the cluster security mode from nonsecure to mixed mode and transports the server certificates to the CTL file. The service then transports the CTL file to all Cisco Unified CallManager and Cisco TFTP servers.

If you activate the service and then upgrade Cisco Unified CallManager, Cisco Unified CallManager automatically reactivates the service after the upgrade.



Tip

You must activate the Cisco CTL Provider service on all servers in the cluster.

To activate the service, perform the following procedure:

Procedure

- Step 1** In Cisco Unified CallManager Serviceability, choose **Tools > Service Activation**.
- Step 2** In the Servers drop-down list box, choose a server where you have activated the Cisco Unified CallManager or Cisco TFTP services.
- Step 3** Click the **Cisco CTL Provider** service radio button.
- Step 4** Click **Save**.
- Step 5** Perform this procedure on all servers in the cluster.



Note

You can enter a CTL port before you activate the Cisco CTL Provider service. If you want to change the default port number, see “Configuring Ports for the TLS Connection” in the *Cisco Unified CallManager Security Guide, Release 5.0(4)*.

- Step 6** Verify that the service runs on all servers in the cluster. In Cisco Unified CallManager Serviceability, choose **Tools > Control Center - Feature Services** to verify the state of the service.

Additional Information

See the “[Related Topics](#)” section on page 31-18.

Activating the Cisco CAPF Service

For information on activating this service, see the “Activating the Certificate Authority Proxy Function Service” section in the *Cisco Unified CallManager Security Guide, Release 5.0(4)*.

**Timesaver**

Performing this task before you install and configure the Cisco CTL client ensures that you do not have to update the CTL file to use CAPF.

Configuring Ports for the TLS Connection

You may have to configure a different port number if the port is currently being used or if you use a firewall and you cannot use the port within the firewall.

The Cisco CTL Provider default port for the TLS connection equals 2444. The Cisco CTL Provider port monitors requests from the Cisco CTL client. This port processes Cisco CTL client requests, such as retrieving the CTL file, setting the clusterwide security mode, saving the CTL file to TFTP servers, and retrieving a list of Cisco Unified CallManager and TFTP servers in the cluster.

The Ethernet Phone Port monitors registration requests from the SCCP phone. In nonsecure mode, the phone connects through port 2000. In mixed mode, the Cisco Unified CallManager port for TLS connection equals the value for the Cisco Unified CallManager port number added to (+) 443; therefore, the default TLS connection for Cisco Unified CallManager equals 2443. Update this setting only if the port number is in use, or if you use a firewall and you cannot use the port within the firewall.

The SIP Secure Port allows Cisco Unified CallManager to listen for SIP messages from SIP phones. The default value equals 5061. If you change this port, you must restart the Cisco CallManager service in Cisco Unified CallManager Serviceability and reset the SIP phones.

**Tip**

After you update the port(s), you must restart the Cisco CTL Provider service in Cisco Unified CallManager Administration.

You must open the CTL ports to the data VLAN from where the CTL client runs. Phones that are running TLS for signaling back to Cisco Unified CallManager also use the ports that the CTL client uses. Ensure that you open these ports to all VLANs where phones are configured for authenticated or encrypted status.

To change the default setting, perform the following procedure:

Procedure

-
- Step 1** Perform the following tasks, depending on the port that you want to change:
- To change the Port Number parameter for the Cisco CTL Provider service, perform [Step 2](#) through [Step 6](#).
 - To change the Ethernet Phone Port or SIP Phone Secure Port settings, perform [Step 7](#) through [Step 11](#).
- Step 2** To change the Cisco CTL Provider port, choose **System > Service Parameters** in Cisco Unified CallManager Administration.
- Step 3** In the Server drop-down list box, choose a server where the Cisco CTL Provider service runs.

Step 4 In the Service drop-down list box, choose **Cisco CTL Provider** service.



Tip For information on the service parameter, click the question mark or the link name.

- Step 5** To change the value for the Port Number parameter, enter the new port number in the Parameter Value field.
- Step 6** Click **Save**.
- Step 7** To change the Ethernet Phone Port or SIP Phone Secure Port settings, choose **System > Cisco Unified CallManager** in Cisco Unified CallManager Administration.
- Step 8** Find a server where the Cisco CallManager service runs, as described in the *Cisco Unified CallManager Administration Guide*; after the results display, click the **Name** link for the server.
- Step 9** After the Cisco Unified CallManager Configuration window displays, enter the new port numbers in the Ethernet Phone Port or SIP Phone Secure Port fields.
- Step 10** Reset the phones and restart the Cisco CallManager service in Cisco Unified CallManager Serviceability.
- Step 11** Click **Save**.

Additional Information

See the [“Related Topics”](#) section on page 31-18.

Installing the Cisco CTL Client

You must use the client and update the CTL file when the following events occur:

- The first time you set the security mode of the cluster
- The first time you create the CTL file
- After the Cisco Unified CallManager installation
- After you restore a Cisco Unified CallManager server or Cisco Unified CallManager data
- After you change the IP address or hostname of the Cisco Unified CallManager server
- After you add or remove a security token, TFTP server, PIX firewall, or Cisco Unified CallManager server
- After you upload a third-party, CA-signed certificate to the platform



Tip

If the Smart Card service is not set to started and automatic on the server or workstation where you plan to install the client, the installation fails.

To install the Cisco CTL client, perform the following procedure:

Procedure

-
- Step 1** From the Windows workstation or server where you plan to install the client, browse to Cisco Unified CallManager Administration, as described in the *Cisco Unified CallManager Administration Guide*.
- Step 2** In Cisco Unified CallManager Administration, choose **Application > Plugins**.
The Find and List Plugins window displays.
- Step 3** From the Plugin Type equals drop-down list box, choose **Installation** and click **Find**.
- Step 4** Locate the Cisco CTL Client.
- Step 5** To download the file, click **Download** on the right side of the window, directly opposite the Cisco CTL Client plug-in name.
- Step 6** Click **Save** and save the file to a location that you will remember.
- Step 7** To begin the installation, double-click **Cisco CTL Client** (icon or executable depending on where you saved the file).



Note You can also click **Open** from the Download Complete box.

- Step 8** The version of the Cisco CTL client displays; click **Continue**.
- Step 9** The installation wizard displays. Click **Next**.
- Step 10** Accept the license agreement and click **Next**.
- Step 11** Choose a folder where you want to install the client. If you want to do so, click Browse to change the default location; after you choose the location, click **Next**.
- Step 12** To begin the installation, click **Next**.
- Step 13** After the installation completes, click **Finish**.
-

Additional Information

See the [“Related Topics” section on page 31-18](#).

Upgrading the Cisco CTL Client and Migrating the Cisco CTL File

If you want to make changes to the CTL file after a Cisco Unified CallManager Release 5.0 to 5.1 upgrade, you must uninstall the Cisco CTL client that you installed prior to the upgrade, install the latest Cisco CTL client, as described in the [“Installing the Cisco CTL Client” section on page 31-6](#), and regenerate the CTL file. If you did not remove or add any servers before the Cisco Unified CallManager upgrade, you do not need to reconfigure the Cisco CTL client after the upgrade. The Cisco Unified CallManager upgrade automatically migrates the data in the CTL file.

When you upgrade from a 4.x release to a 5.x release and security is enabled on the cluster, you must uninstall the Cisco CTL client that you installed prior to the upgrade, install the latest Cisco CTL client, and regenerate the CTL file. Follow this procedure to enable security on the upgraded cluster:

Procedure

-
- Step 1** Uninstall the existing Cisco CTL client.
- Step 2** Install the new Cisco CTL client as described in the [“Installing the Cisco CTL Client”](#) section on page 31-6.
- Step 3** Run the Cisco CTL client by using at least one of the previously used USB keys, as described in [“Configuring the Cisco CTL Client”](#) section on page 31-8.
- Step 4** Restart the Cisco CallManager and Cisco TFTP services in Cisco Unified CallManager Serviceability on all Cisco Unified CallManager servers that run these services and on all TFTP servers in the cluster.
-

Additional Information

See the [“Related Topics”](#) section on page 31-18.

Configuring the Cisco CTL Client

**Tip**

Configure the Cisco CTL client during a scheduled maintenance window because you must restart the Cisco Unified CallManager and Cisco TFTP services in Cisco Unified CallManager Serviceability on all Cisco Unified CallManager servers that run these services and on all TFTP servers in the cluster.

The Cisco CTL client performs the following tasks:

- Sets the Cisco Unified CallManager cluster security mode.

**Tip**

You cannot set the Cisco Unified CallManager clusterwide parameter to mixed mode through the Enterprise Parameters window of Cisco Unified CallManager Administration. You must configure the CTL client to set the clusterwide mode. For more information, see the [“Cisco CTL Client Configuration Settings”](#) section on page 31-12.

- Creates the Certificate Trust List (CTL), which is a file that contains certificate entries for security tokens, Cisco Unified CallManager, PIX firewall, and CAPF server.

The CTL file indicates the servers that support TLS for the phone connection. The client automatically detects the Cisco Unified CallManager, Cisco CAPF, and PIX firewall and adds certificate entries for these servers.

The security tokens that you insert during the configuration sign the CTL file.

Before You Begin**Tip**

See [Upgrading the Cisco CTL Client and Migrating the Cisco CTL File, page 31-7](#) for more information about configuring the CTL file when you upgrade Cisco Unified CallManager.

Before you configure the Cisco CTL client, verify that you activated the Cisco CTL Provider service and the Cisco Certificate Authority Proxy Function service in Cisco Unified CallManager Serviceability. Obtain at least two security tokens; the Cisco certificate authority issues these security tokens. The security tokens must come from Cisco. You will insert the tokens one at a time into the USB port on the server/workstation. If you do not have a USB port on the server, you may use a USB PCI card.

Obtain the following passwords, hostnames/IP addresses, and port numbers:

- Administrative username and password for Cisco Unified CallManager
- Security token administrative password
- Administrative username and password for the PIX firewall

See [Table 31-2](#) for a description of the preceding information.

**Tip**

Before you install the Cisco CTL client, verify that you have network connectivity to each server in the cluster. To ensure that you have network connectivity to all servers in the cluster, issue a ping command, as described in the *Cisco Unified Communications Operating System Administration Guide*.

If you installed multiple Cisco CTL clients, Cisco Unified CallManager only accepts CTL configuration information on one client at a time, but you can perform configuration tasks on up to five Cisco CTL clients simultaneously. While you perform configuration tasks on one client, Cisco Unified CallManager automatically stores the information that you entered on the other clients.

After you complete the Cisco CTL client configuration, the CTL client performs the following tasks:

- Writes the CTL file to all Cisco Unified CallManager servers in the cluster.
- Writes CAPF capf.cer to all Cisco Unified CallManager subsequent nodes (not first node) in the cluster.
- Writes CAPF certificate file in PEM format to all Cisco Unified CallManager subsequent nodes (not first node) in the cluster.
- Writes the file to all configured TFTP servers
- Writes the file to all configured PIX firewalls
- Signs the CTL file with the private key of the security token that exists in the USB port at the time you create the CTL file.

To configure the client, perform the following procedure:

Procedure

-
- Step 1** Obtain at least two security tokens that you purchased.
- Step 2** Perform one of the following tasks:
- Double-click the **Cisco CTL Client** icon that exists on the desktop of the workstation/server where you installed it.
 - Choose **Start > Programs > Cisco CTL Client**.
- Step 3** Enter the configuration settings for the Cisco Unified CallManager server, as described in [Table 31-2](#); click **Next**.
- Step 4** Click **Set Cisco Unified CallManager Cluster to Mixed Mode**, as described in [Table 31-2](#); click **Next**.
- Step 5** Perform the following tasks, depending on what you want to accomplish:
- To add a security token, see [Step 6](#) through [Step 12](#).

- To complete the Cisco CTL client configuration, see [Step 17](#) through [Step 21](#).

**Caution**

You need a minimum of two security tokens the first time that you configure the client. Do not insert the tokens until the application prompts you to do so. If you have two USB ports on the workstation or server, do not insert two security tokens at the same time.

- Step 6** When the application prompts you to do so, insert one security token in an available USB port on the workstation or server where you are currently configuring the Cisco CTL client; click **OK**.
- Step 7** The security token information displays for the token that you inserted; click **Add**.
- Step 8** The detected certificate entries display in the pane.
- Step 9** To add other security token(s) to the certificate trust list, click **Add Tokens**.
- Step 10** If you have not already done so, remove the token that you inserted into the server or workstation. When the application prompts you to do so, insert the next token and click **OK**.
- Step 11** The security token information for the second token displays; click **Add**.
- Step 12** For all security tokens, repeat [Step 9](#) through [Step 11](#).
- Step 13** The certificate entries display in the pane.
- Step 14** Enter the configuration settings, as described in [Table 31-2](#).
- Step 15** Click **Next**.
- Step 16** Enter the configuration settings, as described in [Table 31-2](#); click **Next**.
- Step 17** When you have added all security tokens and servers, click **Finish**.
- Step 18** Enter the username password for the security token, as described in [Table 31-2](#); click **OK**.
- Step 19** After the client creates the CTL file, a window displays the server, file location, and status of the CTL file on each server. Click **Finish**.
- Step 20** Reset all devices in the cluster. See the [“Resetting the Devices, Restarting Services, or Rebooting the Server/Cluster”](#) section on page 30-10.
- Step 21** In Cisco Unified CallManager Serviceability, restart the Cisco Unified CallManager and Cisco TFTP services on all Cisco Unified CallManager servers that run these services and on all TFTP servers in the cluster.
- Step 22** After you create the CTL file, you may remove the security token from the USB port. Store all security tokens in a safe place that you will remember.

Additional Information

See the [“Related Topics”](#) section on page 31-18.

Updating the CTL File

You must update the CTL file if the following scenarios occur:

- If you add a new Cisco Unified CallManager server to the cluster
- If you change the name or IP address of the Cisco Unified CallManager server in the cluster
- If you change the IP address or hostname for any configured TFTP servers or PIX firewall

- If you enabled the Cisco Certificate Authority Function service in Cisco Unified CallManager Serviceability
- If you need add or remove a security token, TFTP server, PIX firewall, or Cisco Unified CallManager server
- If you restore a Cisco Unified CallManager server or Cisco Unified CallManager data
- After you upload a third-party, CA-signed certificate to the platform

**Tip**

Cisco strongly recommends that you update the file when minimal call-processing interruptions will occur.

To update the information that exists in CTL file, perform the following procedure:

Procedure

- Step 1** Obtain one security token that you inserted to configure the latest CTL file.
- Step 2** Double-click the **Cisco CTL Client** icon that exists on the desktop of the workstation/server where you installed it.
- Step 3** Enter the configuration settings for the Cisco Unified CallManager server, as described in [Table 31-2](#); click **Next**.

**Tip**

You make updates in this window for the Cisco Unified CallManager server.

- Step 4** To update the CTL file, click **Update CTL File**, as described in [Table 31-2](#); click **Next**.

**Caution**

For all CTL file updates, you must insert one security token that already exists in the CTL file into the USB port. The client validates the signature of the CTL file through this token. You cannot add new tokens until the CTL client validates the signature. If you have two USB ports on the workstation or server, do not insert both security tokens at the same time.

- Step 5** If you have not already inserted one security token in an available USB port on the workstation or server where you are currently updating the CTL file, insert one of the security tokens; click **OK**.
- Step 6** The security token information displays for the token that you inserted; click **Next**.
The detected certificate entries display in the pane.

**Tip**

You cannot update the Cisco Unified CallManager or Cisco TFTP entries from this pane. To update the Cisco Unified CallManager entry, click **Cancel** and perform [Step 2](#) through [Step 6](#) again.

- Step 7** To update existing Cisco CTL entries or to add or delete security tokens, consider the following information:
 - To update servers settings or to add new security tokens, see [“Configuring the Cisco CTL Client” section on page 31-8](#).

- To delete a security token, see the [“Deleting a CTL File Entry” section on page 31-12](#).

Additional Information

See the [“Related Topics” section on page 31-18](#).

Deleting a CTL File Entry

At any time, you can delete some CTL entries that display in the CTL Entries window of the Cisco CTL client. After you open the client and follow the prompts to display the CTL Entries window, highlight the item to delete and click **Delete Selected** to delete the entry.

You cannot delete servers that run Cisco Unified CallManager, Cisco TFTP, PIX firewall, or Cisco CAPF from the CTL file.

Two security token entries must exist in the CTL file at all times. You cannot delete all security tokens from the file.

Additional Information

See the [“Related Topics” section on page 31-18](#).

Updating the Clusterwide Security Mode

You must use the Cisco CTL client to configure the clusterwide security mode. You cannot change the clusterwide security mode from the Enterprise Parameters window in Cisco Unified CallManager Administration.

To change the clusterwide security mode after the initial configuration of the Cisco CTL client, you must update the CTL file. Navigate to the Cluster Security Mode window, change the mode setting, and click **Next**, then **Finish**, as described in the [“Updating the CTL File” section on page 31-10](#) and [Table 31-2](#).

If you change the clusterwide security mode from mixed to nonsecure mode, the CTL file still exists on the servers in the cluster, but the CTL file does not contain any certificates. Because no certificates exist in the CTL file, the phone requests an unsigned configuration file and registers as nonsecure with Cisco Unified CallManager.

Cisco CTL Client Configuration Settings

The cluster can exist in one of two modes, as described in [Table 31-2](#). Only mixed mode supports authentication. When you configure the Cisco CTL client for authentication, you must choose Set Cisco Unified CallManager Cluster to Mixed Mode.

Use [Table 31-2](#) to configure the Cisco CTL client for the first time, to update the CTL file, or to change the mode from mixed to nonsecure.

- For configuration tips, see the [“Configuration Tips for Cisco CTL Client Configuration” section on page 31-2](#).
- For related information and procedures, see the [“Related Topics” section on page 31-18](#).

Table 31-2 Configuration Settings for CTL Client

Setting	Description
Cisco Unified CallManager Server	
Hostname or IP Address	Enter the hostname or IP address for the first node.
Port	Enter the port number, which equals the CTL port for the Cisco CTL Provider service that runs on the specified Cisco Unified CallManager server. The default port number equals 2444.
Username and Password	Enter the same username and password that has administrative privileges on the first node.
Security Mode Radio Buttons	
Set Cisco Unified CallManager Cluster to Mixed Mode	Mixed mode allows authenticated or encrypted Cisco Unified IP Phones and nonauthenticated Cisco Unified IP Phones to register with Cisco Unified CallManager. In this mode, Cisco Unified CallManager ensures that authenticated or encrypted devices use a secure port. Note Cisco Unified CallManager disables auto-registration if you configure the cluster for mixed mode.
Set Cisco Unified CallManager Cluster to Non-Secure Mode	All devices register as unauthenticated with Cisco Unified CallManager, and Cisco Unified CallManager supports image authentication only. When you choose this mode, the CTL client removes the certificates for all entries that are listed in the CTL file, but the CTL file still exists in the directory that you specified. The phone requests unsigned configuration files and registers as nonsecure with Cisco Unified CallManager. Tip To revert the phone to the default nonsecure mode, you must delete the CTL file from the phone and all Cisco Unified CallManager servers. You can use auto-registration in this mode.
Update CTL File	After you have created the CTL file, you must choose this option to make any changes to the CTL file. Choosing this option ensures that the Cluster Security mode does not change.
CTL Entries Radio Buttons	
Add Tokens	Click this button to add additional security token(s) to the certificate trust list. If you have not already done so, remove the token that you initially inserted into the server or workstation. When the application prompts you to do so, insert the next token and click OK. When the security token information for the additional token displays, click Add. For all security tokens, repeat these tasks.
Add TFTP Server	Click this button to add an Alternate TFTP server to the certificate trust list. For information on the settings, click the Help button after the Alternate TFTP Server tab settings display. After you enter the settings, click Next.

Table 31-2 Configuration Settings for CTL Client (continued)

Setting	Description
Add Firewall	Click this button to add a firewall (TLS proxy server) to the certificate trust list. For information on the settings, click the Help button after the Firewall tab settings display. After you enter the settings, click Next.
Alternate TFTP Server	
Hostname or IP Address	Enter the hostname or IP address for the TFTP server. Alternate TFTP server designates a Cisco TFTP server that exists in a different cluster. If you use two different clusters for the alternate TFTP server configuration, both clusters must use the same clusterwide security mode, which means that you must install and configure the Cisco CTL client in both clusters. Likewise, both clusters must run the same version of Cisco Unified CallManager. Ensure that the path in the TFTP service parameter, FileLocation, is the same for all servers in the cluster.
Port	Not required with this release of Cisco Unified CallManager.
Username and Password	Not required with this release of Cisco Unified CallManager.
TLS Proxy Server	
Hostname or IP Address	Enter the hostname or IP address for the TLS proxy.
Port	Enter the port number, which equals the CTL port for the Cisco CTL Provider service that runs on the firewall. The default port number equals 2444.
Username and Password	Enter the same username and password that has administrative privileges on the first node.
Security Token	
User Password	The first time that you configure the Cisco CTL client, enter Cisco123 , the case-sensitive default password, to retrieve the private key of the certificate and ensure that the CTL file gets signed.

Verifying the Security Mode for the Cisco Unified CallManager Cluster

To verify the security mode for the Cisco Unified CallManager cluster, perform the following procedure:

Procedure

- Step 1** From Cisco Unified CallManager Administration, choose **System > Enterprise Parameters**.
- Step 2** Locate the **Cluster Security Mode** field. If the value in the field displays as 1, you correctly configured the Cisco Unified CallManager cluster for mixed mode. (Click the field name for more information.)



Tip You cannot configure this value in Cisco Unified CallManager Administration. This value displays after you configure the Cisco CTL client.

Additional Information

See the [“Related Topics” section on page 31-18](#).

Setting the Smart Card Service to Started and Automatic

If the Cisco CTL client installation detects that the Smart Card service is disabled, you must set the Smart Card service to automatic and started on the server or workstation where you are installing the Cisco CTL plug-in.



Tip You cannot add the security tokens to the CTL file if the service is not set to started and automatic.

After you upgrade the operating system, apply service releases, upgrade Cisco Unified CallManager, and so on, verify that the Smart Card service is started and automatic.

To set the service to started and automatic, perform the following procedure:

Procedure

- Step 1** On the server or workstation where you installed the Cisco CTL client, choose **Start > Programs > Administrative Tools > Services** or **Start > Control Panel > Administrative Tools > Services**.
- Step 2** From the Services window, right-click the **Smart Card** service and choose **Properties**.
- Step 3** In the Properties window, verify that the General tab displays.
- Step 4** From the Startup type drop-down list box, choose **Automatic**.
- Step 5** Click **Apply**.
- Step 6** In the Service Status area, click **Start**.

- Step 7** Click **OK**.
- Step 8** Reboot the server or workstation and verify that the service is running.
-

Additional Information

See the [“Related Topics”](#) section on page 31-18.

Changing the Security Token Password (Etoken)

This administrative password retrieves the private key of the certificate and ensures that the CTL file gets signed. Each security token comes with a default password. You can change the security token password at any time. If the Cisco CTL client prompts you to change the password, you must change the password before you can proceed with the configuration.

To review pertinent information on setting passwords, click the **Show Tips** button. If you cannot set the password for any reason, review the tips that display.

To change the security token password, perform the following procedure:

Procedure

-
- Step 1** Verify that you have installed the Cisco CTL client on a Windows server or workstation.
- Step 2** If you have not already done so, insert the security token into the USB port on the Windows server or workstation where you installed the Cisco CTL client.
- Step 3** Choose **Start > Programs > etoken > Etoken Properties**; right-click **etoken** and choose **Change etoken password**.
- Step 4** In the Current Password field, enter the password that you originally created for the token.
- Step 5** Enter a new password.
- Step 6** Enter the new password again to confirm it.
- Step 7** Click **OK**.
-

Additional Information

See the [“Related Topics”](#) section on page 31-18.

Deleting the CTL File on the Cisco Unified IP Phone

**Caution**

Cisco recommends that you perform this task in a secure lab environment, especially if you do not plan to delete the CTL file from the Cisco Unified CallManager servers in the cluster.

Delete the CTL file on the Cisco Unified IP Phone if the following cases occur:

- You lose all security tokens that signed the CTL file.
- The security tokens that signed the CTL file appear compromised.

- You move a phone out of a secure cluster; for example, to a storage area, to a nonsecure cluster, or to another secure cluster in a different domain.
- You move a phone from an area with an unknown security policy to a secure cluster.
- You change the alternate TFTP server address to a server that does not exist in the CTL file.

To delete the CTL file on the Cisco Unified IP Phone, perform the tasks in [Table 31-3](#).

Table 31-3 *Deleting the CTL File on the Cisco Unified IP Phone*

Cisco Unified IP Phone Model	Tasks
Cisco Unified IP Phones 7960 and 7940	Under the Security Configuration menu on the phone, press CTL file , unlock or **# , and erase .
Cisco Unified IP Phone 7970	Perform one of the following methods: • Unlock the Security Configuration menu, as described in <i>Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager</i>. Under the CTL option, press the Erase softkey. • Under the Settings menu, press the Erase softkey. Note Pressing the Erase softkey under the Settings menu deletes other information besides the CTL file. For additional information, refer to the <i>Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager</i>.

Additional Information

See the “[Related Topics](#)” section on page 31-18.

Determining the Cisco CTL Client Version

To determine which version of the Cisco CTL client you are using, perform the following procedure:

Procedure

-
- Step 1** Perform one of the following tasks:
- Double-click the **Cisco CTL Client** icon that exists on the desktop.
 - Choose **Start > Programs > Cisco CTL Client**.
- Step 2** In the Cisco CTL client window, click the icon in the upper, left corner of the window.
- Step 3** Choose **About Cisco CTL Client**. The version of the client displays.
-

Additional Information

See the “[Related Topics](#)” section on page 31-18.

Verifying or Uninstalling the Cisco CTL Client

Uninstalling the Cisco CTL client does not delete the CTL file. Likewise, the clusterwide security mode and the CTL file do not change when you uninstall the client. If you choose to do so, you can uninstall the CTL client, install the client on a different Windows workstation or server, and continue to use the same CTL file.

To verify that the Cisco CTL client installed, perform the following procedure:

Procedure

-
Step 1	Choose Start > Control Panel > Add Remove Programs .
Step 2	Double-click Add Remove Programs .
Step 3	To verify that the client installed, locate Cisco CTL Client .
Step 4	To uninstall the client, click Remove .
-

Additional Information

See the [“Related Topics”](#) section on page 31-18.

