Cisco Intercompany Media Engine Installation and Configuration Guide

Release 8.6(1)

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

Text Part Number: OL-24962-01

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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

Cisco Intercompany Media Engine Installation and Configuration Guide
© 2011 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface ix

Overview 1-1

- Features and Benefits 1-1
- How It Works 1-2
  - Validation Rules 1-4
  - PSTN Fallback 1-5
- Components 1-6
- Deployment Models 1-8
  - Basic Deployment 1-8
  - Off-path Deployment 1-9
- Related Topics 1-10

Installation and Cisco IME Server Configuration 2-1

- Important Considerations 2-1
- Frequently Asked Questions About the Installation 2-2
  - How Much Time Does the Installation Require? 2-2
  - What User Names and Passwords Do I Need to Specify? 2-2
  - What is a Strong Password? 2-3
  - What is the Cisco Unified Communications Answer File Generator? 2-3
  - Which Servers Does Cisco Support for this Installation? 2-4
  - Which SFTP Servers Does Cisco Support? 2-4
  - May I Install Other Software on the Server? 2-4
- Pre-Installation Tasks 2-5
  - Allowing Network Traffic 2-6
  - Obtaining a License File 2-8
  - Gathering Information for an Installation 2-9
- Starting the Installation 2-13
- Post-Installation Tasks 2-17
  - Uploading a License File 2-22
  - Certificate Purchase and Enrollment 2-22
  - Manually Renewing a Cisco Intercompany Media Engine Certificate 2-24
- Resetting Administrator and Security Passwords 2-25
- Upgrading Cisco Intercompany Media Engine Software 2-26
- Troubleshooting Installation 2-27

Handling Network Errors During Installation 2-27
Examining Log Files 2-28
Related Topics 2-28

Cisco IME