Where to Find More Information

Related Topics

- [System Requirements](#), page 30-4
- [Cisco CTL Client Overview](#), page 31-2
- [Cisco CTL Client Configuration Checklist](#), page 31-3
- [Activating the Cisco CTL Provider Service](#), page 31-4
- [Activating the Cisco CAPF Service](#), page 31-5
- [Configuring Ports for the TLS Connection](#), page 31-5
- [Installing the Cisco CTL Client](#), page 31-6
- [Upgrading the Cisco CTL Client and Migrating the Cisco CTL File](#), page 31-7
- [Configuring the Cisco CTL Client](#), page 31-8
- [Updating the CTL File](#), page 31-10
- [Deleting a CTL File Entry](#), page 31-12
- [Updating the Clusterwide Security Mode](#), page 31-12
- [Cisco CTL Client Configuration Settings](#), page 31-12
- [Verifying the Security Mode for the Cisco Unified CallManager Cluster](#), page 31-15
- [Setting the Smart Card Service to Started and Automatic](#), page 31-15
- [Deleting the CTL File on the Cisco Unified IP Phone](#), page 31-16
- [Determining the Cisco CTL Client Version](#), page 31-17
- [Verifying or Uninstalling the Cisco CTL Client](#), page 31-18

- Using the Certificate Authority Proxy Function, *Cisco Unified CallManager Security Guide, Release 5.0(4)*

Related Cisco Documentation

Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager

Troubleshooting Guide for Cisco Unified CallManager



Configuring a Phone Security Profile

This chapter contains information on the following topics:

- [Phone Security Profile Overview, page 32-1](#)
- [Configuration Tips for Phone Security Profiles, page 32-1](#)
- [Finding a Phone Security Profile, page 32-2](#)
- [Configuring a Phone Security Profile, page 32-3](#)
- [Phone Security Profile Configuration Settings, page 32-4](#)
- [Applying a Phone Security Profile, page 32-9](#)
- [Deleting a Phone Security Profile, page 32-10](#)
- [Finding Phones That Use Phone Security Profiles, page 32-11](#)
- [Where to Find More Information, page 32-11](#)

Phone Security Profile Overview

Cisco Unified CallManager Administration groups security-related settings for a phone type and protocol into security profiles to allow you to assign a single security profile to multiple phones. Security-related settings include device security mode, digest authentication, and some CAPF settings. You apply the configured settings to a phone when you choose the security profile in the Phone Configuration window.

Installing Cisco Unified CallManager provides a set of predefined, nonsecure security profiles for auto-registration. To enable security features for a phone, you must configure a new security profile for the device type and protocol and apply it to the phone.

Only the security features that the selected device and protocol support display in the security profile settings window.

Configuration Tips for Phone Security Profiles

Consider the following information when you configure phone security profiles in Cisco Unified CallManager Administration:

- When you configure phones, you must select a security profile in the Phone Configuration window. If the device does not support security, apply the nonsecure profile.

- You cannot delete or change predefined, nonsecure profiles.
- You cannot delete a security profile that is currently assigned to a device.
- If you change the settings in a security profile that is already assigned to a phone, the reconfigured settings apply to all phones that are assigned that profile.
- You can rename security files that are assigned to devices. The phones that are assigned the old profile name and settings assume the new profile name and settings.
- The CAPF settings in the Phone Security Profile, authentication and key size, also display in the Phone Configuration window. You must configure CAPF settings for certificate operations that involve manufacture-installed certificates (MICs) or locally significant certificates (LSCs). You can update these fields directly in the Phone Configuration window.
 - If you update the CAPF settings in the security profile, the settings get updated in the Phone Configuration window.
 - If you update the CAPF settings in the Phone Configuration window and a matching profile is found, Cisco Unified CallManager applies the matching profile to the phone.
 - If you update the CAPF settings in the Phone Configuration window, and no matching profile is found, Cisco Unified CallManager creates a new profile and applies the new profile to the phone.
- If you configured the device security mode prior to a Cisco Unified CallManager 5.0 or later upgrade, Cisco Unified CallManager creates a profile that is based on the model and protocol and applies the profile to the device.
- Cisco recommends using manufacturer-installed certificates (MICs) for LSC installation only. Cisco supports LSCs to authenticate the TLS connection with Cisco Unified CallManager. Because MIC root certificates can be compromised, customers who configure phones to use MICs for TLS authentication or for any other purpose do so at their own risk. Cisco assumes no liability if MICs are compromised.

Cisco recommends upgrading Cisco Unified IP Phone models 7906, 7911, 7941, 7961, 7970, and 7971 to use LSCs for TLS connection to Cisco Unified CallManager and removing MIC root certificates from the Cisco Unified CallManager trust store to avoid possible future compatibility issues. See [“Phone Certificate Types” section on page 30-13](#) for more information.

Finding a Phone Security Profile

To find a phone security profile, perform the following procedure:

Procedure

- Step 1** In Cisco Unified CallManager Administration, choose **System > Security Profile > Phone Security Profile**.
All security profiles that are available on the system display.
- Step 2** From the drop-down list boxes, choose your search criteria for the security profiles that you want to list and click **Find**.



Note To find all security profiles that are registered in the database, click **Find** without specifying any search criteria.

The window refreshes and displays the security profiles that match your search criteria.

Step 3 Click the **Name** link for the security profile that you want to view.



Tip To search for the Name or Description within the search results, check the **Search Within Results** check box, enter your search criteria as described in this procedure, and click **Find**.

Additional Information

See the [“Related Topics” section on page 32-11](#).

Configuring a Phone Security Profile

To add, update, or copy a security profile, perform the following procedure:

Procedure

- Step 1** In Cisco Unified CallManager Administration, choose **System > Security Profile > Phone Security Profile**.
- Step 2** Perform one of the following tasks:
- To add a new profile, click the **Add New** button and continue with [Step 3](#).
 - To copy an existing security profile, locate the appropriate profile as described in [“Finding a Phone Security Profile” section on page 32-2](#), click the **Copy** button next to the security profile that you want to copy, and continue with [Step 3](#).
 - To update an existing profile, locate the appropriate security profile as described in [“Finding a Phone Security Profile” section on page 32-2](#) and continue with [Step 3](#).
- Step 3** Enter the appropriate settings as described in [Table 32-1](#) for SCCP phones or [Table 32-2](#) for SIP phones.
- Step 4** Click **Save**.

Additional Steps

After you create the security profile, apply it to the phone, as described in the [“Applying a Phone Security Profile” section on page 32-9](#).

If you configured digest authentication in the phone security profile for a SIP phone, you must configure the digest credentials in the End User Configuration window. You then must associate the user with the phone by using the Digest User setting in the Phone Configuration window.

Additional Information

See the [“Related Topics” section on page 32-11](#).

Phone Security Profile Configuration Settings

Table 32-1 describes the settings for the SCCP phone security profiles.

Table 32-2 describes the settings for the SIP phone security profile.

Only settings that the selected phone type and protocol support display.

- For configuration tips, see the “[Configuration Tips for Phone Security Profiles](#)” section on page 32-1.
- For related information and procedures, see the “[Related Topics](#)” section on page 32-11.

Table 32-1 **SCCP Phone Security Profile**

Setting	Description
Name	Enter a name for the security profile. When you save the new profile, the name displays in the Device Security Profile drop-down list box in the Phone Configuration window for the phone type and protocol. Tip Include the device model and protocol in the security profile name to help you find the correct profile when you are searching for or updating a profile.
Description	Enter a description for the security profile.
Device Security Mode	From the drop-down list box, choose one of the following options: • Non Secure—No security features except image authentication exist for the phone. A TCP connection opens to Cisco Unified CallManager. • Authenticated—Cisco Unified CallManager provides integrity and authentication for the phone. A TLS connection that uses NULL/SHA opens. • Encrypted—Cisco Unified CallManager provides integrity, authentication, and encryption for the phone. A TLS connection that uses AES128/SHA opens for signaling, and SRTP carries the media for all phone calls.
TFTP Encrypted Config	When this check box is checked, Cisco Unified CallManager encrypts phone downloads from the TFTP server. Refer to “Configuration File Encryption” section on page 30-21, and “Configuring Encrypted Phone Configuration Files” procedure on page 33-1, for more information.

Table 32-1 SCCP Phone Security Profile (continued)

Setting	Description
Authentication Mode	This field allows you to choose the authentication method that the phone uses during the CAPF certificate operation. From the drop-down list box, choose one of the following options: • By Authentication String—Installs/upgrades, deletes, or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone. • By Null String—Installs/upgrades, deletes, or troubleshoots a locally significant certificate without user intervention. This option provides no security; Cisco strongly recommends that you choose this option only for closed, secure environments. • By Existing Certificate (Precedence to LSC)—Installs/upgrades, deletes, or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If a LSC exists in the phone, authentication occurs via the LSC, regardless whether a MIC exists in the phone. If a MIC and LSC exist in the phone, authentication occurs via the LSC. If a LSC does not exist in the phone, but a MIC does exist, authentication occurs via the MIC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. At any time, the phone uses only one certificate to authenticate to CAPF even though a MIC and LSC can exist in the phone at the same time. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate via the other certificate, you must update the authentication mode. • By Existing Certificate (Precedence to MIC)—Installs/upgrades, deletes, or troubleshoots a locally significant certificate if a LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs via the MIC, regardless whether a LSC exists in the phone. If a LSC exists in the phone, but a MIC does not exist, authentication occurs via the LSC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. Note The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window (see “Configuration Tips for Phone Security Profiles” section on page 32-1, for more details). Refer to the <i>Cisco Unified CallManager Administration Guide</i> for information about configuring these settings on the Phone Configuration window.

Table 32-1 *SCCP Phone Security Profile (continued)*

Setting	Description
Key Size	For this setting that is used for CAPF, choose the key size for the certificate from the drop-down list box. The default setting equals 1024. Other options include 512 and 2048. If you choose a higher key size than the default setting, the phones take longer to generate the entropy that is required to generate the keys. Key generation, which is set at low priority, allows the phone to function while the action occurs. Depending on the phone model, you may notice that key generation takes up to 30 or more minutes to complete. Note The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window (see “Configuration Tips for Phone Security Profiles” section on page 32-1 for more details). Refer to the <i>Cisco Unified CallManager Administration Guide</i> for configuring these settings on the Phone Configuration window.

Table 32-2 *SIP Phone Security Profile*

Setting	Description
Name	Enter a name for the security profile. When you save the new profile, the name displays in the Device Security Profile drop-down list box in the Phone Configuration window for the phone type and protocol. Tip Include the device model and protocol in the security profile name to help you find the correct profile when you are searching for or updating a profile.
Description	Enter a description for the security profile.
Nonce Validity Time	Enter the number of minutes (in seconds) that the nonce value is valid. The default value equals 600 (10 minutes). When the time expires, Cisco Unified CallManager generates a new value. Note A nonce value, a random number that supports digest authentication, gets used to calculate the MD5 hash of the digest authentication password.
Device Security Mode	From the drop-down list box, choose one of the following options: • Non Secure—No security features except image authentication exist for the phone. A TCP connection opens to Cisco Unified CallManager. • Authenticated—Cisco Unified CallManager provides integrity and authentication for the phone. A TLS connection that uses NULL/SHA opens. • Encrypted—Cisco Unified CallManager provides integrity, authentication, and encryption for the phone. A TLS connection that uses AES128/SHA opens for signaling, and SRTP carries the media for all phone calls on all SRTP-capable SIP hops.

Table 32-2 SIP Phone Security Profile (continued)

Setting	Description
Transport Type	When Device Security Mode is Non Secure, choose one of the following options from the drop-down list box (some options may not display): • TCP—Choose the Transmission Control Protocol to ensure that packets get received in the same order as the order in which they are sent. This protocol ensures that no packets get dropped, but the protocol does not provide any security. • UDP—Choose the User Datagram Protocol to ensure that packets are received quickly. This protocol, which can drop packets, does not ensure that packets are received in the order in which they are sent. This protocol does not provide any security. • TCP + UDP—Choose this option if you want to use a combination of TCP and UDP. This option does not provide any security. When Device Security Mode is Authenticated or Encrypted, TLS specifies the Transport Type. TLS provides signaling integrity, device authentication, and signaling encryption (encrypted mode only) for SIP phones. If Device Security Mode cannot be configured in the profile, the transport type specifies UDP.
Enable Digest Authentication	If you check this check box, Cisco Unified CallManager challenges all SIP requests from the phone. Digest authentication does not provide device authentication, integrity, or confidentiality. Choose a security mode of authenticated or encrypted to use these features. Note For more information on digest authentication, see “Digest Authentication” section on page 30-17 and “Configuring Digest Authentication for the SIP Phone” in the <i>Cisco Unified CallManager Security Guide, Release 5.0(4)</i>.
TFTP Encrypted Config	When this check box is checked, Cisco Unified CallManager encrypts phone downloads from the TFTP server. This option exists for Cisco phones only. Tip Cisco recommends that you enable this option and configure a symmetric key to secure digest credentials and administrative passwords. Refer to “Configuration File Encryption” section on page 30-21, and “Configuring Encrypted Phone Configuration Files” section on page 33-1, for more information.
Exclude Digest Credentials in Configuration File	When this check box is checked, Cisco Unified CallManager omits digest credentials in phone downloads from the TFTP server. This option exists for Cisco Unified IP SIP Phone models 7905, 7912, 7940, and 7960 only. Refer to “Configuration File Encryption” section on page 30-21, and “Configuring Encrypted Phone Configuration Files” section on page 33-1, for more information.

Table 32-2 SIP Phone Security Profile (continued)

Setting	Description
Authentication Mode	This field allows you to choose the authentication method that the phone uses during the CAPF certificate operation. This option exists for Cisco phones only. From the drop-down list box, choose one of the following options: • By Authentication String—Installs/upgrades or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone. • By Null String—Installs/upgrades or troubleshoots a locally significant certificate without user intervention. This option provides no security; Cisco strongly recommends that you choose this option only for closed, secure environments. • By Existing Certificate (Precedence to LSC)—Installs/upgrades or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If a LSC exists in the phone, authentication occurs via the LSC, regardless whether a MIC exists in the phone. If a LSC does not exist in the phone, but a MIC does exist, authentication occurs via the MIC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. At any time, the phone uses only one certificate to authenticate to CAPF even though a MIC and LSC can exist in the phone at the same time. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate via the other certificate, you must update the authentication mode. • By Existing Certificate (Precedence to MIC)—Installs/upgrades or troubleshoots a locally significant certificate if a LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs via the MIC, regardless whether a LSC exists in the phone. If a LSC exists in the phone, but a MIC does not exist, authentication occurs via the LSC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. Note The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window (see “Configuration Tips for Phone Security Profiles” section on page 32-1 in this section for more details). Refer to the <i>Cisco Unified CallManager Administration Guide</i> for information about configuring these settings on the Phone Configuration window.

Table 32-2 SIP Phone Security Profile (continued)

Setting	Description
Key Size	For this setting that is used for CAPF, choose the key size for the certificate from the drop-down list box. The default setting equals 1024. Other options include 512 and 2048. If you choose a higher key size than the default setting, the phones take longer to generate the entropy that is required to generate the keys. Key generation, which is set at low priority, allows the phone to function while the action occurs. Depending on the phone model, you may notice that key generation takes up to 30 or more minutes to complete. Note The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window (see “Configuration Tips for Phone Security Profiles” section on page 32-1, in this section for more details). Refer to the <i>Cisco Unified CallManager Administration Guide</i> for information about configuring these settings on the Phone Configuration window.
SIP Phone Port	This setting applies to SIP phones that are using UDP transport. Enter the port number for Cisco Unified SIP IP Phones that are using UDP to listen for SIP messages from Cisco Unified CallManager. The default setting equals 5060. Phones that are using TCP or TLS ignore this setting.

Applying a Phone Security Profile

You apply a phone security profile to the phone in the Phone Configuration window.

Before You Begin

Before you apply a security profile that uses certificates for authentication of the phone, ensure that phone contains a locally significant certificate (LSC) or manufacture-installed certificate (MIC). If the phone does not contain a certificate, perform the following steps:

1. In the Phone Configuration window, apply a nonsecure profile.
2. In the Phone Configuration window, install a certificate by configuring the CAPF settings. For more information on performing this task, see the “Using the Certificate Authority Proxy Function” chapter in the *Cisco Unified CallManager Security Guide, Release 5.0(4)*.
3. In the Phone Configuration window, apply a device security profile that is configured for authentication or encryption.

To apply a phone security profile to a device, perform the following procedure:

Procedure

-
- Step 1** Find the phone, as described in the *Cisco Unified CallManager Administration Guide*.
 - Step 2** After the Phone Configuration window displays, locate the **Device Security Profile**.

- Step 3** From the **Device Security Profile** drop-down list box, choose the security profile that applies to the device. Only the phone security profiles that are configured for the phone type and protocol display.
- Step 4** Click **Save**.
- Step 5** To reset the phone, click **Reset**.
-

Additional Steps

If you configured digest authentication for SIP phones, you must configure the digest credentials in the End User Configuration window. Then, you must configure the Digest User setting in the Phone Configuration window. For more information about configuring digest users and digest credentials, refer to the “Configuring Digest Authentication for the SIP Phone” chapter in the *Cisco Unified CallManager Security Guide, Release 5.0(4)*.

Additional Information

See the [“Related Topics” section on page 32-11](#).

Deleting a Phone Security Profile

This section describes how to delete a phone security profile from the Cisco Unified CallManager database.

Before You Begin

Before you can delete a security profile from Cisco Unified CallManager Administration, you must apply a different profile to the devices or delete all devices that use the profile. To find out which devices use the profile, choose **Dependency Records** from the Related Links drop-down list box in the Security Profile Configuration window and click **Go**.

If the dependency records feature is not enabled for the system, go to **System > Enterprise Parameters** and change the Enable Dependency Records setting to True. A message displays information about high CPU consumption that relates to the dependency records feature. Save your change to activate dependency records. For more information about dependency records, refer to the *Cisco Unified CallManager System Guide*.

Procedure

- Step 1** Find the security profile by using the procedure in the [“Finding a Phone Security Profile” section on page 32-2](#).
- Step 2** To delete multiple security profiles, check the check boxes next to the appropriate check box in the Find and List window; then, click the **Delete Selected** icon or the **Delete Selected** button.

- Step 3** To delete a single security profile, perform one of the following tasks:
- In the Find and List window, check the check box next to the appropriate security profile; then, click the **Delete Selected** icon or the **Delete Selected** button.
 - In the Find and List window, click the Name link for the security profile. After the specific Security Profile Configuration window displays, click the **Delete** icon or the **Delete** 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 32-11.

Finding Phones That Use Phone Security Profiles

To find a phone that uses the Phone Security Profile, perform the following procedure:

- Step 1** In Cisco Unified CallManager Administration, choose **Device > Phone**.
- Step 2** From the **Find Phone where** drop-down list box, choose **Security Profile**.
- Step 3** If you want to do so, specify additional search criteria for the security profile by choosing an option in the drop-down list box next to the Find Phone drop-down list box; then, enter the specific search criteria.
- Step 4** After you specify your search criteria, click **Find**. The search results display.
-

Additional Information

See the [“Related Topics”](#) section on page 32-11.

Where to Find More Information

Related Topics

- [Digest Authentication](#), page 30-17
- [Configuration File Encryption](#), page 30-21
- [Phone Security Profile Overview](#), page 32-1
- [Configuration Tips for Phone Security Profiles](#), page 32-1
- [Finding a Phone Security Profile](#), page 32-2
- [Configuring a Phone Security Profile](#), page 32-3
- [Phone Security Profile Configuration Settings](#), page 32-4
- [Applying a Phone Security Profile](#), page 32-9
- [Deleting a Phone Security Profile](#), page 32-10
- [Finding Phones That Use Phone Security Profiles](#), page 32-11
- [Configuring Encrypted Phone Configuration Files](#), page 33-1

- Configuring Digest Authentication for the SIP Phone, *Cisco Unified CallManager Security Guide, Release 5.0(4)*
- Phone Hardening, *Cisco Unified CallManager Security Guide, Release 5.0(4)*

Related Cisco Documentation

Cisco Unified CallManager Administration Guide

Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager



Configuring Encrypted Phone Configuration Files

After you configure security-related settings, the phone configuration file contains sensitive information, such as digest passwords and phone administrator passwords. To ensure privacy of the configuration file, you must configure the configuration files for encryption.

This chapter contains information on the following topics:

- [Understanding Encryption of the Phone Configuration File, page 33-1](#)
- [Supported Phone Models, page 33-4](#)
- [Configuration Tips for Encrypted Configuration Files, page 33-4](#)
- [Encryption Configuration File Configuration Checklist, page 33-5](#)
- [Enabling Phone Configuration File Encryption, page 33-6](#)
- [Configuring Manual Key Distribution, page 33-6](#)
- [Manual Key Distribution Configuration Settings, page 33-7](#)
- [Entering the Symmetric Key on the Phone, page 33-7](#)
- [Verifying That an LSC or MIC Certificate Is Installed, page 33-8](#)
- [Verifying That the Phone Configuration File Is Encrypted, page 33-8](#)
- [Disabling Encryption for the Phone Configuration Files, page 33-9](#)
- [Where to Find More Information, page 33-10](#)

Understanding Encryption of the Phone Configuration File

To secure digest credentials and secured passwords in phone downloads from Cisco Unified CallManager, you must enable the TFTP Encrypted Config option in the Phone Security Profile Configuration window and perform additional tasks in Cisco Unified CallManager Administration.

After you enable the TFTP Encrypt Config option, configure the required parameters in Cisco Unified CallManager Administration and the phone and restart required services in Cisco Unified CallManager Serviceability, the TFTP server

1. Deletes all clear text configuration files on disk
2. Generates encrypted versions of the configuration files.

If the phone supports encrypted phone configuration files and if you performed the necessary tasks for phone configuration file encryption, the phone requests an encrypted version of the configuration file.

**Warning**

If digest authentication is True for the SIP phone when the TFTP encrypted configuration setting is False, digest credentials may get sent in the clear. See [“Disabling Encryption for the Phone Configuration Files” section on page 33-9](#) for more information.

Some phone models do not support encrypted phone configuration files, as described in [“Supported Phone Models” section on page 33-4](#). The phone model and protocol determine the method that the system uses to encrypt the configuration file. Supported methods rely on Cisco Unified CallManager functionality and a firmware load that supports encrypted configuration files. If you downgrade the phone firmware load to a version that does not support encrypted configuration files, the TFTP server offers an unencrypted configuration file that provides minimal configuration settings, and the phone may not perform as expected.

To ensure that you maintain the privacy of the key information, Cisco strongly recommends that you perform the tasks that are associated with encrypted phone configuration files in a secure environment.

Cisco Unified CallManager supports the following methods:

- [Manual Key Distribution](#)
- [Symmetric Key Encryption with Phone Public Key](#)

The information in the [“Manual Key Distribution”](#) and [“Symmetric Key Encryption with Phone Public Key”](#) sections assumes that you configured the cluster for Mixed Mode and that you enabled the TFTP Encrypted Config parameter in Cisco Unified CallManager Administration.

Manual Key Distribution

**Tip**

For a list of phone models that support this method, see [“Supported Phone Models” section on page 33-4](#).

With manual key distribution, a 128- or 256-bit symmetric key, which is stored in the Cisco Unified CallManager database, encrypts the phone configuration file after the phone resets. To determine the key size for your phone model, see [“Supported Phone Models” section on page 33-4](#).

To encrypt the configuration file, the administrator can either manually enter the key into Cisco Unified CallManager Administration or prompt Cisco Unified CallManager Administration to generate the key in the Phone Configuration window. After the key exists in the database, the administrator or user must enter the key into the phone by accessing the user interface on the phone; the phone stores the key in flash as soon as you press the **Accept** softkey. After the key is entered, the phone requests an encrypted configuration file after it is reset. After the required tasks occur, the symmetric key uses RC4 or AES 128 encryption algorithms to encrypt the configuration file. To determine which phones use the RC4 or AES 128 encryption algorithms, see [“Supported Phone Models” section on page 33-4](#).

When the phone contains the symmetric key, the phone always requests the encrypted configuration file. Cisco Unified CallManager downloads the encrypted configuration file to the phone, which the TFTP server signs. Not all phone types validate the signer of the configuration file; see [“Supported Phone Models” section on page 33-4](#) for more information.

The phone decrypts the file contents by using the symmetric key that is stored in flash. If decryption fails, the configuration file does not get applied to the phone.

**Tip**

If the TFTP Encrypted Config setting gets disabled, administrators must remove the symmetric key from the phone GUI so that the phone requests an unencrypted configuration file the next time that it is reset.

Symmetric Key Encryption with Phone Public Key

**Tip**

For a list of phone models that support this method, see [“Supported Phone Models” section on page 33-4](#).

For more information about The Certificate Authority Proxy Function (CAPF), see “Certificate Authority Proxy Function Overview” section in the *Cisco Unified CallManager Security Guide, Release 5.0(4)*. The Certificate Authority Proxy Function (CAPF) authenticates Cisco Unified IP Phones to Cisco Unified CallManager and issues phone certificates (LSCs).

If the phone contains a manufacturing-installed certificate (MIC) or a locally significant certificate (LSC), the phone contains a public and private key pair, which are used for PKI encryption.

If you are using this method for the first time, the phone compares the MD5 hash of the phone certificate in the configuration file to the MD5 hash of the LSC or MIC. If the phone does not identify a problem, the phone requests an encrypted configuration file from the TFTP server after the phone resets. If the phone identifies a problem, for example, the hash does not match, the phone does not contain a certificate, or the MD5 value is blank, the phone attempts to initiate a session with CAPF unless the CAPF authentication mode equals By Authentication String (in which case, you must manually enter the string). CAPF extracts the phone public key from the LSC or MIC, generates a MD5 hash, and stores the values for the public key and certificate hash in the Cisco Unified CallManager database. After the public key gets stored in the database, the phone resets and requests a new configuration file.

After the public key exists in the database and the phone resets, the symmetric key encryption process begins after the database notifies TFTP that the public key exists for the phone. The TFTP server generates a 128-bit symmetric key, which encrypts the configuration file with the Advanced Encryption Standard (AES) 128 encryption algorithm. Then, the phone public key encrypts the symmetric key, which it includes in the signed envelope header of the configuration file. The phone validates the file signing, and, if the signature is valid, the phone uses the private key from the LSC or MIC to decrypt the encrypted symmetric key. The symmetric key then decrypts the file contents.

Every time that you update the configuration file, the TFTP server automatically generates a new key to encrypt the file.

**Tip**

For phones that support this encryption method, the phone uses the encryption configuration flag in the configuration file to determine whether to request an encrypted or unencrypted file. If the TFTP Encrypted Config setting is disabled, and Cisco Unified IP Phone models 7911, 7941, 7961, 7970, and 7971 request an encrypted file (.enc.sgn file), Cisco Unified CallManager sends a ‘file not found error’ to the phone. The phone then requests an unencrypted, signed file (.sgn file).

If the TFTP Encrypted Config setting is enabled but the phone requests an unencrypted configuration file for some reason, the TFTP server offers an unencrypted file that contains minimal configuration settings. After the phone receives the minimum configuration, the phone can detect error conditions, such as key mismatch, and may start a session with CAPF to synchronize the phone public key with the Cisco Unified CallManager database. If the error condition is resolved, the phone requests an encrypted configuration file the next time that it resets.

Supported Phone Models

You can encrypt the phone configuration file for the following Cisco Unified IP Phone models:

Phone Model and Protocol	Encryption Method
Cisco Unified SIP IP Phone 7905 or 7912	Manual key distribution— Encryption algorithm: RC4 Key size: 256 bits File signing support: No
Cisco Unified SIP IP Phone 7940 or 7960	Manual key distribution— Encryption algorithm: Advanced Encryption Standard (AES) 128 Key size: 128 bits File signing support: These SIP phones receive signed, encrypted configuration files but ignore the signing information.
Cisco Unified SIP IP Phone 7970 or 7971; Cisco Unified SIP IP Phone 7941 or 7961; Cisco Unified SIP IP Phone 7911; Cisco Unified SIP IP Phone 7906 Cisco Unified SCCP IP Phone 7970 or 7971; Cisco Unified SCCP IP Phone 7941 or 7961; Cisco Unified SCCP IP Phone 7911; Cisco Unified SCCP IP Phone 7906	Symmetric key encryption with phone public key (PKI encryption)— Encryption algorithm: AES 128 Key size: 128 bits File signing support: Yes

Configuration Tips for Encrypted Configuration Files

Cisco recommends that you enable the TFTP Encrypted Config flag to secure confidential data in phone downloads. For phones that do not have PKI capabilities, you must also configure a symmetric key in Cisco Unified CallManager Administration and in the phone. If the symmetric key is missing from either the phone or Cisco Unified CallManager or if a mismatch occurs when the TFTP Encrypted Config flag is set, the phone cannot register.

Consider the following information when you configure encrypted configuration files in Cisco Unified CallManager Administration:

- Only phones that support encrypted configuration files display the TFTP Encrypted Config flag in the phone security profile. You cannot configure encrypted configuration files for Cisco Unified IP SCCP Phone models 7905, 7912, 7940, and 7960 because these phones do not receive confidential data in the configuration file download.
- The default setting for TFTP Encrypted Config specifies false (not checked). If you apply the default, non-secure profile to the phone, digest credentials and secured passwords get sent in the clear.
- For Cisco Unified Phone models that use public key encryption, Cisco Unified CallManager does not require you to set the Device Security Mode to authenticated or encrypted to enable encrypted configuration files. Cisco Unified CallManager uses the CAPF process for downloading its public key during registration.

- You may choose to download unencrypted configuration files to phones if you know your environment is secure or to avoid manually configuring symmetric keys for phones that are not PKI-enabled; however, Cisco does not recommend using this method.
- For Cisco Unified IP SIP Phone models 7905, 7912, 7940, and 7960, Cisco Unified CallManager Administration provides a method of sending digest credentials to the phone that is easier, but less secure, than using an encrypted configuration file. This method, which is useful for initializing digest credentials because it does not require you to first configure a symmetric key and enter it on the phone, uses the TFTP Exclude Digest Credential in Configuration File setting.

With this method, you send the digest credentials to the phone in an unencrypted configuration file. After the credentials are in the phone, Cisco recommends that you keep the TFTP file encryption setting disabled and enable the TFTP Exclude Digest Credential in Configuration File flag on the corresponding security profile window, which will exclude digest credentials from future downloads.

After digest credentials exist in these phones and an incoming file does not contain digest credentials, the existing credentials remain in place. The digest credentials remain intact until the phone is factory reset or new credentials (including blanks) are received.

If you change digest credentials for a phone or end user, temporarily disable the Exclude Digest Credentials flag on the corresponding security profile window to download the new digest credentials to the phone.

Encryption Configuration File Configuration Checklist

Use [Table 33-1](#) to guide you through the configuration process for encrypted configuration files in Cisco Unified CallManager Administration.

Table 33-1 *Encryption Configuration File Configuration Checklist*

Configuration Steps		Related Procedures and Topics
Step 1	Verify that the Cluster Security Mode is configured for Mixed Mode.	Configuring the Cisco CTL Client, page 31-1
Step 2	In Cisco Unified CallManager Administration, check the TFTP Encrypted Config check box in the Phone Security Profile. Be sure to apply the profile to the phone.	• Configuration Tips for Encrypted Configuration Files, page 33-4 • Enabling Phone Configuration File Encryption, page 33-6 • Applying a Phone Security Profile, page 32-9
Step 3	Determine which phones support manual key distribution and which phones support symmetric key encryption with phone public key (PKI encryption).	Supported Phone Models, page 33-4

Table 33-1 **Encryption Configuration File Configuration Checklist (continued)**

Configuration Steps		Related Procedures and Topics
Step 4	If your phone supports manual key distribution, perform the manual key distribution tasks in Cisco Unified CallManager Administration.	• Configuration Tips for Encrypted Configuration Files, page 33-4 • Configuring Manual Key Distribution, page 33-6 • Manual Key Distribution Configuration Settings, page 33-7
Step 5	If your phone supports manual key distribution, enter the symmetric key on the phone; reset the phone.	Entering the Symmetric Key on the Phone, page 33-7
Step 6	If your phone supports the method, symmetric key encryption with phone public key (PKI encryption), verify that a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone.	• Verifying That an LSC or MIC Certificate Is Installed, page 33-8 • Using the Certificate Authority Proxy Function, <i>Cisco Unified CallManager Security Guide, Release 5.0(4)</i>

Enabling Phone Configuration File Encryption

The TFTP server queries the database when it builds the configuration file. If the phone security profile that is applied to the phone has the TFTP encrypted configuration flag set, the TFTP server builds an encrypted configuration file.

To access the TFTP encryption flag, find the appropriate device security profile for the phone, as described in [“Finding a Phone Security Profile” section on page 32-2](#). Check the TFTP Encrypted Config check box to enable configuration file encryption.

Additional Information

See the [“Related Topics” section on page 33-10](#)

Configuring Manual Key Distribution

To determine whether your phone supports manual key distribution, see [“Supported Phone Models” section on page 33-4](#).

The following procedure assumes that

- The phone exists in the Cisco Unified CallManager database,
- A compatible firmware load exists on the TFTP server,
- You enabled the TFTP Encrypted Config parameter in Cisco Unified CallManager Administration.

Procedure

-
- Step 1** Find the phone, as described in the *Cisco Unified CallManager Administration Guide*.
- Step 2** After the Phone Configuration window displays, configure the manual key distribution settings that are described in [Table 33-2](#). After you have configured these settings, the key should not be changed.
- Step 3** Click **Save**.

- Step 4** Enter the symmetric key on the phone and then reset the phone. For information on how to perform these tasks, refer to the phone administration guide that supports your phone model.

Additional Information

See the [“Related Topics” section on page 33-10](#).

Manual Key Distribution Configuration Settings

[Table 33-2](#) describes the manual distribution configuration settings in the Phone Configuration window.

- For configuration tips, see the [“Configuration Tips for Encrypted Configuration Files” section on page 33-4](#).
- For related information and procedures, see the [“Related Topics” section on page 33-10](#).

Table 33-2 *Manual Key Distribution Configuration Settings*

Setting	Description
Symmetric Key	Enter a string of hexadecimal characters that you want to use for the symmetric key. Valid characters include numerals, 0-9, and uppercase /lowercase 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 After the key is configured, you should not change it.
Generate String	If you want Cisco Unified CallManager Administration to generate a hexadecimal string for you, click the Generate String button. After the key is configured, you should not change it.
Revert to Database Value	If you want to restore the value that exists in the database, click this button.

Entering the Symmetric Key on the Phone

For information on how to enter the symmetric key on the phone after you configure manual key distribution in Cisco Unified CallManager Administration, refer to the Cisco Unified IP Phone administration guide that supports your phone model and protocol.

Verifying That an LSC or MIC Certificate Is Installed

This procedure applies to Cisco Unified IP Phones that use PKI encryption. To determine whether your phone supports the method, symmetric key encryption with phone public key (PKI encryption), see the [“Supported Phone Models” section on page 33-4](#).

The following procedure assumes that the phone exists in the Cisco Unified CallManager database and that you enabled the TFTP Encrypted Config parameter in Cisco Unified CallManager Administration.

Procedure

-
- Step 1** Verify that a manufacture-installed certificate (MIC) or a locally significant certificate (LSC) exists in the phone.
- Tip** By choosing the Troubleshooting option in the CAPF settings section of the Phone Configuration window, you can verify that an LSC or MIC exists in the phone in Cisco Unified CallManager administration. The Delete and Troubleshoot options do not display if a certificate does not exist in the phone.
- You can also verify that an LSC or MIC exists in the phone by checking the security configuration at the phone. Refer to the Cisco Unified IP Phone administration guides for Cisco Unified IP Phone models that support this version of Cisco Unified CallManager for more information.
- Step 2** If a certificate does not exist, install an LSC by using the CAPF functionality in the Phone Configuration window. For information on how to install a LSC, see “Using the Certificate Authority Proxy Function” in the *Cisco Unified CallManager Security Guide, Release 5.0(4)*.
- Step 3** After you configure the CAPF settings, click **Save**.
- Step 4** In the Phone Configuration window, click **Reset**. The phone requests an encrypted configuration file from the TFTP server after the phone resets
-

Additional Information

See the [“Related Topics” section on page 33-10](#).

Verifying That the Phone Configuration File Is Encrypted

When the phone configuration file is encrypted, it uses the following format:

- Cisco Unified IP Phone models 7905 and 7912 (SIP protocol only)—LD <MAC>.x
- Cisco Unified IP Phone models 7940 and 7960 (SIP protocol only)—SIP<MAC>.cnf.enc.sgn
- Cisco Unified IP Phone models 7911, 7941, 7961, 7970, and 7971 —SEP<MAC>.cnf.xml.enc.sgn

To access the configuration file at the phone, refer to the Cisco Unified IP Phone administration guides for Cisco Unified IP Phone models that support encryption and this version of Cisco Unified CallManager for more information.

Disabling Encryption for the Phone Configuration Files

To disable encryption for the phone configuration files, you must uncheck the TFTP Encrypted Config check box in the phone security profile in Cisco Unified CallManager Administration and save your change.



Warning

If digest authentication is True for the SIP phone when the TFTP encrypted configuration setting is False, digest credentials may get sent in the clear.

After you update the setting, the encryption keys for the phone remain in the Cisco Unified CallManager database.

If Cisco Unified IP Phone models 7911, 7941, 7961, 7970, and 7971 request an encrypted file (.enc.sgn file) when the encrypted configuration setting gets updated to false, the phone requests a unencrypted, signed file (.sgn file).

If Cisco Unified IP SIP Phone models 7940/7960/7905/7912 request an encrypted file when the encryption configuration setting gets updated to false, administrators must remove the symmetric key from the phone GUI so the phone requests an unencrypted configuration file the next time that it is reset.



Tip

For Cisco Unified IP SIP Phone models 7940 and 7960, enter a 32-byte 0 as the key value for the symmetric key at the phone GUI to disable encryption. For Cisco Unified IP SIP Phone models 7905 and 7912, delete the symmetric key at the phone GUI to disable encryption. For information on how to perform these tasks, refer to the phone administration guide that supports your phone model.

Excluding Digest Credentials from Phone Configuration File Download

To exclude digest credentials from the configuration file that is sent to phones after the initial configuration, check the TFTP Exclude Digest Credentials in Configuration File check box for the security profile that is applied to the phone. Only Cisco Unified IP SIP Phone models 7905, 7912, 7940, and 7960 support this option.

You may need to uncheck this check box to update the configuration file for changes to digest credentials. See the [“Configuration Tips for Encrypted Configuration Files”](#) section on page 33-4 for more information.

Additional Information

See the [“Related Topics”](#) section on page 33-10.

Where to Find More Information

Related Topics

- [Understanding Encryption of the Phone Configuration File, page 33-1](#)
- [Supported Phone Models, page 33-4](#)
- [Configuration Tips for Encrypted Configuration Files, page 33-4](#)
- [Encryption Configuration File Configuration Checklist, page 33-5](#)
- [Enabling Phone Configuration File Encryption, page 33-6](#)
- [Configuring Manual Key Distribution, page 33-6](#)
- [Manual Key Distribution Configuration Settings, page 33-7](#)
- [Entering the Symmetric Key on the Phone, page 33-7](#)
- [Verifying That an LSC or MIC Certificate Is Installed, page 33-8](#)
- [Verifying That the Phone Configuration File Is Encrypted, page 33-8](#)
- [Disabling Encryption for the Phone Configuration Files, page 33-9](#)
- [Excluding Digest Credentials from Phone Configuration File Download, page 33-9](#)
- [Using the Certificate Authority Proxy Function, *Cisco Unified CallManager Security Guide, Release 5.0\(4\)*](#)
- [Configuration Tips for Phone Security Profiles, page 32-1](#)

Related Cisco documentation

- *Cisco Unified CallManager Bulk Administration Guide*
- Cisco Unified IP Phone administration guide for the phone model and protocol



PART 10

Cisco Unified CallManager Bulk Administration Guide





Working with Licenses

The Cisco Unified Presence Server (CUPS), a critical component for delivering the full value of a Cisco Unified Communications environment, collects information about user availability. Using this information, applications such as Cisco Unified Personal Communicator (CUPC) and Cisco Unified CallManager can improve productivity by determining the most effective way for collaborative communication.

You can use the CUPS menu in BAT to update and export licenses of all CUPS and CUPC users.



Note

You can also use BAT for the bulk license capability assignment for CUPS and CUPC using Update CUPS/CUPC Users menu.

Using the CUPS Menu

This section describes the CUPS menu in BAT and details its use to update and export the CUPS and CUPC users.

New additions to the Bulk Administration menu under CUPS include the following two items:

- **Export CUPS/CUPC Users** — Bulk Administration>CUPS>Export CUPS/CUPC Users
- **Update CUPS/CUPC Users** — Bulk Administration>CUPS>Update CUPS/CUPC Users

Export CUPS/CUPC Users

You can use the Export Users Query window to obtain the current license information about all users for CUPS and CUPC.



Note

No option currently exists to select a subset of CUPS users; all CUPS users in the system get exported to file.

Use the following steps to Export licenses:

- Step 1** Navigate to the Export Users Query window.
- Step 2** To view the basic user information and their license status, click Find.
- Step 3** To view the Export window for CUPS/CUPC, click Next.

Step 4 Specify the file name to be exported and click Submit to start the BAT job.

Step 5 Go to the Job Scheduler window to view the status of the BAT job that is submitted.



Note After the job is completed, you can go to the Upload/Download Files window to download the exported .csv file.

Update CUPS/CUPC Users

Use the following steps to add/change the license:

Step 1 Use the Upload/Download Files window to upload the csv file.



Note You must ensure that you select the correct BAT target and transaction type while uploading the csv file.

Step 2 Navigate to the Update CUPS window, select the csv file that is uploaded, and submit the job.



Note You can choose to run the job immediately or later by clicking the respective radio button. If you choose Run Later, you need to use the Job Scheduler window to schedule and activate this job.

Step 3 Use the Job Scheduler window to monitor the progress of the BAT job that is submitted.



Note Refer to the *Cisco Unified CallManager Bulk Administration Guide 5.0(4)* for detailed information on the rest of the BAT features.



Updating the Region Matrix

The region tables define physical locations, whereas the region matrix tables define available bandwidth within (intra) and between (inter) regions. Use the Region Matrix menu in BAT to populate or depopulate the region matrix.

Populating and Depopulating the Region Matrix

Use the following steps to populate or depopulate the region matrix:

-
- Step 1** Choose **Bulk Administration>Region Matrix>Populate/Depopulate Region Matrix**. The Region Matrix Configuration window displays.
 - Step 2** In the Region Matrix Options section, choose Populate Region Matrix or Depopulate Region Matrix based on what you want to do.
 - Step 3** In the Job Information section, enter a name for the job. This helps you to identify your job.
 - Step 4** Select Run now or Run later depending upon when you want to run the job.
 - Step 5** Click the Submit button.
 - Step 6** View the Job Scheduler window to check the status of the job that you submitted. You can use this window to reschedule the job if required.



Note

Unlike other BAT processes, the progress of a job to populate or depopulate the region matrix cannot be measured in terms of records passed, failed, or processed. You can view the results only after the entire process is complete.



Note

The number of records criterion does not apply to this transaction.

An administrator can change the region bandwidth defaults, however, you cannot do this through the BAT menu.

**Note**

Choose **System>Service Parameters** in Cisco Unified CallManager to access the region bandwidth defaults. The parameter type specifies Cisco CallManager, and the four parameters of interest comprise part of the Clusterwide Parameters (System - Location and Region) section.

**Note**

Refer to the *Cisco Unified CallManager Bulk Administration Guide 5.0(4)* for detailed information on the rest of the BAT features.



PART 11

Cisco Unified CallManager Developers Guide





AXL Programming

To access all AXL SOAP API downloads and AXL requests and responses found in this chapter, refer to http://www.cisco.com/pcgi-bin/dev_support/access_level/product_support

This chapter contains the following sections:

- [Introduction, page 36-1](#)
- [Target Audience for this Chapter, page 36-2](#)
- [New and Changed Information, page 36-2](#)
- [AXL API, page 36-3](#)
- [Example AXL Requests, page 36-5](#)
- [Throttling of Requests, page 36-12](#)
- [The AXL Schema Documentation, page 36-12](#)
- [Example XML Structure, page 36-13](#)
- [Authentication, page 36-14](#)
- [Data Encryption, page 36-14](#)
- [Integration Considerations and Interoperability, page 36-14](#)

Introduction

The Administrative XML Layer (AXL) Application Programming Interface (API) provides a mechanism for inserting, retrieving, updating, and removing data from the database by using an eXtensible Markup Language (XML) Simple Object Access Protocol (SOAP) interface. This allows a programmer to access Cisco Unified CallManager data by using XML and receive the data in XML form, instead of using a binary library or DLL.

The AXL API methods, known as requests, use a combination of HTTP and SOAP. SOAP is an XML remote procedure call (RPC) protocol. Users perform requests by sending XML data to the Cisco Unified CallManager server. The server then returns the AXL response, which is also a SOAP message.

Target Audience for this Chapter

This chapter targets somewhat experienced developers who need to access one or more of the following items:

- Cisco Unified CallManager data
- Cisco Unified CallManager data in XML format
- Cisco Unified CallManager data in a platform-independent manner

This chapter assumes the developer has knowledge of a high-level programming language such as C++, Java, or an equivalent language. Developers must also have knowledge or experience in the following areas:

- TCP/IP Protocol
- [Hypertext Transport Protocol](#)
- Socket programming
- [XML](#)

In addition, users of the AXL API must have a firm grasp of XML Schema, which is used to define the AXL requests, responses, and errors. For more information on XML Schema, refer to <http://www.w3.org/TR/xmlschema-0/>.



Caution

The AXL API allows you to modify the Cisco Unified CallManager system database. AXL acts as a provisioning and configuration API, not as a real-time API. You must use caution when using AXL, because each API call impacts the system. Misuse of the API can lead to dropped calls and slower performance.

New and Changed Information

AXL APIs

The following list provides AXL API calls that are new in Release 5.1:

- addSIPRealm
- updateSIPRealm
- getSIPRealm
- removeSIPRealm

These APIs add and update credentials (passwordreserve) in siprealm.

New Service Parameter

Cisco Unified CallManager Administration 5.1 release adds a new service parameter, “Send Valid Namespace in AXL Response,” under the Cisco Database Layer Monitor service. This parameter determines the namespace that gets sent in the AXL response from Cisco Unified CallManager.

When this parameter specifies True, Cisco Unified CallManager sends the valid namespace (that is, <http://www.cisco.com/AXL/API/1.0>) in the AXL response so the namespace matches the AXL schema specification.

If the parameter specifies False, Cisco Unified CallManager sends an invalid namespace (that is, <http://www.cisco.com/AXL/1.0>) in the AXL response, which does not match the AXL schema specification.

The default service parameter value specifies False to maintain backward compatibility with the AXL response in the Cisco Unified CallManager 5.0 release. Cisco recommends that you set this parameter to True so Cisco Unified CallManager sends the valid namespace.

AXL API

Request methods represent XML structures that are passed to the AXL API server. The server receives the XML structures and executes the request. If the request completes successfully, the appropriate AXL response gets returned. All responses get named identically to the associated requests, except that the word “Response” is appended.

For example, the XML response returned from an addPhone request gets named addPhoneResponse.

If an error occurs, an XML error structure gets returned wrapped inside a SOAP Fault structure (see the “[AXL Error Codes](#)” section on page 36-3).

AXL Compliance

The Cisco Unified CallManager AXL implementation complies with [XML Schema 1.0](#), which was tested for XML Schema compliance with a third-party application that is called XML Spy version 4.x. Early versions of the MSXML schema validator did not support enough of the XML Schema 1.0 recommendation to be used.

The Cisco Unified CallManager AXL implementation also complies with [SOAP 1.1](#) as defined by the World Wide Web Consortium as well as [HTTPS 1.1](#). The AXL API runs as an independent service that can be accessed only via HTTPS.

AXL Error Codes

If an exception occurs on the server, or if any other error occurs during the processing of an AXL request, an error gets returned in the form of a SOAP Fault message:

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
  SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
    <SOAP-ENV:Fault>
      <faultcode>SOAP-ENV:Client</faultcode>
      <faultstring>
        <![CDATA[
          An error occurred during parsing
          Message: End element was missing the character '>'.

          Source = Line : 41, Char : 6
          Code : c00ce55f, Source Text : </re
        ]]>
      </faultstring>
    </SOAP-ENV:Fault>
```

```

    </SOAP-ENV:Body>
  </SOAP-ENV:Envelope>

```

SOAP Fault messages can also contain more detailed information. The following example depicts a detailed SOAP Fault.

```

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
    <SOAP-ENV:Fault>
      <faultcode>SOAP-ENV:Client</faultcode>
      <faultstring>Device not found with name SEP003094C39708.</faultstring>
      <detail xmlns:axl="http://www.cisco.com/AXL/1.0"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://www.cisco.com/AXL/1.0
          http://myhost/CMapi/AXL/V1/axlsoap.xsd">
        <axl:error sequence="1234">
          <code>0</code>
          <message>
<![CDATA[
Device not found with name SEP003094C39708.
]]>
          </message>
        </axl:error>
      </detail>
    </SOAP-ENV:Fault>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

The <detail> element of a SOAP Fault includes error codes. The axl:Error element represents the errors. If a response to a request contains an <error> element, the user agent can determine the cause of the error by looking at the subelements of the <error> tag.

The following list describes the <error> elements:ws The user agent uses the <code> element, a numerical value, to find what type of error occurred. The error codes follow:

Error Code	Description
Less than 5000	These errors directly correspond to DBL Exception error codes. Refer to the documentation for the DBLException class for explanations of these errors.
5000	Unknown Error —An unknown error occurred while the request was processed. This can occur due to a problem on the server but can also be due to errors in the request.
5001	Parser Error —An error occurred while the XML request was being parsed.
5002	Unknown Request Error —The user agent submitted a request that is unknown to the API.
5003	Invalid Value Exception —The API detected an invalid value in the XML request.
5004	AXL Unavailable Exception —This error indicates that the AXL service is too busy to handle the request at this time. The request should be sent again at a later time.

Error Code	Description
5005	Unexpected Node Exception —The server encountered an unexpected element. For example, if the server expects the next node to be <name>, but encounters <protocol>, this error gets returned. Malformed requests that do not adhere to the latest AXL Schema will cause these errors.
5007	Item Not Valid Error —The specified item gets identified as invalid, which means that it does not exist or that it was specified incorrectly at input.

message

The system provides the <message> element so the user agent gets a detailed error message that explains the error.

request

The system provides the <request> element so the user agent can determine the type of request that generated this error. Because this element is optional, it may not always appear.

Example AXL Requests

No platform considerations exist in Cisco Unified CallManager Release 5.1. The client must be able to send an HTTPS request to the AXL endpoint.

The following examples describe how to make an AXL request and read back the response to the request.

Ensure each SOAP request is sent to the web server via an HTTPS POST. The endpoint URL represents the AXL web service that is running on a Cisco CallManager server. The following list contains the only four required HTTPS headers.

- POST :8443/axl/

The first header specifies that this particular POST is intended for the Cisco AXL Web Service. The AXL API only responds to the POST method.

- content-type: text/xml

The second header confirms that the data that is being sent to AXL is XML. If this header is not found, an HTTP 415 error gets returned to the client.

- Authorization: Basic <some Base 64 encoded string>

The third header gives the Base64 encoding of the user name and password for the administrator of the AXL Server. Because Base64 encoding takes three 8-bit bytes and represents them as four printable ASCII characters, if the encoded header does not contain an even multiple of four ASCII characters (16, 20, 24, and so on), you must add padding characters (=) to complete the final group of four as in the following examples.

If authentication of the user fails, an HTTP 401 Access Denied error gets returned to the client.

- content-length: <a positive integer>

The fourth header specifies the length (in bytes) of the AXL request.

**Note**

Currently, the content length cannot exceed 40 kilobytes. If a request is received that is greater than 40 kilobytes, an HTTP 413 error message gets returned.

The following example contains an HTTPS header for an AXL SOAP request:

```
POST :8443/axl
Host: axl.myhost.com:80
Accept: text/*
Authorization: Basic bGFycnk6Y3VybHkgYW5kIG1vZQ==
Content-type: text/xml
Content-length: 613
```

The following AXL request gets used in the code examples that display in the following sections. This example shows a getPhone request:

```
POST :8443/axl
Host: axl.myhost.com:80
Accept: text/*
Authorization: Basic bGFycnk6Y3VybHkgYW5kIG1vZQ==
Content-type: text/xml
Content-length: 613

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">

  <SOAP-ENV:Body>

    <axl:getPhone xmlns:axl="http://www.cisco.com/AXL/1.0"
xsi:schemaLocation="http://www.cisco.com/AXL/1.0 http://ccmserver/schema/axlsoap.xsd"
sequence="1234">
      <phoneName>SEP22222222245</phoneName>
    </axl:getPhone>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

C or C++ Example

This code example uses a hard-coded AXL request and sends it to the AXL Server that is running on the local system (localhost).

It then reads the response and outputs the response to the screen.

```
#include <sys/socket.h>
#include <sys/types.h>
#include <stdlib.h>
#include <openssl/ssl.h>
#include <stdio.h>
#include <unistd.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <strings.h>
#include <openssl/x509.h>
#include <openssl/crypto.h>
#include <iostream>
#include <string>
using namespace std;
typedef unsigned char byte;

void encodeBase64( const string& inBuf, string &outBuf )
{
    unsigned int i;
    unsigned int j;
    bool hiteof = false;
    byte dtable[256];
```

```

outBuf.erase();

for(i= 0;i<9;i++)
{
    dtable[i]= 'A'+i;
    dtable[i+9]= 'J'+i;
    dtable[26+i]= 'a'+i;
    dtable[26+i+9]= 'j'+i;
}
for(i= 0;i<8;i++)
{
    dtable[i+18]= 'S'+i;
    dtable[26+i+18]= 's'+i;
}
for(i= 0;i<10;i++)
{
    dtable[52+i]= '0'+i;
}

dtable[62]= '+';
dtable[63]= '/';

j = 0;
while(!hiteof)
{
    byte igroup[3],ogroup[4];
    int c,n;

    igroup[0]= igroup[1]= igroup[2]= 0;
    for(n= 0;n<3;n++){
        if( j < inBuf.size() )
        {
            c = inBuf[j++];
        } else
        {
            hiteof = true;
            break;
        }
        igroup[n]= (byte)c;
    }
    if(n> 0)
    {
        ogroup[0]= dtable[igroup[0]>>2];
        ogroup[1]= dtable[((igroup[0]&3)<<4) | (igroup[1]>>4)];
        ogroup[2]= dtable[((igroup[1]&0xF)<<2) | (igroup[2]>>6)];
        ogroup[3]= dtable[igroup[2]&0x3F];

        if(n<3)
        {
            ogroup[3]= '=';
            if(n<2)
            {
                ogroup[2]= '=';
            }
        }
        for(i= 0;i<4;i++)
        {
            outBuf += ogroup[i];
        }
    }
}
}

```

```

string getAuthorization()
{
    string m_encode64,name;
    //You should change name to your own axl server user name and passwd
    //in this example,"CCMAdministrator" is user name, "cisco_cisco" is passwd.
    name="CCMAdministrator:cisco_cisco";
    encodeBase64(name,m_encode64);
    return m_encode64;
}

void
BuildDeviceNameSQL(string &buf,    // Buffer to build AXL
                  string& deviceNumber, // DN
                  string& seqNum )
{
    const int BUFSIZE = 2048;
    char buff[BUFSIZE];           // Temp buffer
    string strHTTPHeader;         // HTTP/AXL Header
    string strAXLRequest;         // AXL Request

    strAXLRequest = "<SOAP-ENV:Envelope xmlns:SOAP-ENV=";
    strAXLRequest += "\"http://schemas.xmlsoap.org/soap/envelope/\"";
    strAXLRequest += " xmlns:SOAP-ENC=\"http://schemas.xmlsoap.org/soap/encoding/\"";
    strAXLRequest += " xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\"";
    strAXLRequest += " xmlns:xsd=\"http://www.w3.org/2001/XMLSchema\"> ";
    strAXLRequest += "<SOAP-ENV:Body> ";
    strAXLRequest += "<m:executeSQLQuery xmlns:m=\"http://www.cisco.com/AXL/API/1.0\"";
sequence = "\" + seqNum + "\"> ";
    strAXLRequest += "<m:sql> ";
    strAXLRequest += "SELECT * FROM Device ";
    strAXLRequest += "</m:sql> ";
    strAXLRequest += "</m:executeSQLQuery> ";
    strAXLRequest += "</SOAP-ENV:Body> ";
    strAXLRequest += "</SOAP-ENV:Envelope>";

    strHTTPHeader = "POST /axl/ HTTP/1.1\r\n";

    strHTTPHeader += "Host: localhost:8443\r\n";
    strHTTPHeader += "Accept: text/*\r\n";
    //strHTTPHeader += "Authorization: Basic YWRtaW5pc3RyYXRvcjpwjaXNjbw== \r\n";

    strHTTPHeader += "Authorization: Basic ";
    strHTTPHeader += getAuthorization() + "\r\n";

    strHTTPHeader += "Content-type: text/xml\r\n";
    strHTTPHeader += "Content-length: ";

    // temporarily use the buffer to store the length of the request
    sprintf( buff, "%d", strAXLRequest.length() );

    strHTTPHeader += buff;
    strHTTPHeader += "\r\nConnection: Keep-Alive";
    strHTTPHeader += "\r\n\r\n";

    // put the HTTP header and SOAP XML together
    buf = strHTTPHeader + strAXLRequest;

    return;
}

```

```

int main(int argc, char** argv)
{
    struct sockaddr_in saddr;
    SSL_METHOD *meth;
    SSL_CTX *sslctx;
    SSL *ssl;
    X509* server_cert;
    string buff,line,seqnum;
    char buffer[2048];
    int status,error;
    char *str;

    if( argc!=3 )
    {
        printf("Usage : ssltest <ip> <port> \n");
        printf("Usage : the default port is 8443 \n");
        printf("Usage : the ip is the ip of ccm5.0 \n");
        printf("Example: ssltest 10.77.31.168 8443 \n");

        exit(2);
    }

    int sock=socket(AF_INET,SOCK_STREAM,IPPROTO_TCP);
    if(sock<0)
    {
        printf("create socket failed\n");
        exit(1);
    }
    saddr.sin_family=AF_INET;
    saddr.sin_port=htons(atoi(argv[2]));
    saddr.sin_addr.s_addr =inet_addr(argv[1]);
    status=connect(sock,(struct sockaddr *)&saddr,sizeof(saddr));
    if(status<0)
    {
        printf("connect to %s failed\n",argv[1]);
        exit(2);
    }
    SSL_library_init();
    meth=TLSv1_client_method();
    sslctx=SSL_CTX_new(meth);
    if(!sslctx)
    {
        printf("SSL_CTX_new failed\n");
        close(sock);
        exit(3);
    }
    SSL_CTX_set_verify(sslctx,SSL_VERIFY_NONE,NULL);
    ssl =SSL_new(sslctx);
    if(!ssl)
    {
        printf("SSL_new failed\n");
        close(sock);
        exit(4);
    }
    status=SSL_set_fd(ssl,sock);
    if(!status)
    {
        printf("SSL_set_fd failed\n");
        close(sock);
        exit(5);
    }
    SSL_set_mode(ssl,SSL_MODE_AUTO_RETRY);
    status=SSL_connect(ssl);
    error=SSL_get_error(ssl,status);

```

```

switch(error)
{
    case SSL_ERROR_NONE:
        printf("connect successful\n");
        break;
    case SSL_ERROR_ZERO_RETURN:
        printf("peer close ssl connection \n");
        break;
    default:
        printf("connect error is %d\n",error);
}

server_cert = SSL_get_peer_certificate (ssl);
if(!server_cert)
{
    printf("get server certificate failed!\n");
    SSL_shutdown(ssl);
    close(sock);
    exit(6);
}
str= X509_NAME_oneline(X509_get_subject_name (server_cert),0,0);
if(str)
{
    printf("subject :%s\n",str);
}
else
    printf("subject is empty\n");
str = X509_NAME_oneline (X509_get_issuer_name (server_cert),0,0);
if(!str)
    printf("issuer name is :%s\n",str);
else
    printf("issuer name is empty \n");
line="12";
seqnum="1234";
BuildDeviceNameSQL(buff,line,seqnum);
SSL_write(ssl,buff.c_str(),buff.length());
printf("\n");
printf("\n");
printf("Request sent is:\n");
printf(buff.c_str());
printf("\n");
printf("\n");
SSL_read(ssl,buffer,sizeof(buffer));

printf("Response from server is: \n%s\n",buffer);
status=SSL_shutdown(ssl);
if(status==1)
    printf("shutdown successful\n");
else
    printf("\nshutdown error code is %d\n",status);
close(sock);
}

```

Java Example

This code example uses a hard-coded AXL request and sends it to the AXL server that is running on the local system (localhost). It then reads the response and outputs the response to the screen.

```

import java.io.*;
import java.net.*;

public class main

```



```

{
public static void main(String[] args)
{
    //Declare references
    String sAXLSOAPRequest = null;    // will hold the complete request,
                                      // HTTPS header and SOAP payload
    String sAXLRequest = null;        // will hold only the SOAP payload
    Socket socket = null;             // socket to AXL server
    OutputStream out = null;          // output stream to server
    InputStream in = null;            // input stream from server
    byte[] bArray = null;             // buffer for reading response from server

    // Build the HTTPS Header
    sAXLSOAPRequest = "POST :8443/axl\r\n";
    sAXLSOAPRequest += "Host: localhost:80\r\n";
    sAXLSOAPRequest += "Authorization: Basic bGFycnk6Y3VybHkgYW5kIGlvZQ==\r\n";
    sAXLSOAPRequest += "Accept: text/*\r\n";
    sAXLSOAPRequest += "Content-type: text/xml\r\n";
    sAXLSOAPRequest += "Content-length: ";

    // Build the SOAP payload
    sAXLRequest = "<SOAP-ENV:Envelope
xmlns:SOAP-ENV=\"http://schemas.xmlsoap.org/soap/envelope/\" ";
    sAXLRequest += "xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\"
xmlns:xsd=\"http://www.w3.org/2001/XMLSchema\"> ";
    sAXLRequest += "<SOAP-ENV:Body> <axl:getPhone
xmlns:axl=\"http://www.cisco.com/AXL/1.0\" ";
    sAXLRequest += " xsi:schemaLocation=\"http://www.cisco.com/AXL/1.0
http://ccmserver/schema/axlsoap.xsd\" ";
    sAXLRequest += "sequence=\"1234\"> <phoneName>SEP22222222245</phoneName> ";
    sAXLRequest += "</axl:getPhone> </SOAP-ENV:Body> </SOAP-ENV:Envelope>";

    // finish the HTTPS Header
    sAXLSOAPRequest += sAXLRequest.length();
    sAXLSOAPRequest += "\r\n\r\n";

    // now add the SOAP payload to the HTTPS header, which completes the AXL SOAP request
    sAXLSOAPRequest += sAXLRequest;

    // now that the message has been built, we can connect to server and send it
    try
    {
        socket = new Socket("localhost", 80);
        out = socket.getOutputStream();
        in = socket.getInputStream();

        // send the request to the host
        out.write(sAXLSOAPRequest.getBytes());

        // read the response from the host
        StringBuffer sb = new StringBuffer(2048);
        bArray = new byte[2048];
        int ch = 0;
        int sum = 0;
        while ( (ch = in.read(bArray)) != -1 )
        {
            sum += ch;
            sb.append(new String(bArray, 0, ch));
        }

        socket.close();

        // output the response to the standard out
        System.out.println(sb.toString());
    }
}

```

```

    } catch (UnknownHostException e)
    {
        System.err.println("Error connecting to host: " + e.getMessage());
        return;
    } catch (IOException ioe)
    {
        System.err.println("Error sending/receiving from server: " +
ioe.getMessage());

        // close the socket
        try
        {
            if (socket != null) socket.close();
        } catch (Exception exc)
        {
            System.err.println("Error closing connection to server: " +
exc.getMessage());
        }
        return;
    }
}

```

In addition to these examples, refer to the AXL Sql Toolkit, which is available for download from the Cisco Unified CallManager server at <https://ccmsvr:8443/plugins/axlsqtoolkit.zip>.

Throttling of Requests

The side effects of updating the Cisco Unified CallManager database can adversely affect system performance; therefore, the system administrator can control how many AXL requests are allowed to update the database per minute. You can control this value by using the Database Layer service parameter “MaxAXLWritesPerMinute.”

AXL accommodates all requests until the “MaxAXLWritesPerMinute” value is reached. Subsequent attempts to modify the database with AXL are rejected with an HTTPS 503 Service Unavailable response. Every minute, AXL resets its internal counter and begins to accept AXL update requests until the limit gets reached again.

The following AXL requests, which are considered “Reads,” do not count against the “MaxAXLWritesPerMinute” service parameter. All other AXL requests that are not in the following list count against the service parameter:

- executeSQLQuery
- doDeviceReset
- all AXL “get” requests
- all AXL “list” requests

The AXL Schema Documentation

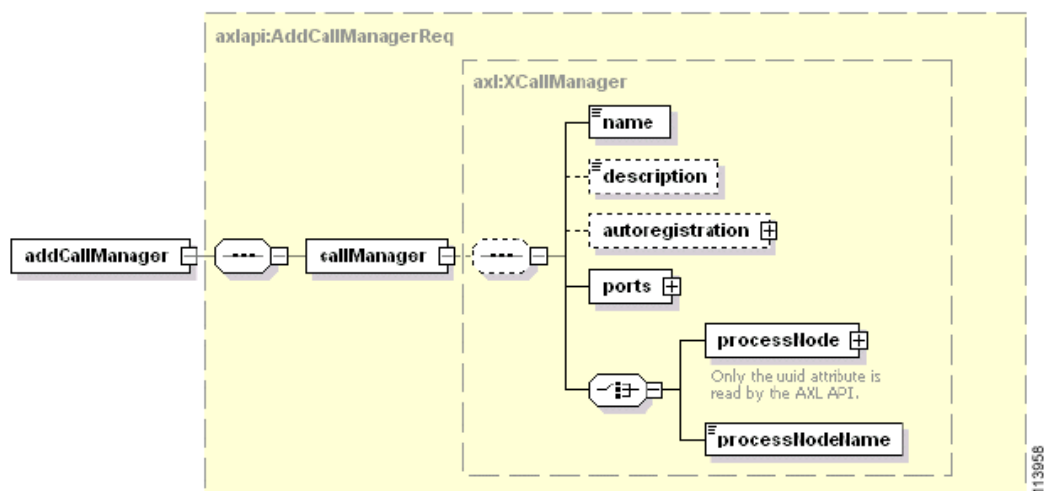
The axlsqtoolkit.zip plugin contains the following six AXL schema files: AXLAPI.wsdl, AXLEnums.xsd, axlmessage.xsd, axlsoap.xsd, axl.xsd, and SoapEnvelope.xsd. These files encapsulate the complete AXL schema (including details of all requests, responses, XML objects, data types, and so on).

The Cisco developer support program also provides the AXL schema files at http://www.cisco.com/pcgi-bin/dev_support/access_level/product_support.

Standard XML handling IDEs and development environments can illuminate or auto-generate 'friendly' formatted documents based on the AXL schema files.

The following example describes a complete auto-generated HTML document based on the schema.

Example XML Structure



The AXL schema, which is provided as an HTML document, graphically describes each request and response. (See http://www.cisco.com/pcgi-bin/dev_support/access_level/product_support.)

The following legend explains the graphics that are used in the AXL schema document.

Request or Response	Element Name	Description
	Complex Element	A complex element can have child elements, as well as attributes. An element with a solid border must appear in an XML instance document.
	Simple Element	A simple element cannot have child elements but can have attributes. An element with a solid border must appear in an XML instance document.
	Optional Element	An optional element need not appear in an instance of the XML. Any type of element can be optional, including sequence and choice elements.

Request or Response	Element Name	Description
	Sequence Element	A sequence element means that all children of this element must appear in the XML in the order in which they are listed.
	Choice Element	A choice element means that only one child of this element can appear in the XML.

Authentication

Deactivate anonymous access to the AXL SOAP service to enforce user authentication. User authentication gets controlled via the HTTPS Basic Authentication scheme; therefore, you must include the Authorization header in the HTTPS header.

For example, if the user agent wants to send the userid “larry” and password “curly and moe”, it would use the following header field:

Authorization: Basic bGFycnk6Y3VybHkgYW5kIG1vZQ==

where the string “bGFycnk6Y3VybHkgYW5kIG1vZQ==” provides the Base64 encoding of “larry:curly and moe.”



Note

The two “equals” characters (=) at the end of the string act as padding characters for Base64 encoding.

Data Encryption

Encrypt AXL SOAP messages by using HTTP SSL. SSL remains functional on the web server by default. AXL requests get made by using the “https” protocol.

Integration Considerations and Interoperability

The AXL API gives much power to developers to modify the Cisco Unified CallManager system database. The developer must use caution when using AXL, because each API call impacts the system. Abuse of the API can lead to dropped calls and slower system performance. AXL acts as a provisioning and configuration API, not as a real-time API.

If AXL is determined to be using too much CPU time, consider lowering the MaxAXLWritesPerMinute service parameter. If this does not solve the problem, consider purchasing a second server to be used only by applications that are using AXL.



Note

Because AXL is not a real-time API, the autologout function of Extension Mobility does not work when the user is logged in/out of EM via the AXL interface.



WebDialer API Programming

This chapter describes the Simple Object Access Protocol (SOAP) and HTML over secure HTTP (HTTPS) interfaces that are used to develop customized directory search applications for Cisco Unified CallManager WebDialer Version 1.2 and contains the following sections:

- [Definitions, page 37-1](#)
- [Overview, page 37-2](#)
- [Call Flows, page 37-6](#)
- [Interfaces, page 37-9](#)
- [Cisco WebDialer WSDL, page 37-16](#)
- [Sample JavaScript, page 37-19](#)

Definitions

Cisco WebDialer Server	A server that hosts the Cisco Unified CallManager WebDialer application
Cisco WebDialer Application	The software that is installed on a Cisco Unified CallManager server. It enables the click-to-dial functionality by creating hyperlinked telephone numbers in a company directory. This functionality allows users to make calls from the web page by clicking the telephone number of the person that they are trying to call. The Cisco Unified CallManager WebDialer application comprises two Java servlets, the WebDialer servlet and the Redirector servlet.
WebDialer Servlet	A Java servlet that allows Cisco Unified CallManager users in a specific cluster to make and end calls, as well as to access their phone and line configuration.
Redirector Servlet	A Java servlet that finds the Cisco Unified CallManager cluster for a request that a Cisco WebDialer user makes. It redirects that request to the specific Cisco WebDialer server that is located in that user Cisco Unified CallManager cluster.

Overview

Cisco Unified CallManager WebDialer, which is installed on a Cisco Unified CallManager server and used in conjunction with Cisco Unified CallManager, allows Cisco Unified IP Phone users to make calls from web and desktop applications. For example, Cisco Unified CallManager WebDialer uses hyperlinked telephone numbers in a company directory to allow users to make calls from a web page by clicking the telephone number of the person that they are trying to call.

The two main components of Cisco Unified CallManager WebDialer comprise the WebDialer Servlet and the Redirector Servlet.

WebDialer Servlet

The WebDialer servlet, a Java servlet, allows Cisco Unified CallManager users in a specific cluster to make and end calls, as well as to access their phone and line configuration.

Cisco WebDialer applications interact with the WebDialer servlet through two interfaces:

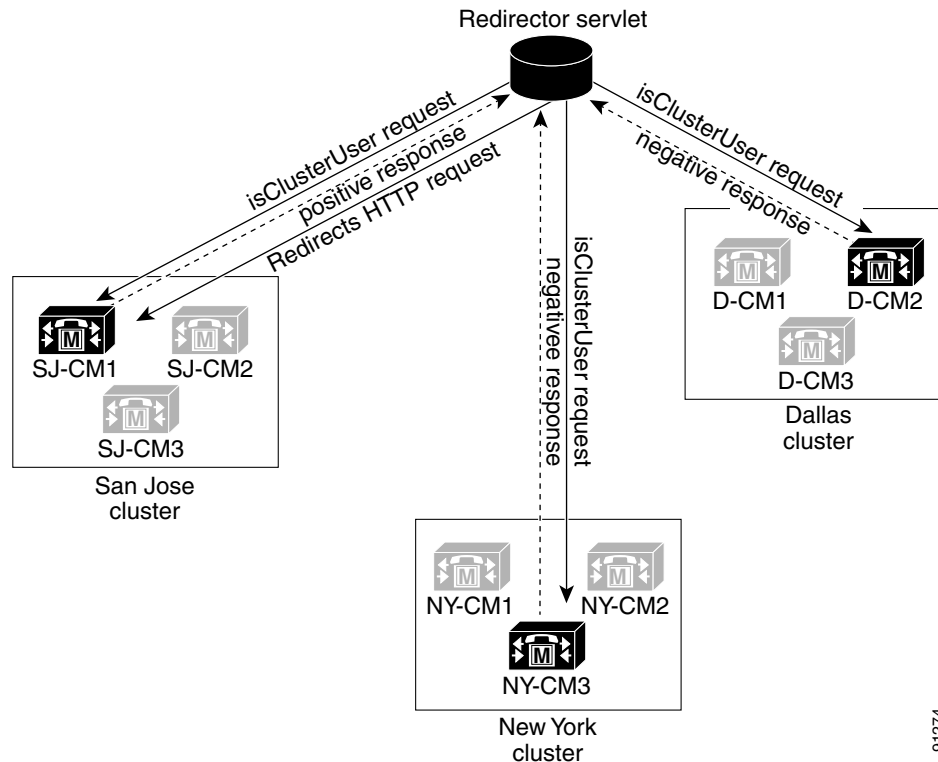
- **SOAP over HTTPS**—This interface that is based on the Simple Object Access Protocol (SOAP) gets used to develop desktop applications such as Microsoft Outlook Add-in and SameTime Client Plug-in. Developers can use the `isClusterUserSoap` interface to design multicenter applications that require functionality similar to a Redirector servlet.
- **HTML over HTTPS**—This interface that is based on the HTTPS protocol gets used to develop web-based applications such as the Cisco Unified CallManager directory search page (`directory.asp`). Developers who use this interface can use the Redirector servlet for designing multicenter applications.

Redirector Servlet

The Redirector servlet, a Java-based servlet, finds the Cisco Unified CallManager cluster for a request that a Cisco WebDialer user makes. It redirects that request to the specific Cisco WebDialer server that is located in that user's Cisco Unified CallManager cluster. Availability of the Redirector servlet occurs only for multicenter applications and only for applications that are developed by using HTML over HTTPS interfaces.

[Figure 37-1](#) illustrates how a Redirector servlet redirects a call in a multicenter environment.

Figure 37-1 Multiple Clusters



Example of Cisco Unified CallManager WebDialer Using the Redirector Servlet

For example, consider three clusters, each one in a single city such as San Jose, Dallas, and New York. Each cluster contains three Cisco Unified CallManager servers with WebDialer servlets that have been configured for Cisco Unified CallManager servers SJ-CM1, D-CM2, and NY-CM3.

The system administrator configures the WebDialer servlets on any Cisco Unified CallManager server by entering the IP address of that specific Cisco Unified CallManager server in the *wdservers* service parameter.

For information on configuring WebDialer and Redirector servlets, refer to the “Cisco WebDialer” chapter in the *Cisco Unified CallManager Features and Services Guide, Release 5.0*.

When a user who is located in San Jose clicks a telephone number in the corporate directory search page that is enabled by Cisco Unified CallManager WebDialer, the following actions happen:

1. The Cisco Unified CallManager server sends an initial *makeCall* HTTPS request to the Redirector servlet.
2. If this request is received for the first time, the Redirector servlet reads the Cisco Unified CallManager WebDialer server cookie and finds it empty.

For a repeat request, the Redirector servlet reads the IP address of the Cisco Unified CallManager WebDialer server that previously serviced the client and sends a *isClusterUser* HTTPS request only to that server.

3. The Redirector servlet sends back a response that asks for information, which results in the authentication dialog box opening for the user.
4. The user enters the Cisco Unified CallManager user ID and password and clicks the **Submit** button.

5. The Redirector servlet reads only the user identification from this information and sends a *isClusterUser* HTTPS request to each Cisco Unified CallManager WebDialer server that the system administrator configured.

Figure 37-1 illustrates how this request is sent to the WebDialer servlets that have been configured for SJ-CM1, D-CM2, and NY-CM3. Depending on the geographical location of the calling party, the WebDialer servlet from the cluster that represents that location responds positively to the Redirector servlet. The remaining WebDialer servlets that were contacted return a negative response. The WebDialer servlet SJ-CM1 responds positively to the request because the calling party is located in San Jose (SJ-CM).

The Redirector servlet redirects the original request from the user to SJ-CM1 and sets a cookie on the user browser for future use.

Changes in Release 5.1

Cisco Unified CallManager Release 5.1 includes the following change to Cisco Unified CallManager WebDialer:

- WebDialer and Redirector now require HTTPS.

Developers should format Redirector and WebDialer requests to use HTTPS. Cisco Unified CallManager requires the secured protocol to prevent unauthorized applications from reading user data.

Refer to the *Cisco Unified CallManager Developers Guide for Release 5.0* for important changes to WebDialer API programming in the 5.0 release.

Cisco WebDialer Security Support

Cisco WebDialer supports secure connections to CTI (TLS connection). For this feature, Cisco WebDialer uses the security API that JTAPI provides. Refer to the *Cisco Unified CallManager JTAPI Developers Guide* for the JTAPI API. WebDialer uses the Application User, “WDSysUser”, for obtaining the CTI connection.

You must complete the following configuration before WebDialer can be configured to open a CTI connection in secure mode.

-
- Step 1** Activate the Cisco CTL Provider service in Cisco Unified CallManager Service Administration.
 - Step 2** Activate the Cisco Certificate Authority Proxy Function Service.
 - Step 3** Download the Cisco CTL Client from the Application plug-in and install it on any machine.
 - Step 4** Run the CTL Client, choose the option to “enable Cluster Security,” and follow the instructions that display. This requires USB E-tokens.
 - Step 5** To verify that cluster security is enabled, go to Cisco Unified CallManager Administration and look at [System-> Enterprise Parameter configuration]. Look at the Security Parameters; the cluster security should be set to 1.
 - Step 6** In Cisco Unified CallManager Administration page, from the User Management drop-down menu, select the Application User CAPF Profile option.
 - Step 7** Click Add new InstanceID.
 - Step 8** In the CAPF Profile configuration window, set up an InstanceID and CAPF profile for the InstanceID for the Application User WDSysUser.
 - a. **InstanceID:** Enter the value of instance ID, for example, 001.

- b. **Certificate Operation:** Select Install/Upgrade from the drop-down menu.
- c. **Authentication Mode:** Select By Authorization String from the drop-down menu.
- d. **Authorization String:** Enter the value of authorization string, for example, 12345.
- e. **Key Size:** Select key size from drop-down menu, for example, 1024.
- f. **Operation Completes By:** Enter the date and time in following format yyyy:mm:dd:hh:mn where yyyy=year, mm=month, dd=date, hh=hour, mn=minutes, such as 2006:07:30:12:30.



Note If this date and time is past, the certificate update operation will fail.

- g. Ignore the **Packet Capture Mode**, **Packet Capture Duration**, and **Certificate** fields.
- h. **Certificate Status:** Select Operation pending from the drop-down menu.
If anything else is selected, the certificate update will fail.

Security Service Parameters

Cisco WebDialer includes two mode-specific service parameters for CTI connection security.

- **CTI Manager Connection Security Flag**—This required service parameter indicates whether security for the Cisco Unified CallManager WebDialer service CTI Manager connection is enabled or disabled.

If enabled (true), Cisco WebDialer will open a secure connection to CTI Manager by using the Application CAPF profile that is configured for the instance ID (as configured in CTI Manager Connection Instance ID service parameter) for Application user WDSysUser. The default value specifies false.

- **Application CAPF Profile Instance ID:** This service parameter specifies the Instance ID of the Application CAPF Profile for Application User WDSysUser that this Cisco Unified CallManager WebDialer server will use to open a secure connection to CTI Manager. You must configure this parameter if the CTI Manager Connection Security Flag parameter is enabled (true).
- **Algorithm:**
 1. Read the service parameters.
 2. Get the node IP/name of the nodes where TFTP and CAPF are activated.
 3. For the instanceID (input in service parameters), if the Certificate Operation is 'Install/Upgrade' or 'Delete', delete the current certificates, if any.
 4. If the Certificate Operation is not 'Install/Upgrade' or 'Delete', and a current certificate exists, use this certificate.
 5. If no certificate is present, request one by using JTAPI API setSecurityPropertyForInstance; this will need username, instanceID, authCode, tftpServerName, tftpPort, capfServerName, capfPort, certPath, and securityFlag. This call will contact the TFTP server, download the certificate, contact the CAPF server, verify the CTL file, and request the client and server certificates.
 6. If Step 5 is successful, set the following items on the ICCNProvider and call `open().provider.setInstanceID(instanceID);provider.setTFTPSTServer(tftpServerName);provider.setCAPFServer(capfServerName);provider.setCertificatePath(certPath);provider.setSecurityOptions(securityFlag);`
 7. If Step 5 fails, throw `initFailedException`. You can see this in the WebDialer traces.

Install Changes

Cisco WebDialer rpm creates a new directory “/usr/local/cm/wd/wd-certificates/” and sets permissions for users on this directory, which is used to store the certificates.

Files Changed: /vob/ccm/Projects/CMApplServices/rpm/cm-webdialer.spec

SIP Phone Support in Cisco WebDialer

Cisco WebDialer supports SIP phones in this release. CTI only supports the new SIP phones and not the existing SIP phones, so the same support is extended by Cisco WebDialer. JTAPI provides the APIs that are used to distinguish between these two kinds of phones and to hide the unsupported phones from the user in the Cisco WebDialer preferences window.

Call Flows

The call flows in this section describe the flow of events for client and browser-based applications that use Cisco Unified CallManager WebDialer, which should help you design customized applications for Cisco WebDialer.

Desktop-based Client Application Call Flow

[Figure 37-2](#) shows the call flow for an outgoing call from a client application such as Microsoft Outlook Plug-in to a WebDialer servlet. The user clicks the **Dial** or **Make Call** button in the address book of the client application. If the user is making a call for the first time, the application does not have authentication or configuration information on the user.

If the user makes a call for the first time,

1. The client sends a makeCallSoap request to the configured WebDialer servlet.
2. The WebDialer servlet attempts to authenticate the user. [Figure 37-2](#) shows an authentication failure that occurred because the authentication information is incomplete or does not exist.
3. The WebDialer servlet sends an authentication failure response to the client application.
4. The client application displays a dialog box on the computer screen of the user that asks for the user ID and password. The user enters this information and clicks the **submit** button. The user ID and password now gets stored for future invocations of the application.
5. The application sends a repeat SOAP request to the WebDialer servlet. The request contains credential information on the user.
6. The WebDialer servlet authenticates the user.
7. The WebDialer servlet reads any missing configuration information in the request.
8. The WebDialer servlet returns a configuration error message to the client application.
9. The client application sends a getConfigSoap request to the WebDialer servlet.
10. The WebDialer servlet responds with the user configuration information that is stored in the directory.
11. The client application displays a configuration dialog box on the user computer screen that asks the user to select or update the configuration. The user enters the information and clicks the **submit** button. The user configuration information now gets stored for future invocations of the application.

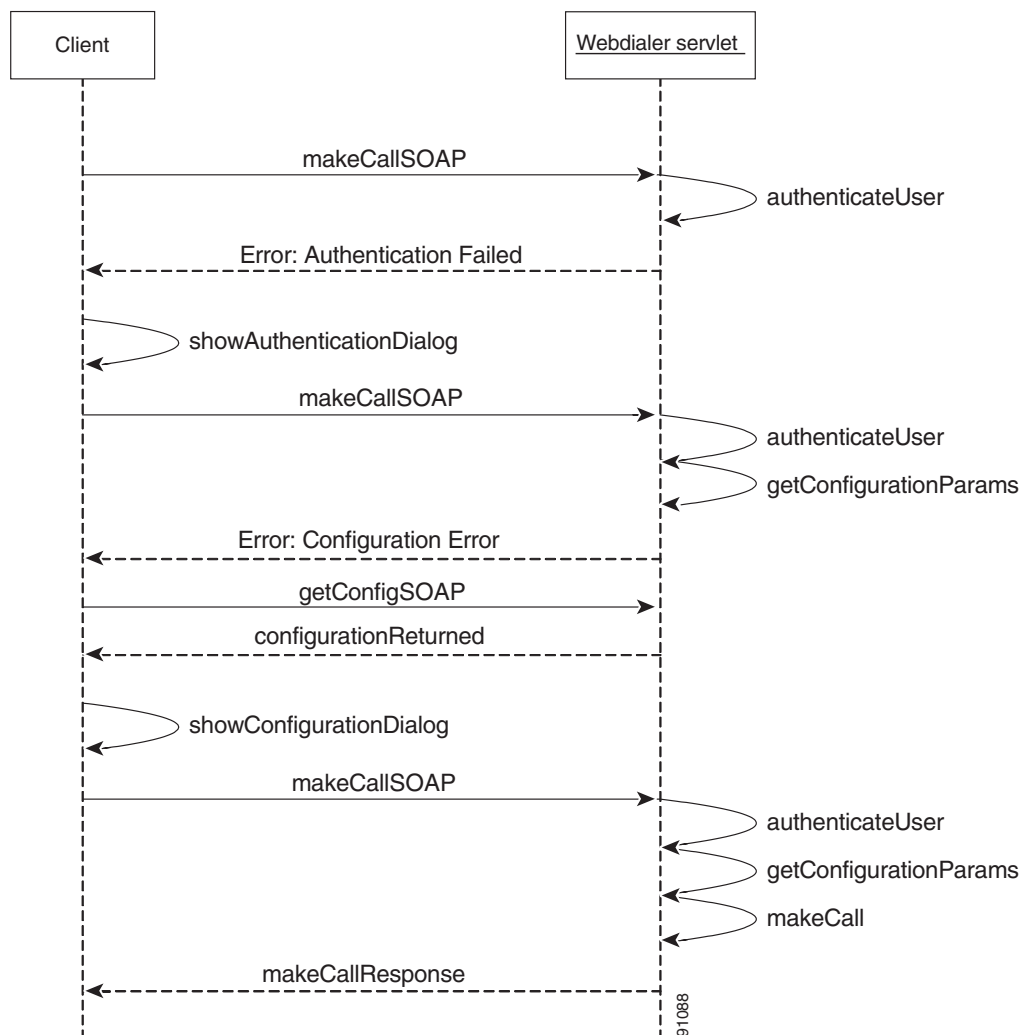
12. The client resends the makeCallSoap request to the WebDialer servlet. This request contains the user configuration information.
13. The WebDialer servlet authenticates the user and dials the telephone number by using the information that the makeCallSoap request contains. It responds to the client with a success or failure message.

**Note**

The call flow goes directly to step 12:

- If the credential and configuration information is already stored when the application is installed.
- For all subsequent requests that the user makes.

Figure 37-2 Cisco Unified CallManager WebDialer Call Flow for a Client-Based Application

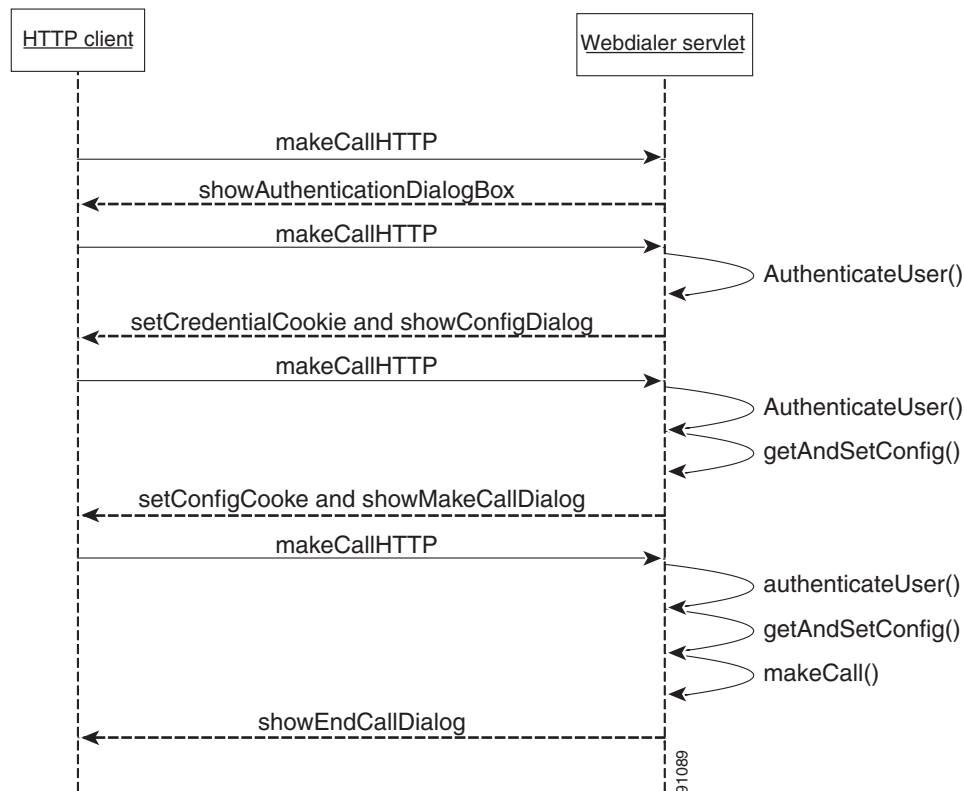


Browser-Based Application Call Flow

Figure 37-3 shows the call flow for an HTTP-based browser application such as a directory search page, personal address book, or the Cisco Unified CallManager directory search page (directory.asp).

The user clicks the **Dial** or **Make Call** button in the address book of the client application. If the user is making a call for the first time, the application does not have authentication or configuration information on the user.

Figure 37-3 Cisco Unified CallManager WebDialer Call Flow for a Browser-Based Application



If the user makes a call for the first time:

1. The client sends a makeCall HTTPS request to the configured WebDialer servlet. The query string contains the number to be called.
2. The WebDialer servlet authenticates the user. Authentication fails because the authentication information is incomplete or does not exist.



Note Authentication succeeds if the user credentials are sent with the request, and the call flow goes directly to number seven.

3. The WebDialer servlet sends an authentication dialog to the client browser for user authentication.
4. The user enters the user ID and password and clicks the **Submit** button.
5. The client sends a makeCallHTTPS request that contains the user credentials to the WebDialer servlet.
6. The WebDialer servlet authenticates the user.
7. The WebDialer servlet reads the configuration information in the cookie that is sent with the request.
8. Assuming that the request is made for the first time, the servlet sends a response that contains a cookie to the client browser. The cookie that contains the client credentials gets stored on the client browser. The client credentials comprise user ID, IP address, and the time of the request.

9. The user enters the updates in the configuration dialog box and clicks the **Submit** button.
10. The client browser sends a makeCall HTTPS request to the WebDialer servlet. The request contains a cookie with the credential and configuration information in parameter form.
11. The WebDialer servlet uses the credentials to authenticate the user and saves the configuration information in its memory.
12. The WebDialer servlet sends a makeCall confirmation dialog to the client browser with the configuration information that is stored in a cookie. The cookie gets stored on the client browser for future invocations.
13. The Make Call dialog box appears on the user computer screen. The user clicks the **Dial** button, which sends another makeCall HTTPS request to the WebDialer servlet.
14. The WebDialer servlet authenticates the user by using the credentials in the cookie, retrieves the configuration information from the cookie, and makes the call.
15. The servlet responds by sending an endCall confirmation dialog to the user to end the call. The End Call dialog box appears on the user computer screen and stays there for the time interval that is configured in the service parameters.

For all subsequent requests, the call flow starts at number 12 and ends at number 15.

Interfaces

Cisco Unified CallManager WebDialer applications interact with the WebDialer servlet through two interfaces:

- **SOAP over HTTPS** — This interface, which is based on the Simple Object Access Protocol (SOAP), gets used to develop desktop applications such as Microsoft Outlook Add-in and SameTime Client Plug-in. Developers can use the isClusterUserSoap interface to design multicloud applications that require functionality similar to a Redirector servlet.
- **HTML over HTTPS** — This interface, which is based on the HTTPS protocol, gets used to develop web-based applications such as the Cisco Unified CallManager directory search page (directory.asp). Developers who are using this interface can use the Redirector servlet for designing multicloud applications.



Note

The following files must be run to properly set the ENV variable and Java classes:
installWDSservice.bat
installWDSOAP.bat

SOAP over HTTPS Interface

To access the SOAP interfaces for Cisco Unified CallManager WebDialer, use the Cisco Unified CallManager WebDialer Web Service Definition Language (WSDL) in the [“Cisco WebDialer WSDL” section on page 37-16](#).

makeCallSoap

You access the makeCallSoap interface by initiating a SOAP request to the URL `https://CCM-IP:8080/webdialer/services/WebdialerSoapService` where CCM-IP specifies the IP address of the Cisco Unified CallManager server where Cisco WebDialer is configured.

Parameter	Mandatory	Description	Data Type	Range Values	Default Value
Destination	Mandatory	Standard canonical form. For example, +1 408 5551212 or extensions such as 2222.	String	None	None
Credential	Mandatory	The user ID or password of the user or proxy user. For more information on creating a proxy user, see the <i>Cisco WebDialer</i> chapter in the <i>Cisco Unified CallManager Features and Services Guide, Release 5.0</i> .	Refer to the credential data type in the “ Cisco WebDialer WSDL ” section on page 37-16.	None	None
Profile	Mandatory	The profile that is used to make a call. A typical profile is a calling device such as an IP phone or line.	Refer to the profile data type in the “ Cisco WebDialer WSDL ” section on page 37-16.	None	None

Results

Refer to the “[Cisco WebDialer WSDL](#)” section on page 37-16 for return values and their data type.

Error Code	Name	Type	Description	Action by application
0	responseCode	Integer	Success	Displays a dialog box.
	responseDescription	String	Success	
1	responseCode	Integer	Call failure error	Displays a relevant error message.
	responseDescription	String	Call failure error	
2	responseCode	Integer	Authentication error	Displays the authentication dialog where the user enters ID and password information.
	responseDescription	String	User authentication error	
3	responseCode	Integer	No authentication proxy rights	Void for user-based applications.
	responseDescription	String	No authentication proxy rights	
4	responseCode	Integer	Directory error	Displays an appropriate directory error message.
	responseDescription	String	Directory error	
5	responseCode	Integer	No device is configured for the user or missing parameters exist in the request.	The application initiates a getConfigSOAP request and displays the selected device and line to the user.
	responseDescription	String	No device is configured for the user or missing parameters exist in the request.	

Error Code	Name	Type	Description	Action by application
6	responseCode	Integer	Service temporarily unavailable	Displays the appropriate error dialog with an option to try again.
	responseDescription	String	Service temporarily unavailable	
7	responseCode	Integer	Destination cannot be reached.	Displays the appropriate error dialog that allows the user to edit the dialed number.
	responseDescription	String	Destination cannot be reached.	
8	responseCode	Integer	Service error	Displays the appropriate error dialog.
	responseDescription	String	Service error	
9	responseCode	Integer	Service overloaded	Displays the appropriate error dialog with an option to try again.
	responseDescription	String	Service overloaded	

endCallSoap

You access the endCallSoap interface by initiating a SOAP request to the URL <https://CCM-IP:8080/webdialer/services/WebdialerSoapService> where CCM_IP specifies the IP address of the Cisco Unified CallManager server where Cisco WebDialer is configured.

Parameter	Mandatory	Description	Data Type	Range Values	Default Value
Credential	Mandatory	The user ID or password of the user or proxy user. For information on creating a proxy user, see the <i>Cisco WebDialer</i> chapter in the <i>Cisco Unified CallManager Features and Services Guide, Release 5.0</i> .	Refer to the credential data type in “ Cisco WebDialer WSDL ” section on page 37-16.	None	None
Profile	Mandatory	The profile that is used to make a call. A typical profile is a calling device such as an IP phone or line.	Refer to the profile data type in the “ Cisco WebDialer WSDL ” section on page 37-16.	None	None

Refer to the “[Cisco WebDialer WSDL](#)” section on page 37-16 for return values and their data type.

Error Code	Name	Type	Description	Action by application
0	responseCode	Integer	Success	Displays a dialog box on the computer screen.
	responseDescription	String	Success	
1	responseCode	Integer	Call failure error	Displays a relevant error message.
	responseDescription	String	Call failure error	
2	responseCode	Integer	Authentication error	Displays authentication dialog for user to enter user ID and password.
	responseDescription	String	User authentication error	
3	responseCode	Integer	No authentication proxy rights	Void for user-based applications.
	responseDescription	String	No authentication proxy rights	
4	responseCode	Integer	Directory error	Displays an appropriate directory error message.
	responseDescription	String	Directory error	
5	responseCode	Integer	No device is configured for the user or missing parameters exist in the request.	The Application initiates a getConfigSOAP request and displays the selected device and line to the user.
	responseDescription	String	No device is configured for the user or missing parameters exist in the request.	
6	responseCode	Integer	Service temporarily unavailable	Displays the appropriate error dialog with an option to try again.
	responseDescription	String	Service temporarily unavailable	
7	responseCode	Integer	Destination cannot be reached.	Displays the appropriate error dialog that allows the user to edit the dialed number.
	responseDescription	String	Destination cannot be reached.	
8	responseCode	Integer	Service error	Displays appropriate error dialog.
	responseDescription	String	Service error	
9	responseCode	Integer	Service overloaded	Displays the appropriate error dialog with an option to try again.
	responseDescription	String	Service overloaded	

getProfileSoap

You access the getProfileSoap interface, which is used by plug-in based clients, by initiating a SOAP request to the URL `https://CCM-IP:8080/webdialer/services/WebdialerSoapService` where CCM-IP specifies the IP address of the Cisco Unified CallManager server where Cisco WebDialer is configured.

Parameter	Mandatory/ Optional	Description	Data Type	Value Range	Default Value
Credential	Mandatory	User ID or password of the user or proxy user. For information on creating a proxy user, see the <i>Cisco WebDialer</i> chapter in <i>Cisco Unified CallManager Features and Services Guide, Release 5.0</i> .	Refer to the credential data type in the “Cisco WebDialer WSDL” section on page 37-16.	None	None
UserID	Mandatory	The user ID for which the configuration is requested.	String	None	None

Refer to the [“Cisco WebDialer WSDL”](#) section on page 37-16 for return values and their data type.

Error Code	Name	Type	Description	Action by plug-in application
0	responseCode	Integer	Returns an array of phones or lines on the phone that is associated with the user. Refer to the Cisco Unified CallManager WebDialer WSDL for the WDDeviceInfo data type.	Displays a dialog box on the computer screen.
	responseDescription	String	Success	
	deviceInfoList	Array	Returns an array of the the WDDeviceInfo data type	
1	responseCode	Integer	No device configured for the user	Displays an appropriate error message.
	responseDescription	String	No device configured for the user	
2	responseCode	Integer	Authentication error	Displays the authentication dialog where the user enters ID and password information.
	responseDescription	String	User authentication error	
3	responseCode	Integer	No authentication proxy rights	Void for user-based applications.
	responseDescription	String	No authentication proxy rights	

Error Code	Name	Type	Description	Action by plug-in application
4	responseCode	Integer	Directory error	Displays an appropriate directory error message.
	responseDescription	String	Directory error	
6	responseCode	Integer	Service temporarily unavailable	Displays the appropriate error dialog with an option to try again.
	responseDescription	String	Service temporarily unavailable	
9	responseCode	Integer	Service overloaded	Displays the appropriate error dialog with an option to try again.
	responseDescription	String	Service overloaded	

isClusterUserSoap

You access the isClusterUserSoap interface by initiating a SOAP request to the URL <https://CCM-IP:8080/webdialer/services/WebdialerSoapService> where CCM-IP specifies the IP address of the Cisco Unified CallManager server where WebDialer is configured.

Use this SOAP interface for multicloud applications that require functionality, similar to a Redirector servlet, for redirecting calls to the various locations where Cisco Unified CallManager WebDialer is installed on a network. The application uses this interface to locate and verify the Cisco Unified CallManager WebDialer that is servicing the user, followed by makeCall, endCall, or getProfile requests to that Cisco WebDialer.

Parameter	Mandatory	Description	Data Type	Range of Values	Default Value
UserID	Mandatory	The user ID for which the request is made.	String	None	None

Refer to the [“Cisco WebDialer WSDL” section on page 37-16](#) for return values and their data type.

Name	Type	Description
result	Boolean	The result specifies true if the user is present in the directory of the cluster. The result specifies false if the user is not present in the directory.

HTML over HTTPS Interfaces

This section describes the HTML over HTTPS interfaces.

makeCall

You use the makeCall interface in customized directory search applications. The Cisco Unified CallManager directory search page (directory.asp) also uses this interface. Access the makeCall interface by initiating an HTTPS request to the URL `https://<ipaddress>/webdialer/Webdialer`. In this URL, ipaddress specifies the IP address of the Cisco Unified CallManager server where Cisco WebDialer is configured.

Browser-based applications in which the browser accepts cookies use this interface. The user profile exists only for the length of the session if the cookies are disabled in a browser. For a sample script that is used to enable directory search pages, go to the [“Sample JavaScript” section on page 37-19](#).

Parameter	Mandatory	Description	Data Type	Range of Values	Default Value
destination	Mandatory	Destination number called by the application. Number gets converted to a regular telephone number by applying the application dial rules. Refer to the <i>Cisco WebDialer</i> chapter in the <i>Cisco Unified CallManager Features and Services Guide, Release 5.0</i> .	String	None	None

Name	Description
result	Cisco Unified CallManager WebDialer displays the appropriate dialog and its applicable success or error message. It displays an authentication dialog if no active session exists.

makeCallProxy

You access the makeCallProxy interface by initiating an HTTPS request to the URL `https://ipaddress/webdialer/Webdialer?cmd=doMakeCallProxy`. Browser-based applications in which the browser accepts cookies use this interface. If the cookies are disabled in a browser, the user profile exists only for the length of the session.

Applications such as a personal address book, defined in the Unified CMUser pages at `https://cmserver/CMUser`, can use the makeCallProxy interface. The credential of the application gets used, as a proxy, to make calls on behalf of users. Because these users have authenticated themselves before accessing the Unified CMUser window, they do not get prompted again for their user ID and password. The application sends the user ID and password of the proxy user in the form of a query string in the request or as a parameter in the body of the POST message.

For a sample script that is used to enable directory search pages, go to the [“Sample JavaScript” section on page 37-19](#).

Parameter	Mandatory	Description	Data Type	Range of Values	Default Value
uid	Mandatory	The user ID for which the request is made	String	None	None
appid	Mandatory	The userid of the application that is making a request on behalf of the user. For example, consider a Unified CM personal address book where the application allows authentication proxy rights. The appid parameter gets used when the user logs in once; for example in the Unified CM User windows. After this login, other pages do not require the user to log in again. For web page applications that are not integrated, appid is the same as userid.	String	None	None
pwd	Mandatory	The password of the appid	String	None	None
destination	Mandatory	The number to be called. The dial plan service converts this number to an E.164 number.	String	None	None

Name	Description
result	Cisco Unified CallManager WebDialer displays the appropriate dialog and its applicable success or error message.

Cisco WebDialer WSDL

The WSDL specification provides the basis for the Web Service Definition Language (WSDL) for Cisco Unified CallManager WebDialer. You can access the WSDL for Cisco Unified CallManager WebDialer on the Cisco Unified CallManager WebDialer server installation at:

<https://CCM-IP:8080/webdialer/services/WebdialerSoapService?wsdl>

Use this specific WSDL and the interfaces that are mentioned in this document to develop customized applications for Cisco Unified CallManager WebDialer. For a list of references on Cisco Unified CallManager, SOAP, and WSDL, refer to the “Related Documentation” section in the Preface to the *Cisco Unified CallManager Developers Guide for Release 5.0*.

```
<wsdl:definitions xmlns:tns="urn:WebdialerSoap"
  xmlns:soap="https://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:http="https://schemas.xmlsoap.org/wsdl/http/"
  xmlns:mime="https://schemas.xmlsoap.org/wsdl/mime/"
  xmlns:xsd="https://www.w3.org/2001/XMLSchema"
  xmlns:soapenc="https://schemas.xmlsoap.org/soap/encoding/"
  xmlns:wsdl="https://schemas.xmlsoap.org/wsdl/" xmlns="https://schemas.xmlsoap.org/wsdl/"
  targetNamespace="urn:WebdialerSoap" name="urn:WebdialerSoap">
  <wsdl:types>
    <xsd:schema xmlns:xsd="https://www.w3.org/2001/XMLSchema"
      xmlns:tns="urn:WebdialerSoap" targetNamespace="urn:WebdialerSoap">
      <xsd:import namespace="https://schemas.xmlsoap.org/soap/encoding/" />
      <xsd:complexType name="CallResponse">
        <xsd:sequence>
          <xsd:element name="responseCode" type="xsd:int" />
        </xsd:sequence>
      </xsd:complexType>
    </xsd:schema>
  </wsdl:types>
</wsdl:definitions>
```

```

        <xsd:element name="description" nillable="true" type="xsd:string"/>
    </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="Credential">
    <xsd:sequence>
        <xsd:element name="userID" nillable="true" type="xsd:string"/>
        <xsd:element name="password" nillable="true" type="xsd:string"/>
    </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="UserProfile">
    <xsd:sequence>
        <xsd:element name="user" nillable="true" type="xsd:string"/>
        <xsd:element name="deviceName" nillable="true" type="xsd:string"/>
        <xsd:element name="lineNumber" nillable="true" type="xsd:string"/>
        <xsd:element name="supportEM" type="xsd:boolean"/>
        <xsd:element name="locale" nillable="true" type="xsd:string"/>
    </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="GetConfigResponse">
    <xsd:sequence>
        <xsd:element name="responseCode" type="xsd:int"/>
        <xsd:element name="description" nillable="true" type="xsd:string"/>
        <xsd:element name="deviceInfoList" nillable="true"
type="tns:ArrayOfWDDDeviceInfo"/>
    </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="WDDDeviceInfo">
    <xsd:sequence>
        <xsd:element name="deviceName" nillable="true" type="xsd:string"/>
        <xsd:element name="lines" nillable="true" type="tns:ArrayOfstring"/>
    </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="ArrayOfWDDDeviceInfo">
    <xsd:complexContent>
        <xsd:restriction base="soapenc:Array">
            <xsd:attribute ref="soapenc:arrayType"
wsdl:arrayType="tns:WDDDeviceInfo[]" />
        </xsd:restriction>
    </xsd:complexContent>
</xsd:complexType>
<xsd:complexType name="ArrayOfstring">
    <xsd:complexContent>
        <xsd:restriction base="soapenc:Array">
            <xsd:attribute ref="soapenc:arrayType" wsdl:arrayType="xsd:string[]" />
        </xsd:restriction>
    </xsd:complexContent>
</xsd:complexType>
</xsd:schema>
</wsdl:types>
<wsdl:message name="makeCallSoap0In">
    <wsdl:part name="cred" type="tns:Credential"/>
    <wsdl:part name="dest" type="xsd:string"/>
    <wsdl:part name="prof" type="tns:UserProfile"/>
</wsdl:message>
<wsdl:message name="makeCallSoap0Out">
    <wsdl:part name="Result" type="tns:CallResponse"/>
</wsdl:message>
<wsdl:message name="endCallSoap1In">
    <wsdl:part name="cred" type="tns:Credential"/>
    <wsdl:part name="prof" type="tns:UserProfile"/>
</wsdl:message>
<wsdl:message name="endCallSoap1Out">
    <wsdl:part name="Result" type="tns:CallResponse"/>
</wsdl:message>
<wsdl:message name="getProfileSoap2In">
    <wsdl:part name="cred" type="tns:Credential"/>
    <wsdl:part name="userid" type="xsd:string"/>

```

```

</wsdl:message>
<wsdl:message name="getProfileSoap2Out">
  <wsdl:part name="Result" type="tns:GetConfigResponse"/>
</wsdl:message>
<wsdl:message name="isClusterUser3In">
  <wsdl:part name="userid" type="xsd:string"/>
</wsdl:message>
<wsdl:message name="isClusterUser2Out">
  <wsdl:part name="Result" type="xsd:boolean"/>
</wsdl:message>
<portType name="WebdialerSoapService">
  <wsdl:operation name="makeCallSoap">
    <wsdl:input message="tns:makeCallSoap0In"/>
    <wsdl:output message="tns:makeCallSoap0Out"/>
  </wsdl:operation>
  <wsdl:operation name="endCallSoap">
    <wsdl:input message="tns:endCallSoap1In"/>
    <wsdl:output message="tns:endCallSoap1Out"/>
  </wsdl:operation>
  <wsdl:operation name="getProfileSoap">
    <wsdl:input message="tns:getProfileSoap2In"/>
    <wsdl:output message="tns:getProfileSoap2Out"/>
  </wsdl:operation>
  <wsdl:operation name="isClusterUserSoap">
    <wsdl:input message="tns:isClusterUser3In"/>
    <wsdl:output message="tns:isClusterUser2Out"/>
  </wsdl:operation>
</portType>
<binding name="WebdialerSoapService" type="tns:WebdialerSoapService">
  <soap:binding style="rpc" transport="https://schemas.xmlsoap.org/soap/http"/>
  <wsdl:operation name="makeCallSoap">
    <soap:operation soapAction="urn:makeCallSoap"/>
    <input>
      <soap:body use="encoded" encodingStyle=
"https://schemas.xmlsoap.org/soap/encoding/" namespace="urn:WebdialerSoap"/>
    </input>
    <output>
      <soap:body use="encoded" encodingStyle=
"https://schemas.xmlsoap.org/soap/encoding/" namespace="urn:WebdialerSoap"/>
    </output>
  </wsdl:operation>
  <wsdl:operation name="endCallSoap">
    <soap:operation soapAction="urn:endCallSoap"/>
    <input>
      <soap:body use="encoded" encodingStyle=
"https://schemas.xmlsoap.org/soap/encoding/" namespace="urn:WebdialerSoap"/>
    </input>
    <output>
      <soap:body use="encoded" encodingStyle=
"https://schemas.xmlsoap.org/soap/encoding/" namespace="urn:WebdialerSoap"/>
    </output>
  </wsdl:operation>
  <wsdl:operation name="getProfileSoap">
    <soap:operation soapAction="urn:getProfileSoap"/>
    <input>
      <soap:body use="encoded" encodingStyle=
"https://schemas.xmlsoap.org/soap/encoding/" namespace="urn:WebdialerSoap"/>
    </input>
    <output>
      <soap:body use="encoded" encodingStyle=
"https://schemas.xmlsoap.org/soap/encoding/" namespace="urn:WebdialerSoap"/>
    </output>
  </wsdl:operation>
  <wsdl:operation name="isClusterUserSoap">
    <soap:operation soapAction="urn:isClusterUserSoap"/>
    <input>

```

```

        <soap:body use="encoded" encodingStyle=
"https://schemas.xmlsoap.org/soap/encoding/" namespace="urn:WebdialerSoap"/>
        </input>
        <output>
        <soap:body use="encoded"
encodingStyle="https://schemas.xmlsoap.org/soap/encoding/" namespace="urn:WebdialerSoap"/>
        </output>
    </wsdl:operation>
</binding>
<service name="WebdialerSoap">
    <port name="WebdialerSoapService" binding="tns:WebdialerSoapService">
        <soap:address location=
"https://WebDialer_ip_address:8080/webdialer/services/WebdialerSoapService"/>
    </port>
</service>
</wsdl:definitions>

```

Sample JavaScript

This sample JavaScript script enables Cisco Unified CallManager WebDialer from a directory search page.

Single Cluster Applications

Use this script for single cluster applications if all users are in only one cluster.

```

function launchWebDialerWindow( url ) {
    webdialer=window.open( url, "webdialer", "status=no, width=420, height=300,
scrollbars=no, resizable=yes, toolbar=no" );
}

function launchWebDialerServlet( destination ) {
    url = 'https://<%=server_name%>/webdialer/Webdialer?destination=' +
escape(destination);
    launchWebDialerWindow( url );
}

!These functions can be called from the HTML page which has a hyperlink to the phone
number to be called. An example of it is:
<TD><A href="javascript:launchWebDialerServlet( <%= userInfo.TelephoneNumber %> )" "><%=
userInfo.TelephoneNumber %></A>&nbsp;</TD>

```

Multiple Cluster Applications

Use this script if all users are spread across different clusters.

```

function launchWebDialerWindow( url ) {
    webdialer=window.open( url, "webdialer", "status=no, width=420, height=300,
scrollbars=no, resizable=yes, toolbar=no" );
}

function launchWebDialerServlet( destination ) {
    url= 'https://<%=server_name%>/webdialer/Redirector?destination='+escape(destination);
    launchWebDialerWindow( url );
}

!These functions can be called from the HTML page which has a hyperlink to the phone
number to be called. An example of it is:
<TD><A href="javascript:launchWebDialerServlet( <%= userInfo.TelephoneNumber %> )" "><%=
userInfo.TelephoneNumber %></A>&nbsp;</TD>

```




PART 12

Cisco Unified IP Phone Information





Enhanced Immediate Divert Behavior

Cisco Unified CallManager 5.1 provides enhanced usage of the **iDivert** key by allowing users to transfer incoming calls directly to their voice messaging system or to the voice messaging system of the original called party. For information on configuring this feature in Cisco Unified CallManager administration, refer to the *Cisco Unified CallManager Features and Services Guide* section of this document, “Immediate Divert” chapter.

How the Phone User Sends a Call to a Voice Messaging System

Users can use **iDivert** to send an active, ringing, or on-hold call to their voice messaging system. Depending on the type of call and their phone configuration, they can also use **iDivert** to send the call to another party's voice messaging system.

- If a call originally gets sent to someone else's phone, **iDivert** allows the user to redirect the call either to their own voice messaging system or to the original called party's voice messaging system. The system administrator must make this option available.
- If a call gets sent to the user directly (not transferred or forwarded to the user), or if the user's phone does not support the option described above, using **iDivert** redirects the call to the user's own voice messaging system.

Phones that Support Enhanced iDivert:

- Cisco Unified IP Phone 7906G and 7911G (SCCP and SIP)
- Cisco Unified IP Phone 7961G/GE and 7941G/GE (SCCP and SIP)
- Cisco Unified IP Phone 7970G/7971G-GE (SCCP and SIP)
- Cisco Unified IP Phone 7905G and 7912G (SCCP only)
- Cisco Unified IP Phone 7960G and 7940G (SCCP only)



Arabic Support

Cisco Unified CallManager Release 5.1 supports Arabic locales on Cisco Unified CallManager user interfaces and Arabic text on phone screen displays for supported phone models.

Phones that Support Arabic:

- Cisco Unified IP Phone 7906G and 7911G
- Cisco Unified IP Phone 7961G/GE and 7941G/GE
- Cisco Unified IP Phone 7970G/7971G-GE





A

AAR

explained [7-1](#)

abbreviated dial

described [11-26](#)

A Cisco DB Replicator service [19-7](#)

A Cisco DB service [19-7](#)

ac user

associating with devices and pilot points [14-28](#)

configuring [14-21](#)

administrators, CAR [24-5](#)

admission control [5-13](#)

Alarm configuration, described [16-1](#)

Alarms

configuration checklist [20-3](#)

configuration overview [20-2](#)

configuring, procedure [16-1](#)

definitions, described [20-2](#)

described [20-1](#)

destinations [16-3](#)

destination settings [16-3](#)

event levels [16-4](#)

event level settings [16-4](#)

Event Viewer [16-3](#)

overview [20-1](#)

SDI trace library [16-3](#)

SDL trace library [16-3](#)

Syslog [16-3](#)

updating, procedure [16-1](#)

viewing information

overview [20-2](#)

alerts

emailing notification [23-61](#)

enabling or disabling, by mail [26-8](#)

notification for a counter [23-61](#)

scheduling notification [23-61](#)

thresholds [23-61](#)

Arabic locales

phone support [39-1](#)

Attendant Console

See Cisco Unified CallManager Attendant Console

audio sources

configuring [12-16](#)

creating for MOH [12-9](#)

default MOH sample [12-9](#)

for MOH [12-8](#)

managing for MOH [12-10](#)

multicast [12-10](#)

storing for MOH [12-9](#)

unicast [12-10](#)

authenticate and show CAR pages [24-14](#)

Authentication [36-14](#)

authentication

device [30-15](#)

digest [30-15](#)

interactions [30-5](#)

overview [30-15](#)

restrictions [30-5](#)

authorization [30-15](#)

interactions [30-5](#)

overview [30-15](#)

automated alternate routing (AAR)

dial prefix matrix example (table) [7-3](#)

enable service parameter [7-3](#)

example [7-2](#)

explained [7-1](#)
 line/DN and AAR groups (table) [7-2](#)
 automatic
 database purge [25-14](#)
 report generation [26-6](#)
 AXL API [36-3](#)
 AXL Compliance [36-3](#)
 AXL Error Codes [36-3](#)
 AXL Schema Documentation [36-12](#)

B

backup
 service
 Cisco DRF Local [19-11](#)
 Cisco DRF Master [19-11](#)
 bandwidth
 used by Cisco Unified CallManager [5-7](#)
 used by codec types (table) [5-8](#)
 barge
 described [11-21](#)
 encryption restrictions with [30-11](#)
 base rate [26-2](#)
 bill
 department detail, report results [28-3](#)
 department summary, report results [28-2](#)
 individual detail, report results [28-3](#)
 individual summary, report results [28-2](#)
 buttons
 directories button [11-29](#)
 messages button [11-28](#)

C

C++ Example [36-6](#)
 call admission control [5-13](#)
 call coverage
 call forwarding [7-11](#)

described [7-11](#)
 hunting [7-11](#)
 maximum hunt timer [7-12](#)
 personal preferences [7-12](#)
 call detail
 conference call detail, report results [28-21](#)
 call diagnostics and voice quality metrics
 described [11-26](#)
 call display restrictions
 configuring in translation pattern [7-29](#)
 called party
 transformations [7-26](#)
 transformations settings [7-28](#)
 transformations settings (table) [7-28](#)
 caller identification
 restrictions [7-29](#)
 support for device control protocols (table) [7-34](#)
 support vs. device control protocols [7-33](#)
 types [7-29](#)
 Call Flows [37-6](#)
 Desktop-based Client Application [37-6](#)
 WebDialer Browser-based Application [37-8](#)
 WebDialer Client-based Application [37-7](#)
 call forward
 described [7-11, 8-6, 11-21](#)
 calling party
 presentation settings [7-29](#)
 restriction settings [7-29](#)
 transformations [7-26](#)
 transformations settings [7-26](#)
 transformations settings (table) [7-27, 7-30](#)
 calling search spaces
 search for phones [11-27](#)
 call park
 described [11-23](#)
 example with MOH [12-5](#)
 call pickup
 described [11-23](#)
 call queuing [14-9](#)

- calls
 - making and receiving multiple per directory number [8-7](#)
 - on-hook call transfer [11-24](#)
- call select
 - described [11-23](#)
- call termination
 - CDR search by [27-4](#)
- call types
 - QoS report results by call types [28-11](#)
- call waiting
 - described [8-7](#)
- CAR
 - administrators, managers, users [24-5](#)
 - automatic database purge configuration [25-14](#)
 - automatic report generation/alert configuration [26-6](#)
 - call termination details, viewing [27-5](#)
 - CDR search
 - by call precedence levels [27-5](#)
 - configuration [27-1](#)
 - malicious calls [27-7](#)
 - overview [24-12](#)
 - CDR search by cause for call termination configuration [27-4](#)
 - CDR search by gateway configuration [27-3](#)
 - CDR search by user extension configuration [27-1](#)
 - checklist [24-15](#)
 - configuration, gateway [25-5](#)
 - described [24-2](#)
 - device reports
 - overview [24-10](#)
 - dial plan default values [25-4](#)
 - disabling automatic database purge [25-14](#)
 - event log report output parameters [25-16](#)
 - event log report status [25-15](#)
 - list of topics [24-1](#)
 - load CDR and CMR values [25-8](#)
 - manual database purge [25-12](#)
 - notification limits configuration [26-8](#)
 - QoS default values [26-5](#)
 - QoS values, defining [26-5](#)
 - rating engine configuration [26-1](#)
 - report configuration, described [26-1](#)
 - reports, results [28-1](#)
 - restoring database purge defaults [25-12](#)
 - restoring dial plan default values [25-4](#)
 - system configuration [24-6, 25-1](#)
 - system log screens, described [25-15](#)
 - system preferences parameters [25-6](#)
 - system reports
 - overview [24-8](#)
 - uninhibited loading of CDR values [25-8](#)
 - user reports [24-7](#)
- car_CDRSearchByCauseCodesReport [27-5](#)
- Catalyst 4000
 - 4224 voice gateway switch [10-7](#)
 - access gateway module [10-7](#)
 - voice gateway modules [10-5](#)
- Catalyst 4224 Voice Gateway Switch [10-7](#)
- Catalyst 6000
 - Cisco Communication Media Module [10-7](#)
 - FXS analog interface module [10-6](#)
 - hookflash transfer [10-6](#)
 - T1/E1 line card [10-6](#)
 - voice gateway modules [10-5](#)
- category
 - adding [18-17](#)
 - deleting [18-18](#)
 - renaming [18-17](#)
- category tabs [23-60](#)
 - sample rates [23-61](#)
- CDR
 - automatic database purge configuration [25-14](#)
 - disabling automatic database purge [25-14](#)
 - disabling loading [25-7](#)
 - dump table [28-25](#)
 - error, report results [28-17](#)
 - load schedule configuration [25-7](#)

- restoring the default load schedule [25-7](#)
- search [27-1](#)
- search by cause for call termination [27-4](#)
- search by gateway [27-3](#)
- search by user extension [27-1](#)
- search by user extension, report results [28-23](#)
- service
 - Cisco CAR Scheduler [19-5](#)
 - Cisco CAR Web Service [19-5](#)
 - Cisco CDR Agent [19-11](#)
 - Cisco SOAP - CDRonDemand Service [19-4](#)
- values
 - CDR load [25-8](#)
- CDR analysis and reporting
 - general information [24-6](#)
 - internationalization [24-14, 24-15](#)
- CDRs
 - understanding [24-1](#)
- CDR values
 - uninhibited loading [25-8](#)
- centralized TFTP
 - configuration tips [6-10](#)
 - master TFTP server [6-9](#)
 - overview [6-9](#)
 - secure clusters [6-10](#)
- Certificate Authority Proxy Function (CAPF)
 - CAPF service [31-5](#)
 - installing [30-12](#)
- certificates
 - external CAs [30-12](#)
 - types [30-12](#)
- Certificate Signing Requests (CSRs) [30-12](#)
- CFA Destination Override service parameter [8-6, 11-22](#)
- Changes in Release 5.0(2) [37-4](#)
- channel associated signaling (CAS) [10-1](#)
- characters, special
 - configuring [7-16](#)
 - described (table) [7-17](#)
- Cisco Access Digital Trunk Gateways
 - DT-24+/DE-30+ [10-2](#)
- Cisco AMC Service [19-10](#)
- Cisco Analog Access
 - perfmon object and counters [23-3](#)
- Cisco Analyzer service [19-4](#)
- Cisco Annunciator Device
 - perfmon object and counters [23-4](#)
- Cisco AXL Web Service [19-5](#)
- Cisco Bulk Provisioning Service [19-5](#)
- Cisco CallManager
 - perfmon object and counters [23-4](#)
- Cisco CallManager Admin service [19-9](#)
- Cisco CallManager Attendant Console
 - perfmon object and counters [23-11](#)
- Cisco CallManager Attendant Console Server
 - service [19-3](#)
 - service parameters [14-32](#)
 - understanding [14-10](#)
- Cisco CallManager Cisco IP Phone Services [19-3](#)
- Cisco CallManager Personal Directory service [19-9](#)
- Cisco CallManager Serviceability service [19-9](#)
- Cisco CallManager System Performance
 - perfmon object and counters [23-12](#)
- Cisco CAR Scheduler service [19-5](#)
- Cisco CAR Web Service [19-5](#)
- Cisco CDP Agent service [19-8](#)
- Cisco CDP service [19-9](#)
- Cisco CDR Agent service [19-11](#)
- Cisco Certificate Authority Proxy Function (CAPF)
 - service [19-6](#)
- Cisco Certificate Expiry Monitor service [19-8](#)
- Cisco Communication Media Module (CMM) [10-7](#)
- Cisco CTIManager
 - perfmon object and counters [23-15](#)
- Cisco CTL Provider service [19-6](#)
- Cisco Database Layer Monitor service [19-8](#)
- Cisco DB Replicator service [19-7](#)
- Cisco DB service [19-7](#)
- Cisco DHCP Monitor service [19-4](#)

- Cisco Dual-Mode Mobility perfmon object and counters [23-16](#)
- Cisco Electronic Notification service [19-8](#)
- Cisco Extended Functions service [19-3](#)
- Cisco Extension Mobility
 - perfmon object and counters [23-17](#)
- Cisco Extension Mobility Application [19-10](#)
- Cisco Gatekeeper
 - perfmon object and counters [23-17](#)
- Cisco H.323
 - perfmon object and counters [23-18](#)
- Cisco Hunt Lists
 - perfmon object and counters [23-19](#)
- Cisco HW Conference Bridge Device
 - perfmon object and counters [23-20](#)
- Cisco IAD2420 Integrated Access Device [10-4](#)
- Cisco IP Communicator
 - default phone button template [11-14](#)
 - described [11-9](#)
- Cisco IP Manager Assistant
 - perfmon object and counters [23-20](#)
- Cisco IP Phone services
 - report results [28-9](#)
- Cisco IP Voice Media Streaming App service [19-3](#)
- Cisco License Manager service [19-8](#)
- Cisco Lines
 - perfmon object and counters [23-21](#)
- Cisco Locations
 - perfmon object and counters [23-21](#)
- Cisco Log Partition Monitoring Tool service [19-9](#)
- Cisco Media Streaming Application
 - perfmon object and counters [23-22](#)
- Cisco Messaging Interface
 - perfmon object and counters [23-25](#)
- Cisco Messaging Interface service [19-3](#)
- Cisco MGCP FXO Device
 - perfmon object and counters [23-25](#)
- Cisco MGCP FXS Device
 - perfmon object and counters [23-26](#)
- Cisco MGCP Gateways
 - perfmon object and counters [23-26](#)
 - Cisco MGCP Gateways [23-27](#)
- Cisco MGCP PRI Device
 - perfmon object and counters [23-27](#)
- Cisco MGCP T1CAS Device
 - perfmon object and counters [23-27](#)
- Cisco MOH Device
 - perfmon object and counters [23-28](#)
- Cisco MTP Device
 - perfmon object and counters [23-29](#)
- Cisco Phones
 - perfmon object and counters [23-29](#)
- Cisco Presence Feature
 - perfmon object and counters [23-30](#)
- Cisco QSIG Features
 - perfmon object and counters [23-30](#)
- Cisco RIS Data Collector service [19-9](#)
- Cisco RTMT Reporter Servlet [19-10](#)
- Cisco Serviceability Reporter service [19-5](#)
- Cisco SIP
 - perfmon object and counters [23-30](#)
- Cisco SIP IP Phones
 - default phone button template (advanced) [11-14](#)
 - default phone button template (basic) [11-14](#)
 - models supported [11-8](#)
 - third-party SIP device differences [4-1](#)
- Cisco SIP Stack
 - perfmon object and counters [23-31](#)
- Cisco SOAP - CDRonDemand Service [19-4](#)
- Cisco SOAP-Log-Collection APIs [19-10](#)
- Cisco SOAP Performance Monitoring APIs service [19-10](#)
- Cisco SW Conf Bridge Device
 - perfmon object and counters [23-39](#)
- Cisco Syslog Agent service [19-8](#)
- Cisco TelePresence
 - described [11-9](#)
- Cisco TFTP Server
 - perfmon object and counters [23-40](#)

- Cisco TFTP service [19-3](#)
 - alternate Cisco file servers [6-8](#)
 - configuration checklist (table) [6-11](#)
 - list of topics [6-1](#)
 - more information [6-11](#)
 - overview [6-1](#)
 - understanding [6-4](#)
- Cisco Tomcat Connector
 - perfmon object and counters [23-43](#)
- Cisco Tomcat service [19-7](#)
- Cisco Tomcat Stats Servlet [19-10](#)
- Cisco Trace Collection Service [19-9](#)
- Cisco Trace Collection Servlet [19-9](#)
- Cisco Transcode Device
 - perfmon object and counters [23-47](#)
- Cisco Unified CallManager
 - bandwidth usage [5-7](#)
 - configuration, configuring [5-2](#)
 - configuring [5-2](#)
 - groups
 - configuring [5-3](#)
 - MOH servers [12-7](#)
 - server, configuring [5-1](#)
 - service
 - Cisco Analyzer [19-4](#)
 - Cisco CallManager [19-2](#)
 - Cisco CallManager Admin [19-9](#)
 - Cisco CallManager Attendant Console Server [19-3](#)
 - Cisco CallManager Personal Directory [19-9](#)
 - Cisco CallManager Serviceability [19-9](#)
 - Cisco CDP [19-9](#)
 - Cisco CTIManager [19-3](#)
 - Cisco DHCP Monitor Service [19-4](#)
 - Cisco Extended Functions [19-3](#)
 - Cisco Extension Mobility Application [19-10](#)
 - Cisco IP Voice Media Streaming App [19-3](#)
 - Cisco Log Partition Monitoring Tool [19-9](#)
 - Cisco Messaging Interface [19-3](#)
 - Cisco TFTP [19-3](#)
 - Cisco Tomcat Stats Servlet [19-10](#)
 - Cisco Trace Collection Service [19-9](#)
 - Cisco Trace Collection Servlet [19-9](#)
 - supported voice codecs [5-7](#)
 - Cisco Unified CallManager Assistant
 - softkey templates
 - described [11-16](#)
 - Cisco Unified CallManager Attendant Console
 - associating devices and pilot points with ac user [14-28](#)
 - client configuration settings (table) [14-37](#)
 - configuration checklist [14-17](#)
 - configuring [14-16](#)
 - configuring attendant settings [14-37](#)
 - configuring held icon timers [14-39](#)
 - CorporateDirectory.txt file
 - creating and uploading [14-33](#)
 - deleting [14-34](#)
 - dependency records [14-40](#)
 - directory [14-9](#)
 - Enabling Super Provider [14-22](#)
 - Firewall Support [14-12](#)
 - hunt groups
 - configuration settings (table) [14-30](#)
 - deleting members [14-32](#)
 - understanding [14-2](#)
 - viewing members [14-32](#)
 - installation and activation [14-16](#)
 - installing [14-35](#)
 - interactions [14-14](#)
 - overview [14-1](#)
 - pilot points
 - configuration settings [14-25](#)
 - configuring [14-24](#)
 - deleting [14-27](#)
 - finding [14-23](#)
 - resetting [14-28](#)
 - understanding [14-2](#)
 - redundancy [14-11](#)
 - restrictions [14-15](#)

- starting after installing Windows XP SP2 [14-36](#)
- system requirements [14-12](#)
- users
 - configuration settings [14-20](#)
 - configuring [14-18](#)
 - configuring the ac user [14-21](#)
 - deleting [14-21](#)
 - finding [14-19](#)
 - understanding [14-2](#)
- Cisco Unified CallManager System Guide
 - conventions [xxv](#)
 - organization [xxiv](#)
 - related documentation [xxv](#)
- Cisco Unified CallManager User Options [11-29](#)
- Cisco Unified IP Phones
 - See also* phones
 - 12 SP+, described [11-7](#)
 - 30 VIP, described [11-8](#)
 - 7902, described [11-6](#)
 - 7905, described [11-6](#)
 - 7906, described [11-5](#)
 - 7910, described [11-5](#)
 - 7911, described [11-5](#)
 - 7912, described [11-4](#)
 - 7914 Expansion Module, described [11-4](#)
 - 7920, described [11-4](#)
 - 7935, described [11-7](#)
 - 7940, described [11-3](#)
 - 7941, described [11-3](#)
 - 7960, described [11-3](#)
 - 7961, described [11-3](#)
 - 7970, described [11-2](#)
 - 7971, described [11-2](#)
 - 7985, described [11-6](#)
- Cisco Unified IP Conference Station 7936,
 - described [11-7](#)
- configuration tips for phone security profiles [32-1](#)
- deleting CTL file [31-16](#)
- directories button [11-29](#)
- encrypted configuration file [33-1](#)
- features
 - abbreviated dial [11-26](#)
 - barge [11-21](#)
 - call diagnostics and voice quality metrics [11-26](#)
 - call forward [11-21](#)
 - call park [11-23](#)
 - call pickup [11-23](#)
 - call select [11-23](#)
 - conference list [11-24](#)
 - described [11-21](#)
 - direct transfer [11-24](#)
 - immediate divert [11-24](#)
 - join [11-24](#)
 - malicious call ID [11-25](#)
 - privacy [11-21](#)
 - quality report tool [11-25](#)
 - service URL [11-26](#)
 - speed dial [11-26](#)
- messages button [11-28](#)
- overview [11-1](#)
- security icons [30-5](#)
 - restrictions [30-9](#)
- supported models
 - described (table) [11-2](#)
 - listed [11-2](#)
- Cisco Unified Personal Communicator
 - described [11-9](#)
- Cisco VG200 Voice Gateway [10-2](#)
- Cisco VG224 Analog Phone Gateway
 - configuring [10-4](#)
 - description [10-4](#)
- Cisco VG248 Analog Phone Gateway
 - configuring [10-2](#)
 - description [10-2](#)
 - gateway redundancy [10-18](#)
- Cisco Video Conference Bridge
 - perfmon object and counters [23-47](#)
- Cisco WebDialer

- perfmon object and counters [23-48](#)
- Cisco WSM Connector
 - perfmon object and counters [23-48](#)
- CLI
 - starting services [15-6](#)
 - stopping services [15-6](#)
- closest-match routing [7-12](#)
- CMLocal date/time group [5-4](#)
- CMR dump table [28-25](#)
- CMR values, CDR load [25-8](#)
- codecs
 - bandwidth used per call (table) [5-8](#)
 - G.711 [5-7](#)
 - G.723 [5-7](#)
 - G.729 [5-7](#)
 - GSM [5-7](#)
 - supported by Cisco Unified CallManager [5-7](#)
 - wideband [5-7](#)
- common phone profiles
 - described [11-20](#)
- conference
 - described [8-7](#)
- conference bridge utilization, report results [28-22](#)
- conference call detail, report results [28-21](#)
- conference list
 - described [11-24](#)
- configuration
 - settings
 - checklist (table) [5-17](#)
 - list of topics [5-1](#)
- configuration checklist
 - CAR [24-15](#)
 - MGCP BRI [10-21](#)
- configuration file
 - encryption [30-19](#)
- configuration profile
 - adding [18-5](#)
 - deleting [18-6](#)
 - restoring [18-6](#)
 - using default [18-5](#)
- configuring [27-5, 27-7](#)
- connected party
 - presentation settings [7-31](#)
 - restriction settings [7-31](#)
 - transformations settings (table) [7-32](#)
- Control Center
 - described [19-12](#)
 - feature services [19-12](#)
 - network services [19-12](#)
 - starting services [15-4](#)
 - starting services, described [19-12](#)
 - stopping services [15-4](#)
 - stopping services, described [19-12](#)
 - viewing service status, described [19-12](#)
 - viewing status [15-4](#)
- conventions [xxv](#)
- CorporateDirectory.txt file
 - creating and uploading [14-33](#)
 - deleting [14-34](#)
- counters
 - adding [23-61](#)
 - alert notification [23-61](#)
 - chart [23-61](#)
 - perfmon, described [23-1](#)
 - properties [23-61](#)
 - zooming [23-61](#)
- CTI
 - Cisco CTIManager
 - perfmon object and counters [23-15](#)
 - Cisco CTIManager service [19-3](#)
 - finding CTI devices [18-10](#)
 - monitoring CTI applications [18-14](#)
 - monitoring CTI devices [18-14](#)
 - monitoring CTI lines [18-15](#)
 - ports
 - described [11-8](#)
 - service
 - Cisco IP Manager Assistant Service [19-4](#)

- Cisco WebDialer Web Service [19-4](#)
 - viewing CTIManager information [18-14](#)
- CTL client
 - CAPF service [31-5](#)
 - clusterwide security mode
 - updating [31-12](#)
 - configuration checklist (table) [31-3](#)
 - configuration settings (table) [31-13](#)
 - configuration tips [31-2](#)
 - configuring [31-8](#)
 - TLS ports [31-5](#)
 - CTL Provider service [31-4](#)
 - deleting CTL file on phone [31-16](#)
 - installing [30-12, 31-6](#)
 - migrating [31-7](#)
 - overview [31-2](#)
 - security mode
 - verifying [31-15](#)
 - security token password
 - changing [31-16](#)
 - setting the Smart Card service [31-15](#)
 - uninstalling [31-18](#)
 - upgrading [31-7](#)
 - verifying [31-18](#)
 - version
 - determining [31-17](#)
- CTL file
 - deleting entry [31-12](#)
 - deleting on phone [31-16](#)
 - updating [31-10](#)
- CTL Provider
 - activating service [31-4](#)
- CUPS license
 - configuring [3-1](#)
- customizing, reports for automatic generation [26-7](#)
- customizing reports for automatic generation [24-11](#)

D

- daily charges, notification limits configuration [26-8](#)
- daily reports
 - scheduling [25-9](#)
- database
 - automatic purge configuration [25-14](#)
 - disabling automatic purge [25-14](#)
 - restoring purge defaults [25-12](#)
 - scalability [12-7](#)
 - service
 - A Cisco DB [19-7](#)
 - A Cisco DB Replicator [19-7](#)
 - Cisco AXL Web Service [19-5](#)
 - Cisco Bulk Provisioning Service [19-5](#)
 - Cisco Database Layer Monitor [19-8](#)
- Database Change Notification Client
 - perfmon object and counters [23-49](#)
- Database Change Notification Server
 - perfmon object and counters [23-50](#)
- Database Change Notification Subscription
 - perfmon object and counters [23-50](#)
- Database Local DSN
 - perfmon object and counters [23-50](#)
- Data Encryption [36-14](#)
- date/time groups
 - CMLocal [5-4](#)
 - described [5-4](#)
- DB User Host Information Counters
 - perfmon object and counters [23-51](#)
- DDI [7-13](#)
 - configuring [7-19](#)
 - explained (table) [7-19](#)
- definitions
 - alarms [20-2](#)
- department bill detail, report results [28-3](#)
- department bill summary, report results [28-2](#)
- dependency records
 - Cisco Unified CallManager Attendant Console [14-40](#)

- directory numbers
 - described [8-9](#)
- gateways [10-16](#)
- phones
 - described [11-30](#)
- system-level settings [5-16](#)
- detail
 - department bill, report results [28-3](#)
 - gateway, report results [28-18](#)
 - individual bill, report results [28-3](#)
 - QoS, report results [28-9](#)
- device authentication [30-15](#)
 - configuration settings (table)
 - for SCCP phone [32-4](#)
 - for SIP phones [32-6](#)
 - configuring for phones [32-3](#)
- device control protocols
 - and caller identification support (table) [7-34](#)
- device pools
 - described [5-10](#)
 - search for phones [11-27](#)
 - updating [5-11](#)
- device reports, CAR [24-10](#)
- devices
 - accessing TFTP server [6-6](#)
 - identifying TFTP server [6-6](#)
 - using Cisco TFTP [6-4](#)
 - using DHCP [6-4](#)
- DHCP
 - and devices [6-4](#)
- dial plan, configuration [25-2](#)
- dial plans
 - accessing gateways [10-16](#)
- digest authentication [30-15](#)
 - configuration settings (table)
 - for SIP phones [32-6](#)
 - configuring for phones [32-3](#)
 - enabling for SIP third-party phones [4-2](#)
- digital trunk gateway
 - DT-24+/DE-30+ [10-2](#)
- digit analysis
 - static
 - caveats [7-15](#)
 - configuration tip [7-14](#)
 - described [7-14](#)
 - example prior to static digit analysis [7-15](#)
 - explained [7-14](#)
 - Unified CallManager Assistant example with static digit analysis [7-16](#)
- directories button
 - configuring [11-29](#)
- directory
 - access [9-3](#)
 - access for Cisco IP telephony endpoints [9-5](#)
 - Cisco DirSync service [19-7](#)
 - Cisco Unified CallManager Attendant Console, understanding [14-9](#)
 - configuration checklist (table) [9-6](#)
 - LDAP [5-12](#)
 - more information [9-7](#)
 - overview [9-1](#)
- directory numbers
 - active check box [8-5](#)
 - call forward
 - busy trigger [8-6, 11-22](#)
 - no answer ring duration [8-6, 11-22](#)
 - call forward information display [8-6, 11-22](#)
 - characteristics [8-1](#)
 - conference [8-7](#)
 - configuration checklist (table) [8-10](#)
 - dependency records
 - described [8-9](#)
 - direct transfer [8-8](#)
 - features [8-5](#)
 - call forward [8-6](#)
 - call waiting [8-7](#)
 - find all directory numbers [8-9](#)
 - join [8-8](#)

- making and receiving multiple calls [8-7](#)
- managing [8-5](#)
- more information [8-11](#)
- overview [8-1](#)
- search tips [8-8](#)
- shared line appearance [8-2](#)
- shared line appearance restrictions [8-4](#)
- transfer [8-7](#)
- update directory number of all devices sharing this line
 - check box [8-5](#)
- direct transfer
 - described [8-8, 11-24](#)
- disabling
 - alerts by mail [26-8](#)
 - automatic CAR and CDR database purge [25-14](#)
 - automatic database purge [25-14](#)
 - CDR loading [25-7](#)
- discard digits instructions (DDI) [7-13](#)
 - configuring [7-19](#)
 - explained (table) [7-19](#)
- divert to voice messaging
 - phone support [38-1](#)
 - phone user [38-1](#)
- DNs
 - characteristics [8-1](#)
 - overview [8-1](#)
- document
 - conventions [xxv](#)
 - organization [xxiv](#)
- documentation
 - related [xxv](#)
- dump table, CDR and CMR [28-25](#)
- duration [26-2](#)

E

- E1 Primary Rate Interface (PRI) [10-1](#)
- enabling
 - alerts by mail [26-8](#)

- reports for automatic generation [26-7](#)
- enabling reports for automatic generation [24-11](#)
- encrypted configuration file
 - configuration checklist (table) [33-5](#)
 - configuration settings (table)
 - for manual key [33-7](#)
 - configuration tips [33-4](#)
 - configuring manual key distribution [33-6](#)
 - disabling [33-9](#)
 - enabling [33-6](#)
 - entering symmetric key [33-7](#)
 - manual key configuration checklist (table) [33-7](#)
 - manual key distribution [33-2](#)
 - phone support [33-4](#)
 - symmetric key encryption with public key [33-3](#)
 - understanding [33-1](#)
 - using symmetric key encryption w/public key [33-8](#)
 - verifying [33-8](#)
- encryption
 - configuration settings (table)
 - for SCCP phone [32-4](#)
 - for SIP phone security profiles [32-6](#)
 - configuring for phones [32-3](#)
 - configuring with barge [30-11](#)
 - installing [30-12](#)
 - interactions [30-5](#)
 - overview [30-19](#)
 - restrictions [30-5, 30-6](#)
 - with authentication [30-7](#)
 - with barge [30-7](#)
 - with media resources [30-8](#)
 - with packet capturing [30-9](#)
 - with phone and trunk devices [30-8](#)
 - with security icons [30-9](#)
 - signaling
 - configuring for phones [32-3](#)
- endCallSoap [37-11](#)
- enterprise parameters
 - described [5-15](#)

Enterprise Replication DBSpace Monitors

perfmon object and counters [23-51](#)

Enterprise Replication Perfmon Counters

perfmon object and counters [23-51](#)

error

CDR report, results [28-17](#)

etoken

changing password [31-16](#)event levels for alarms [16-4](#)

event log

generating [25-15](#)event log, generating [24-6](#)

event log report

output [25-16](#)status [25-15](#)Example AXL Requests [36-5](#)Example XML Structure [36-13](#)

expansion module

Cisco Unified IP Phone 7914 [11-4](#)

extension

CDR search by [27-1](#)CDR search by, report results [28-23](#)

external route plan wizard

described [7-34](#)generated route filters [7-35](#)generated route groups [7-36](#)generated route lists [7-36](#)generated route patterns [7-37](#)

F

features

immediate divert [13-1](#)phone features (table) [11-15](#)

feature services

activating [15-1, 19-1](#)configuration checklist (table) [19-13](#)deactivating [15-1](#)described [19-1](#)multiserver recommendations (table) [15-2](#)starting [15-4, 19-1](#)stopping [15-4, 19-1](#)viewing status [15-4, 19-1](#)

fields

requiring route patterns (table) [7-18](#)file authentication [30-15](#)configuring for phones [32-3](#)

fixed audio source

configuration settings (table) [12-23](#)configuring [12-21, 12-22](#)deleting [12-22](#)Foreign Exchange Office (FXO) [10-1](#)Foreign Exchange Station (FXS) [10-1](#)FXO [10-1](#)FXS [10-1](#)

G
G.711 [5-7](#)G.723 [5-7](#)G.729 [5-7](#)

gateway

CDR search by [27-3](#)configuration for CAR [25-5](#)QoS report results by gateway [28-11](#)gateway detail, report results [28-18](#)

gateways

Catalyst 4000 Access Gateway Module [10-7](#)Catalyst 4224 gateway [10-7](#)Catalyst 6000 FXS Analog Interface Module [10-6](#)Catalyst 6000 T1/E1 and Services Module [10-6](#)Cisco Communications Media Module [10-7](#)Cisco IOS H.323 devices [10-7](#)Cisco voice gateways [10-1](#)configuration checklist (table) [10-20](#)dependency records [10-16](#)failover and fallback [10-17](#)H.323 devices list [10-7](#)

- models (table) [10-9](#)
- more information [10-22](#)
- overview [10-1](#)
- port types (table) [10-9](#)
- related to dial plans [10-16](#)
- signaling protocols (table) [10-9](#)
- standalone
 - digital trunk [10-2](#)
 - IAD2420 [10-4](#)
 - VG200 voice [10-2](#)
 - VG224 analog phone [10-4](#)
 - VG248 analog phone [10-2](#)
- summary of voice gateways (table) [10-9](#)
- trunk interfaces
 - table [10-9](#)
- gateway summary, report results [28-19](#)
- gateway utilization, report results [28-21](#)
- generating
 - event log [25-15](#)
- getProfileSoap [37-13](#)
- Global Directory
 - displaying with directories button [11-29](#)
- groups, Cisco Unified CallManager
 - configuring [5-3](#)
- groups, date/time [5-4](#)
- GSM [5-7](#)

H

H.323

- Cisco IOS gateways [10-7](#)
- clients [11-8](#)
- gateways [10-7](#)
- IOS gateway redundancy [10-17](#)
- held icon timers, configuring [14-39](#)
- hookflash transfer [10-6](#)
- Host Resources Agent service [19-8](#)
- HTML over HTTP Interfaces [37-15](#)
- hunt groups

- broadcast, understanding [14-8](#)
- circular, understanding [14-6](#)
- configuration settings (table) [14-30](#)
- configuring [14-29](#)
- deleting members [14-32](#)
- linked, understanding [14-5](#)
- understanding [14-2](#)
- viewing members [14-32](#)
- hunting
 - described [7-11](#)
 - example [7-11](#)
 - maximum hunt timer [7-12](#)
 - personal preferences [7-12](#)
- hunt lists
 - described [7-10](#)
- hunt pilots
 - described [7-10](#)
 - wildcards [7-16](#)

- image authentication [30-15](#)
- immediate divert
 - configuration checklist (table) [13-9](#)
 - described [11-24](#)
 - installing and activating [13-9](#)
 - interactions [13-6](#)
 - more information [13-11](#)
 - overview [13-1](#)
 - restrictions [13-8](#)
 - setting service parameters [13-10](#)
 - system requirements [13-2](#)
 - using [13-4](#)
- individual bill detail, report results [28-3](#)
- individual bill summary, report results [28-2](#)
- Install Changes [37-6](#)
- Integration Considerations [36-14](#)
- integrity
 - overview [30-15](#)

Interfaces [37-9](#)
 internationalization for CDR analysis and reporting [24-14](#)
 Introduction [36-1](#)
 IP
 perfmon object and counters [23-51](#)
 IP Phones
 See Cisco Unified IP Phones
 IPSec [30-12](#)
 isClusterUserSoap [37-14](#)

J

Java Example [36-10](#)
 JavaScript sample [37-19](#)
 join
 described [8-8, 11-24](#)

L

LDAP
 described [5-12](#)
 directory
 more information [9-7](#)
 overview [9-1](#)
 license capabilities assignment
 adding for multiple users [3-3](#)
 adding for one user [3-2](#)
 configuration settings (table) [3-4](#)
 configuring [3-1](#)
 finding [3-1](#)
 updating for multiple users [3-3](#)
 updating for one user [3-2](#)
 line groups
 described [7-9](#)
 load
 CDR schedule configuration [25-7](#)
 disabling CDR [25-7](#)
 restoring the default CDR schedule [25-7](#)

locations
 and regions [5-9](#)
 logon page [24-14](#)
 Log Partition Monitoring
 service [19-9](#)
 logs
 perfmon [23-62](#)

M

mail server parameters [25-2](#)
 makeCall [37-15](#)
 makeCallProxy [37-15](#)
 makeCallSoap [37-9](#)
 malicious call ID
 described [11-25](#)
 managers, CAR [24-5](#)
 manual database purge, configuration [25-12](#)
 master TFTP server
 sending files to the master TFTP server [6-9](#)
 maximum hunt timer [7-12](#)
 media encryption (*See also* encryption)
 overview [30-19](#)
 media information [28-25](#)
 Memory
 perfmon object and counters [23-52](#)
 messages button [11-28](#)
 MGCP
 gateway redundancy [10-17](#)
 MGCP BRI
 configuring [10-21](#)
 illustration of call flow [10-5](#)
 MIB2 Agent service [19-8](#)
 MLPP
 described [5-15](#)
 mode
 mixed [30-9](#)
 nonsecure [30-9](#)
 modifying files [6-10](#)

MOH

- audio files
 - deleting [12-30](#)
 - displaying [12-28](#)
 - managing [12-28](#)
 - uploading [12-29](#)
- audio sources [12-16](#)
 - configuration settings (table) [12-19](#)
 - configuring [12-18](#)
 - deleting [12-19](#)
 - explained [12-8](#)
 - finding [12-17](#)
- call park example [12-5](#)
- characteristics [12-3](#)
- configuration checklist (table) [12-14](#)
- configuring [12-23](#)
- creating audio sources [12-9](#)
- database scalability [12-7](#)
- default MOH sample [12-9](#)
- definitions [12-2](#)
- described [12-1](#)
- failover and fallback [12-13](#)
- features
 - database requirements [12-7](#)
 - database scalability [12-7](#)
 - manageability [12-7](#)
 - MOH servers [12-5](#)
 - server manageability [12-6](#)
 - server redundancy [12-6](#)
 - server scalability [12-6](#)
- fixed audio source [12-21](#)
 - configuration settings (table) [12-23](#)
 - configuring [12-22](#)
 - deleting [12-22](#)
- functionality [12-4](#)
- list of topics [12-1](#)
- managing audio sources [12-10](#)
- monitoring performance
 - overview (table) [12-15](#)
 - service states [12-16](#)
 - requirements and limits [12-12](#)
 - server configuration settings (table) [12-26](#)
- servers
 - characteristics [12-5](#)
 - configuring [12-24](#)
 - database requirements [12-7](#)
 - explained [12-8](#)
 - finding [12-23](#)
 - manageability [12-6](#)
 - perfmon counters [12-15](#)
 - redundancy [12-6](#)
 - resetting [12-25](#)
 - scalability [12-6](#)
 - storing audio sources [12-9](#)
 - supported features [12-5](#)
 - transfer hold example [12-5](#)
 - understanding [12-1](#)
 - user hold example [12-5](#)
- monitoring
 - CTI applications [18-14](#)
 - CTI devices [18-10, 18-14](#)
 - CTI lines [18-15](#)
 - gateways [18-10](#)
 - H.323 devices [18-10](#)
 - hunt list [18-10](#)
 - media resources [18-10](#)
 - performance [23-61](#)
 - phones [18-10](#)
 - predefined objects [18-7](#)
 - services [18-7](#)
 - SIP trunk [18-10](#)
 - voice-mail devices [18-10](#)
- monthly reports
 - scheduling [25-11](#)
- multicast
 - audio sources for MOH [12-10](#)
 - configuration checklist (table) [12-12](#)
 - explained [12-10](#)

Multiple Cluster Applications [37-19](#)

Multiple Clusters [37-3](#)

music on hold (MOH)

audio sources [12-8](#)

call park example [12-5](#)

characteristics [12-3](#)

configuration checklist (table) [12-14](#)

creating audio sources [12-9](#)

default MOH sample [12-9](#)

definitions [12-2](#)

described [12-1](#)

failover and fallback [12-13](#)

functionality [12-4](#)

list of topics [12-1](#)

managing audio sources [12-10](#)

monitoring performance

overview (table) [12-15](#)

service states [12-16](#)

requirements and limits [12-12](#)

servers

characteristics [12-5](#)

database requirements [12-7](#)

explained [12-8](#)

manageability [12-6](#)

perfmon counters [12-15](#)

redundancy [12-6](#)

scalability [12-6](#)

storing audio sources [12-9](#)

supported features [12-5](#)

transfer hold example [12-5](#)

understanding [12-1](#)

user hold example [12-5](#)

Control Center [19-7](#)

described [19-7](#)

starting [15-4, 19-7](#)

stopping [15-4, 19-7](#)

viewing status [15-4, 19-7](#)

New and Changed Information [36-2](#)

notification limits [26-8](#)

NT Event Viewer [16-3](#)

Number of Replicates

perfmon object and counters [23-55](#)

O

object

perfmon, described [23-1](#)

object and counters

Database Change Notification Client [23-49](#)

on-hook call transfer [11-24](#)

organization [xxiv](#)

Overview [37-2](#)

overview

automatic report generation [26-6](#)

error and event logs [24-6](#)

P

parameters

enterprise

described [5-15](#)

factoring time of day for rating [26-3](#)

factoring voice quality for rating [26-4](#)

mail server configuration [25-2](#)

service

described [5-16](#)

Maximum Phone FallBack Queue Depth [11-30](#)

setting the base rate and duration for rating [26-2](#)

system configuration [25-1](#)

Partition

N

Network Agent Adaptor service [19-8](#)

Network Interface

perfmon object and counters [23-54](#)

network services

- perfmon object and counters [23-55](#)
- Partition Support [37-6](#)
- perfmon
 - counters
 - adding [23-61](#)
 - category tabs, described [23-60](#)
 - chart [23-61](#)
 - properties [23-61](#)
 - sample rates [23-61](#)
 - zooming [23-61](#)
 - logs [23-62](#)
 - object and counters
 - Cisco Analog Access [23-3](#)
 - Cisco Annunciator Device [23-4](#)
 - Cisco CallManager [23-4](#)
 - Cisco CallManager Attendant Console [23-11](#)
 - Cisco CallManager System Performance [23-12](#)
 - Cisco CTIManager [23-15](#)
 - Cisco Dual-Mode Mobility [23-16](#)
 - Cisco Extension Mobility [23-17](#)
 - Cisco Gatekeeper [23-17](#)
 - Cisco H.323 [23-18](#)
 - Cisco Hunt Lists [23-19](#)
 - Cisco HW Conference Bridge Device [23-20](#)
 - Cisco IP Manager Assistant [23-20](#)
 - Cisco Lines [23-21](#)
 - Cisco Locations [23-21](#)
 - Cisco Media Streaming Application [23-22](#)
 - Cisco Messaging Interface [23-25](#)
 - Cisco MGCP FXO Device [23-25](#)
 - Cisco MGCP FXS Device [23-26](#)
 - Cisco MGCP Gateways [23-26](#)
 - Cisco MGCP PRI Device [23-27](#)
 - Cisco MGCP T1CAS Device [23-27](#)
 - Cisco MOH Device [23-28](#)
 - Cisco MTP Device [23-29](#)
 - Cisco Phones [23-29](#)
 - Cisco Presence Feature [23-30](#)
 - Cisco QSIG Feature [23-30](#)
 - Cisco SIP [23-30](#)
 - Cisco SIP Stack [23-31](#)
 - Cisco SW Conf Bridge Device [23-39](#)
 - Cisco TFTP Server [23-40](#)
 - Cisco Tomcat Connector [23-43](#)
 - Cisco Transcode Device [23-47](#)
 - Cisco Video Conference Bridge [23-47](#)
 - Cisco WebDialer [23-48](#)
 - Cisco WSM Connector [23-48](#)
 - Database Change Notification Server [23-50](#)
 - Database Change Notification Subscription [23-50](#)
 - Database Local DSN [23-50](#)
 - DB User Host Information [23-51](#)
 - described [23-1](#)
 - Enterprise Replication [23-51](#)
 - Enterprise Replication DBSpace Monitors [23-51](#)
 - IP [23-51](#)
 - Memory [23-52](#)
 - Network Interface [23-54](#)
 - Partition [23-55](#)
 - Process [23-56](#)
 - Processor [23-57](#)
 - System [23-58](#)
 - TCP [23-58](#)
 - Thread [23-59](#)
 - Tomcat JVM [23-45](#)
 - Tomcat Web Application [23-46](#)
- perfmon counters
 - counter descriptions (table) [12-16](#)
 - using to view MOH servers [12-15](#)
- performance monitoring
 - category tabs, described [23-60](#)
 - counters
 - adding [23-61](#)
 - chart [23-61](#)
 - properties [23-61](#)
 - zooming [23-61](#)
 - Number of Replicates [23-55](#)
 - object and counters

- Cisco Analog Access [23-3](#)
- Cisco Annunciator Device [23-4](#)
- Cisco CallManager [23-4](#)
- Cisco CallManager Attendant Console [23-11](#)
- Cisco CallManager System Performance [23-12](#)
- Cisco CTIManager [23-15](#)
- Cisco Dual-Mode Mobility [23-16](#)
- Cisco Extension Mobility [23-17](#)
- Cisco Gatekeeper [23-17](#)
- Cisco H.323 [23-18](#)
- Cisco Hunt Lists [23-19](#)
- Cisco HW Conference Bridge Device [23-20](#)
- Cisco IP Manager Assistant [23-20](#)
- Cisco Lines [23-21](#)
- Cisco Locations [23-21](#)
- Cisco Media Streaming Application [23-22](#)
- Cisco Messaging Interface [23-25](#)
- Cisco MGCP FXO Device [23-25](#)
- Cisco MGCP FXS Device [23-26](#)
- Cisco MGCP Gateways [23-26](#)
- Cisco MGCP PRI Device [23-27](#)
- Cisco MGCP T1CAS Device [23-27](#)
- Cisco MOH Device [23-28](#)
- Cisco MTP Device [23-29](#)
- Cisco Phones [23-29](#)
- Cisco Presence Feature [23-30](#)
- Cisco QSIG Feature [23-30](#)
- Cisco SIP [23-30](#)
- Cisco SIP Stack [23-31](#)
- Cisco SW Conf Bridge Device [23-39](#)
- Cisco TFTP Server [23-40](#)
- Cisco Tomcat Connector [23-43](#)
- Cisco Transcode Device [23-47](#)
- Cisco Video Conference Bridge [23-47](#)
- Cisco WebDialer [23-48](#)
- Cisco WSM Connector [23-48](#)
- Database Change Notification Server [23-50](#)
- Database Change Notification Subscription [23-50](#)
- Database Local DSN [23-50](#)
- DB User Host Information [23-51](#)
- described [23-1](#)
- Enterprise Replication [23-51](#)
- Enterprise Replication DBSpace Monitors [23-51](#)
- IP [23-51](#)
- Memory [23-52](#)
- Network Interface [23-54](#)
- Number of Replicates [23-55](#)
- Partition [23-55](#)
- Process [23-56](#)
- Processor [23-57](#)
- System [23-58](#)
- TCP [23-58](#)
- Thread [23-59](#)
- Tomcat JVM [23-45](#)
- Tomcat Web Application [23-46](#)
- sample rates [23-61](#)
- service
 - Cisco AMC Service [19-10](#)
 - Cisco CallManager Cisco IP Phone Services [19-3](#)
 - Cisco CallManager Serviceability RTMT [19-10](#)
 - Cisco CCM SNMP Service [19-6](#)
 - Cisco Extended Functions [19-3](#)
 - Cisco RIS Data Collector [19-9](#)
 - Cisco RTMT Reporter Servlet [19-10](#)
 - Cisco Serviceability Reporter [19-5](#)
- personal preferences [7-12](#)
- phone button templates
 - 12 series, default template [11-14](#)
 - 30 SP+, default template [11-13](#)
 - 30 VIP, default template [11-13](#)
 - 7902, default template [11-13](#)
 - 7905 SCCP, default template [11-13](#)
 - 7905 SIP, default template [11-13](#)
 - 7906 SCCP, default template [11-13](#)
 - 7906 SIP, default template [11-13](#)
 - 7910, default template [11-13](#)
 - 7911 SCCP, default template [11-12](#)
 - 7911 SIP, default template [11-13](#)

- 7912 SCCP, default template [11-12](#)
- 7912 SIP, default template [11-12](#)
- 7920, default template [11-12](#)
- 7940 SCCP, default template [11-12](#)
- 7940 SIP, default template [11-12](#)
- 7941 G-GE SCCP, default template [11-12](#)
- 7941 SCCP, default template [11-12](#)
- 7941 SIP, default template [11-12](#)
- 7960 SCCP, default template [11-12](#)
- 7960 SIP, default template [11-12](#)
- 7961 G-GE SCCP, default template [11-11](#)
- 7961 SCCP, default template [11-11](#)
- 7961 SIP, default template [11-11](#)
- 7970 SCCP, default template [11-11](#)
- 7970 SIP, default template [11-11](#)
- 7971 SCCP, default template [11-11](#)
- 7971 SIP, default template [11-11](#)
- 7985, default template [11-11](#)
- analog phone, default template [11-14](#)
- ATA 186, default template [11-14](#)
- Cisco IP Communicator, default template [11-14](#)
- Cisco TelePresence, default template [11-14](#)
- CN622, default template [11-14](#)
- conference station 7935, default template [11-13](#)
- conference station 7936, default template [11-13](#)
- IP-STE, default template [11-14](#)
- ISDN BRI Phone, default template [11-14](#)
- third-party SIP device, default template [11-14](#)
- VGC phone, default template [11-14](#)
- VGC Virtual, default template [11-14](#)
- phone NTP reference
 - configuring for SIP phones [5-4](#)
- phones
 - See also* Cisco Unified IP Phones
 - administration tips [11-27](#)
 - associating with users [11-27](#)
 - button templates
 - default [11-10](#)
 - described [11-10](#)
 - guidelines [11-14](#)
 - listed by model (table) [11-11](#)
 - common phone profiles [11-20](#)
 - dependency records
 - described [11-30](#)
 - failover and fallback [11-30](#)
 - features
 - described (table) [11-15](#)
 - privacy [11-21](#)
 - find all phones [11-28](#)
 - methods for adding [11-20](#)
 - more information [11-35](#)
 - SCCP configuration checklist (table) [11-31](#)
 - search by authentication string [11-28](#)
 - search by calling search space [11-27](#)
 - search by call pickup group [11-28](#)
 - search by description [11-27](#)
 - search by device name [11-27](#)
 - search by device pool [11-27](#)
 - search by device protocol [11-28](#)
 - search by device type [11-28](#)
 - search by directory number [11-27](#)
 - search by LSC status [11-28](#)
 - search by security profile [11-28](#)
 - search tips [11-27](#)
 - search within results [11-28](#)
 - SIP configuration checklist (table) [11-31](#)
 - softkey templates
 - add application [11-17](#)
 - configure softkey layout [11-18](#)
 - described [11-16](#)
- pilot points
 - associating with the ac user [14-28](#)
 - configuration settings [14-25](#)
 - configuring [14-24](#)
 - deleting [14-27](#)
 - finding [14-23](#)
 - resetting [14-28](#)
 - understanding [14-2](#)

platform services

- Cisco CDP Agent [19-8](#)
- Cisco Certificate Expiry Monitor Service [19-8](#)
- Cisco DB [19-7](#)
- Cisco Electronic Notification [19-8](#)
- Cisco License Manager [19-8](#)
- Cisco Syslog Agent [19-8](#)
- Cisco Tomcat [19-7](#)
- Host Resources Agent [19-8](#)
- MIB2 Agent [19-8](#)
- Network Agent Adaptor [19-8](#)
- SNMP Master Agent [19-8](#)

polling intervals

- sample rate [23-61](#)

polling rate [18-13](#)

port

- CTL Provider [31-5](#)
- Ethernet phone [31-5](#)
- SIP secure [31-5](#)

ports

- CTI
 - described [11-8](#)

predefined objects

- monitoring [18-7](#)

preferences

- system configuration [25-6](#)

presentation settings

- calling party [7-29](#)
- connected party [7-31](#)

privacy

- described [11-21](#)

Process

- perfmon object and counters [23-56](#)

Processor

- perfmon object and counters [23-57](#)

profiles

- common phone [11-20](#)

protocols

- Skinnny Client Control Protocol [10-3](#)

Skinnny Client Control Protocol (SCCP) Gateway Protocol [10-17](#)Skinnny Gateway Protocol [10-16](#)

purge

- automatic database configuration [25-14](#)
- disabling automatic database [25-14](#)
- restoring database defaults [25-12](#)

Q

QoS

- default values [26-5](#)
- defining values [26-5](#)
- notification limits configuration [26-8](#)

QoS by call types, report results [28-11](#)QoS by gateway, report results [28-11](#)QoS detail, report results [28-9](#)QoS summary, report results [28-11](#)Q signaling (QSIG) [10-1](#)QSIG trunk interface [10-1](#)

quality report tool

- described [11-25](#)

R
rating engine, configuration [26-1](#)

rating parameters

- factoring time of day [26-3](#)
- factoring voice quality [26-4](#)
- setting the base rate and duration [26-2](#)

Real-Time Monitoring Tool

alerts

- notification for a counter [23-61](#)

category

- adding [18-17](#)
- deleting [18-18](#)
- renaming [18-17](#)

category tabs, described [23-60](#)

configuration profile

- adding [18-5](#)
- deleting [18-6](#)
- restoring [18-6](#)
- using default [18-5](#)
- counters
 - adding [23-61](#)
 - alert notification [23-61](#)
 - chart [23-61](#)
 - monitor [23-61](#)
- e-mail notification, configuring [18-4](#)
- finding
 - CTI applications [18-14](#)
 - CTI devices [18-14](#)
 - CTI lines [18-15](#)
 - devices [18-10](#)
- installing [18-1](#)
- list of topics [22-1](#)
- loading [18-3](#)
- logging and report generation
 - call log [22-9](#)
 - device log [22-13](#)
 - server log [22-7](#)
 - service log [22-11](#)
- monitoring
 - call processing [18-7](#)
 - CTIManager [18-7](#)
 - devices [18-7](#)
 - predefined objects [18-7](#)
 - server [18-7](#)
 - services [18-7](#)
 - summary [18-7](#)
- monitoring predefined objects [18-7](#)
- monitoring summary [18-7](#)
- overview [22-1](#)
- polling interval [23-61](#)
- polling rate, configuring [18-13](#)
- sample rate [23-61](#)
- service
 - Cisco AMC Service [19-10](#)
 - Cisco CallManager Serviceability RTMT [19-10](#)
 - Cisco RTMT Reporter Servlet [19-10](#)
 - Cisco Syslog Agent [19-8](#)
 - uninstalling [18-2](#)
 - using [18-3](#)
 - viewing
 - CTIManager information [18-14](#)
 - device properties [18-12](#)
 - phone information [18-12](#)
 - view tab
 - summary [22-6](#)
 - window components [22-3](#)
 - zooming a counter [23-61](#)
- Redirector Servlet [37-2](#)
- redundancy
 - Cisco Unified CallManager Attendant Console [14-11](#)
 - Cisco VG248 [10-18](#)
 - IOS H.323 gateways [10-17](#)
 - MGCP gateway [10-17](#)
 - MOH servers [12-6](#)
 - support for gateways [10-17](#)
- regions
 - adding [2-3](#)
 - and call admission control [5-9](#)
 - and locations [5-9](#)
 - configuration settings (table) [2-5](#)
 - configuring [2-1](#)
 - deleting [2-7](#)
 - described [5-5](#)
 - example (figure) [5-9](#)
 - finding [2-1](#)
- related documentation [xxv](#)
- report
 - CDR search [27-1](#)
 - CDR search by cause for call termination [27-4](#)
 - CDR search by gateway [27-3](#)
 - CDR search by user extension [27-1](#)
- report configuration, CAR [26-1](#)
- report results

- CDR error [28-17](#)
- CDR search by user extension [28-23](#)
- Cisco IP Phone services [28-9](#)
- conference bridge utilization [28-22](#)
- conference call detail [28-21](#)
- department bill, detail [28-3](#)
- department bill, summary [28-2](#)
- gateway detail [28-18](#)
- gateway summary [28-19](#)
- gateway utilization [28-21](#)
- individual bill, detail [28-3](#)
- individual bill, summary [28-2](#)
- QoS by gateway [28-11](#)
- QoS detail [28-9](#)
- QoS report by call types [28-11](#)
- QoS summary [28-11](#)
- route group utilization [28-21](#)
- route list utilization [28-21](#)
- route pattern utilization [28-21](#)
- system overview [28-16](#)
- top N by charge [28-4](#)
- top N by duration [28-4](#)
- top N by number of calls [28-5](#)
- traffic summary [28-12](#)
- traffic summary by extensions [28-12](#)
- voice mail utilization [28-23](#)
- Reports
 - CAR report results [28-1](#)
- reports
 - automatic generation configuration [26-6](#)
 - automatic report generation/alert [26-6](#)
 - customizing for automatic generation [24-11, 26-7](#)
 - enabling for automatic generation [24-11, 26-7](#)
 - overview [24-15](#)
 - perfmon logs [23-62](#)
 - scheduling daily [25-9](#)
 - scheduling monthly [25-11](#)
 - scheduling weekly [25-10](#)
 - system overview results [28-16](#)
 - user, CAR [24-7](#)
- restore
 - service
 - Cisco DRF Local [19-11](#)
 - Cisco DRF Master [19-11](#)
- restoring
 - CAR database purge defaults [25-12](#)
 - default CDR load schedule [25-7](#)
- restriction settings
 - calling party [7-29](#)
 - connected party [7-31](#)
- Results [37-10](#)
- route
 - group utilization, report results [28-21](#)
 - list utilization, report results [28-21](#)
 - pattern utilization, report results [28-21](#)
- route filters
 - associated with route lists (table) [7-35](#)
 - described [7-35](#)
- route groups
 - described [7-5](#)
 - generated [7-36](#)
 - related to dial plans [10-16](#)
- route lists
 - associated route filters (table) [7-35](#)
 - described [7-5](#)
 - generated [7-36](#)
 - types (table) [7-37](#)
 - types, example [7-5](#)
- route patterns
 - closest-match routing [7-12](#)
 - considerations for using [7-6](#)
 - explained [7-6](#)
 - fields in Cisco Unified CallManager (table) [7-18](#)
 - generated with external route plan wizard [7-37](#)
 - usage [7-6](#)
 - using the @ wildcard character [7-13](#)
 - wildcards [7-16](#)
- route plans

- and Cisco Analog Access Gateways (figure) [7-9](#)
- and Cisco Digital Access Gateways (figure) [7-8](#)
- external route plan wizard
 - generated route filters [7-35](#)
 - generated route groups [7-36](#)
 - generated route lists [7-36](#)
 - generated route patterns [7-37](#)
- list of topics [7-1](#)
- more information [7-38](#)
- overview [7-4](#)
- report [7-38](#)
- routing
 - automated alternate [7-1](#)
 - closest-match [7-12](#)

S

- sample rate [23-61](#)
- schedule
 - CDR load configuration [25-7](#)
 - restoring the default CDR load [25-7](#)
- scheduling
 - daily reports [25-9](#)
 - monthly reports [25-11](#)
 - weekly reports [25-10](#)
- search
 - by authentication string [11-28](#)
 - by calling search space [11-27](#)
 - by call pickup group [11-28](#)
 - by description [11-27](#)
 - by device name [11-27](#)
 - by device pool [11-27](#)
 - by device protocol [11-28](#)
 - by device type [11-28](#)
 - by directory number [8-8, 11-27](#)
 - by LSC status [11-28](#)
 - by security profile [11-28](#)
 - CDR by cause for call termination [27-4](#)
 - CDR by gateway [27-3](#)
 - CDR by user extension [27-1](#)
 - CDR by user extension, report results [28-23](#)
 - CDRs [27-1](#)
 - for all directory numbers in the database [8-9](#)
 - for all phones in the database [11-28](#)
 - for directory numbers [8-8](#)
 - for phones [11-27](#)
 - within results [11-28](#)
- secure sockets layer (SSL)
 - installing [30-12](#)
- security
 - authentication overview [30-15](#)
 - authorization overview [30-15](#)
 - best practices [30-10](#)
 - certificate types [30-12](#)
 - configuration checklist for authentication and encryption (table) [30-22](#)
 - CTL client overview [31-2](#)
 - encryption overview [30-19](#)
 - external CAs [30-12](#)
 - features list [30-4](#)
 - features list (table) [30-5](#)
 - installing [30-12](#)
 - interactions [30-5](#)
 - rebooting the cluster [30-10](#)
 - rebooting the server [30-10](#)
 - resetting devices [30-10](#)
 - restarting Cisco Unified CallManager service [30-10](#)
 - restrictions [30-5, 30-6](#)
 - service
 - Cisco Certificate Authority Proxy Function (CAPF) [19-6](#)
 - Cisco CTL Provider [19-6](#)
 - system requirements [30-4](#)
 - terminology (table) [30-2](#)
 - tokens [31-2, 31-6, 31-8, 31-10, 31-16](#)
 - using barge with encryption [30-11](#)
 - where to find more information [30-25](#)
- security mode

- clusterwide
 - configuring [31-12](#)
 - verifying [31-15](#)
- restrictions
 - cluster and device modes [30-9](#)
- security profile
 - applying to phones [32-9](#)
 - configuration settings (table)
 - for SCCP phone [32-4](#)
 - for SIP phones [32-6](#)
 - configuration tips for phones [32-1](#)
 - configuring for phones [32-3](#)
 - deleting for phones [32-10](#)
 - finding for phones [32-2](#)
 - finding phones that use [32-11](#)
 - overview for phones [32-1](#)
 - search for phones [11-28](#)
- server, Cisco Unified CallManager
 - configuring [5-1](#)
- server, mail parameters [25-2](#)
- service
 - A Cisco DB [19-7](#)
 - A Cisco DB Replicator [19-7](#)
 - Cisco AMC Service [19-10](#)
 - Cisco Analyzer [19-4](#)
 - Cisco AXL Web Service [19-5](#)
 - Cisco Bulk Provisioning Service [19-5](#)
 - Cisco CallManager [19-2](#)
 - Cisco CallManager Admin [19-9](#)
 - Cisco CallManager Attendant Console Server [19-3](#)
 - Cisco CallManager Cisco IP Phone Services [19-3](#)
 - Cisco CallManager Personal Directory [19-9](#)
 - Cisco CallManager Serviceability [19-9](#)
 - Cisco CallManager Serviceability RTMT [19-10](#)
 - Cisco CAR Scheduler [19-5](#)
 - Cisco CAR Web Service [19-5](#)
 - Cisco CCM SNMP Service [19-6](#)
 - Cisco CDP [19-9](#)
 - Cisco CDP Agent [19-8](#)
 - Cisco CDR Agent [19-11](#)
 - Cisco Certificate Authority Proxy Function (CAPF) [19-6](#)
 - Cisco Certificate Expiry Monitor [19-8](#)
 - Cisco CTIManager [19-3](#)
 - Cisco CTL Provider [19-6](#)
 - Cisco Database Layer Monitor [19-8](#)
 - Cisco DHCP Monitor Service [19-4](#)
 - Cisco DirSync [19-7](#)
 - Cisco DRF Local [19-11](#)
 - Cisco DRF Master [19-11](#)
 - Cisco Electronic Notification [19-8](#)
 - Cisco Extended Functions [19-3](#)
 - Cisco Extension Mobility Application [19-10](#)
 - Cisco IP Manager Assistant [19-4](#)
 - Cisco IP Voice Media Streaming App [19-3](#)
 - Cisco License Manager [19-8](#)
 - Cisco Log Partition Monitoring Tool [19-9](#)
 - Cisco Messaging Interface [19-3](#)
 - Cisco RIS Data Collector [19-9](#)
 - Cisco RTMT Reporter Servlet [19-10](#)
 - Cisco Serviceability Reporter [19-5](#)
 - Cisco SOAP - CDRonDemand Service [19-4](#)
 - Cisco SOAP-Log Collection APIs [19-10](#)
 - Cisco SOAP Performance Monitoring APIs [19-10](#)
 - Cisco Syslog Agent [19-8](#)
 - Cisco TFTP [19-3](#)
 - Cisco Tomcat [19-7](#)
 - Cisco Tomcat Stats Servlet [19-10](#)
 - Cisco Trace Collection Service [19-9](#)
 - Cisco Trace Collection Servlet [19-9](#)
 - Cisco WebDialer Web Service [19-4](#)
 - configuration checklist (table) [19-13](#)
 - Control Center, described [19-12](#)
 - feature services [19-1](#)
 - Host Resources Agent [19-8](#)
 - MIB2 Agent [19-8](#)
 - Native Agent Adaptor [19-8](#)
 - network services [19-7](#)

- SNMP Master Agent [19-8](#)
- starting services, described [19-12](#)
- stopping services, described [19-12](#)
- viewing service status, described [19-12](#)
- service activation
 - activating [15-1](#)
 - deactivating [15-1](#)
 - multiserver recommendations (table) [15-2](#)
- service parameter
 - CFA Destination Override [8-6, 11-22](#)
- service parameters
 - Automated Alternate Routing Enable [7-3](#)
 - described [5-16](#)
 - Maximum Phone FallBack Queue Depth [11-30](#)
- services
 - activating [15-1](#)
 - deactivating [15-1](#)
 - monitoring [18-7](#)
 - starting [15-4](#)
 - stopping [15-4](#)
 - viewing status [15-4](#)
- service URL
 - described [11-26](#)
- settings
 - called party transformations
 - configuring [7-28](#)
 - explained (table) [7-28](#)
 - calling party transformations
 - explained (table) [7-27, 7-30](#)
 - configuring
 - checklist (table) [5-17](#)
 - described [5-1](#)
 - connected party transformations
 - explained (table) [7-32](#)
 - special characters [7-16](#)
- shared line appearance
 - active check box [8-5](#)
 - described [8-2](#)
 - restrictions [8-4](#)
 - update directory number of all devices sharing this line
 - check box [8-5](#)
- signaling authentication
 - overview [30-15](#)
- signaling encryption
 - overview [30-19](#)
- signaling protocols, gateway [10-9](#)
- Simple Network Management Protocol
 - service
 - Cisco CCM SNMP Service [19-6](#)
 - Cisco CDP Agent [19-8](#)
 - Host Resources Agent [19-8](#)
 - MIB2 Agent [19-8](#)
 - Network Agent Adaptor [19-8](#)
 - SNMP Master Agent [19-8](#)
- SIP
 - configuration differences [4-1](#)
 - configuring third-party devices [4-1](#)
 - third-party SIP phone configuration checklist
 - (table) [4-4](#)
 - third-party SIP phones and TFTP [4-2](#)
- SIP phone
 - NTP reference [5-4](#)
- SIP phones
 - enabling digest authentication
 - third-party phones [4-2](#)
 - See* Cisco SIP IP Phones
- Site Administrator Security Token (SAST) [31-2](#)
- Skinny Client Control Protocol [10-3](#)
- Skinny Client Control Protocol (SCCP) Gateway Protocol [10-17](#)
- Skinny Gateway Protocol [10-16](#)
- SNMP
 - service
 - Cisco CCM SNMP Service [19-6](#)
 - Cisco CDP [19-9](#)
 - Cisco CDP Agent [19-8](#)
 - Host Resources Agent [19-8](#)
 - MIB2 Agent [19-8](#)
 - Network Agent Adaptor [19-8](#)

SNMP Master Agent [19-8](#)

SNMP Master Agent service [19-8](#)

SOAP

- service
 - Cisco SOAP - CDRonDemand Service [19-4](#)
 - Cisco SOAP-Log Collection APIs [19-10](#)
 - Cisco SOAP Performance Monitoring APIs [19-10](#)

SOAP over HTTP Interface [37-9](#)

softkey templates

- call states described (table) [11-18](#)
- layout (figure) [11-19](#)
- operation [11-19](#)

softphone [11-9](#)

special characters

- configuring [7-16](#)
- described (table) [7-17](#)
- explained [7-16](#)

speed dial

- described [11-26](#)

static digit analysis

- caveats [7-15](#)
- configuration tip [7-14](#)
- described [7-14](#)
- example prior to static digit analysis [7-15](#)
- explained [7-14](#)
- Unified CallManager Assistant example with static digit analysis [7-16](#)

summary

- department bill, report results [28-2](#)
- gateway, report results [28-19](#)
- individual bill, report results [28-2](#)
- QoS, report results [28-11](#)
- traffic, report results [28-12](#)
- traffic by extensions, report results [28-12](#)

System

- perfmon object and counters [23-58](#)

system, CAR [24-6](#)

system-level configuration settings [5-1](#)

system log screens

CAR [25-15](#)

system overview, report results [28-16](#)

system parameters, configuration [25-1](#)

system preferences

- configuration [25-6](#)

system preferences parameters for CAR [25-6](#)

system reports, CAR [24-8](#)

T

T1 Primary Rate Interface (PRI) [10-1](#)

table, CDR and CMR dump [28-25](#)

Target Audience for this Chapter [36-2](#)

TCP

- perfmon object and counters [23-58](#)

templates, phone button

- 12 series, default [11-14](#)
- 30 SP+, default [11-13](#)
- 30 VIP, default [11-13](#)
- 7902, default [11-13](#)
- 7905 SCCP, default [11-13](#)
- 7905 SIP, default [11-13](#)
- 7906 SCCP, default [11-13](#)
- 7906 SIP, default [11-13](#)
- 7910, default [11-13](#)
- 7911 SCCP, default [11-12](#)
- 7911 SIP, default [11-13](#)
- 7912 SCCP, default [11-12](#)
- 7912 SIP, default [11-12](#)
- 7920, default [11-12](#)
- 7940 SCCP, default [11-12](#)
- 7940 SIP, default [11-12](#)
- 7941 G-GE SCCP, default [11-12](#)
- 7941 SCCP, default [11-12](#)
- 7941 SIP, default [11-12](#)
- 7960 SCCP, default [11-12](#)
- 7960 SIP, default [11-12](#)
- 7961 G-GE SCCP, default [11-11](#)
- 7961 SCCP, default [11-11](#)

- 7961 SIP, default [11-11](#)
- 7970 SCCP, default [11-11](#)
- 7970 SIP, default [11-11](#)
- 7971 SCCP, default [11-11](#)
- 7971 SIP, default [11-11](#)
- 7985, default [11-11](#)
- analog phone, default [11-14](#)
- ATA 186, default [11-14](#)
- Cisco IP Communicator, default [11-14](#)
- Cisco TelePresence, default [11-14](#)
- CN622, default [11-14](#)
- conference station 7935, default [11-13](#)
- conference station 7936, default [11-13](#)
- default [11-10](#)
- described [11-10](#)
- guidelines [11-14](#)
- IP-STE, default [11-14](#)
- ISDN BRI phone, default [11-14](#)
- listed by model (table) [11-11](#)
- third-party SIP device, default [11-14](#)
- VGC phone, default [11-14](#)
- VGC Virtual, default [11-14](#)
- templates, softkey
 - add application [11-17](#)
 - configure softkey layout [11-18](#)
 - described [11-16](#)
 - layout (figure) [11-19](#)
 - operation [11-19](#)
- TFTP [6-9](#)
 - alternate Cisco file server fields [6-8](#)
 - alternate Cisco file servers [6-8](#)
 - centralized TFTP [6-9, 6-10](#)
 - configuration checklist (table) [6-11](#)
 - configuration tips
 - alternate Cisco file server fields [6-10](#)
 - configuring a redundant or load-sharing TFTP server [6-8](#)
 - customizing files [6-10](#)
 - list of topics [6-1](#)
 - master TFTP server [6-9](#)
 - more information [6-11](#)
 - multiple cluster environment [6-9](#)
 - overview [6-1](#)
 - process overview for Cisco SIP IP phones [6-2](#)
 - process overview for SCCP devices [6-2](#)
 - server
 - accessing [6-6](#)
 - identifying [6-6](#)
 - third-party SIP phones [4-2](#)
 - understanding [6-4](#)
- TFTP services [31-2](#)
- Thread
 - perfmon object and counters [23-59](#)
- Throttling Requests [36-12](#)
- time of day [26-3](#)
- time zones [5-4](#)
- TLS Proxy server [31-2](#)
- Tomcat JVM
 - perfmon object and counters [23-45](#)
- Tomcat Web Application
 - perfmon object and counters [23-46](#)
- top N
 - by charge, report results [28-4](#)
 - by duration, report results [28-4](#)
 - by number of calls, report results [28-5](#)
- top N by charge, report results [28-4](#)
- top N by duration, report results [28-4](#)
- top N by number of calls, report results [28-5](#)
- Trace
 - configuration
 - described [21-2](#)
 - configuration and collection checklist [21-4](#)
 - list of topics [21-1](#)
 - overview [21-1](#)
 - trace and log central
 - described [21-3](#)
 - troubleshooting trace setting
 - described [21-2](#)

traffic summary, report results [28-12](#)
 traffic summary by extensions, report results [28-12](#)
 transfer
 described [8-7](#)
 on-hook [11-24](#)
 transfer hold, example with MOH [12-5](#)
 transformations
 called party [7-26](#)
 calling party [7-26](#)
 translation patterns
 and called party transformations settings [7-28](#)
 and calling party presentation and restriction settings [7-29](#)
 and calling party presentation settings (table) [7-30](#)
 and connected party presentation and restriction settings [7-31](#)
 and connected party presentation settings (table) [7-32](#)
 and route plan report [7-38](#)
 use for failover [7-14](#)
 transport layer security (TLS) [30-12](#)
 port [31-5](#)
 transport security
 and real-time protocol (RTP) [30-12](#)
 and secure real-time protocol (SRTP) [30-12](#)
 configuration settings (table)
 for SCCP phone [32-4](#)
 for SIP phone [32-6](#)
 configuring for SIP phones [32-3](#)
 IPSec [30-12](#)
 TLS [30-12](#)
 Trivial File Transfer Protocol (TFTP) [6-1](#)
 troubleshooting
 deleting CTL file on phone [31-16](#)
 Troubleshooting Trace Setting
 configuration [17-1](#)
 trunk interfaces
 E1 PRI [10-1](#)
 FXO [10-1](#)
 FXS [10-1](#)

QSIG [10-1](#)
 T1 CAS [10-1](#)
 T1 PRI [10-1](#)

U

unicast
 audio sources for MOH [12-10](#)
 explained [12-10](#)
 uninhibited loading of CDR values [25-8](#)
 user
 configure phone features [11-29](#)
 user hold, example with MOH [12-5](#)
 user options
 Cisco Unified CallManager User Options [11-29](#)
 user reports, CAR [24-7](#)
 users
 Cisco Unified CallManager Attendant Console
 configuring [14-18](#)
 understanding [14-2](#)
 users, CAR [24-5](#)
 using [25-12](#)
 utilization
 conference bridge, report results [28-22](#)
 gateway, report results [28-21](#)
 route group, report results [28-21](#)
 route list, report results [28-21](#)
 voice mail, report results [28-23](#)

V

video phones
 Cisco Unified IP Phone 7985 [11-6](#)
 voice codecs
 bandwidth used per call (table) [5-8](#)
 G.711 [5-7](#)
 G.723 [5-7](#)
 G.729 [5-7](#)

GSM [5-7](#)

supported by Cisco Unified CallManager [5-7](#)

wideband [5-7](#)

voice gateways

See gateways

voice mail

configuring messages button [11-28](#)

voice mail utilization, report results [28-23](#)

voice quality [26-4](#)

W

WebDialer

Servlet [37-2](#)

Single Cluster Applications [37-19](#)

SIP Support [37-6](#)

Support for Enhancements in CTI and JTAPI [37-4](#)

Using the Redirector Servlet [37-3](#)

WSDL [37-16](#)

weekly reports

scheduling [25-10](#)

wideband [5-7](#)

wildcards

described (table) [7-17](#)

for hunt pilots [7-16](#)

for route patterns [7-16](#)

using @ in route patterns [7-13](#)

Z

zooming a counter [23-61](#)

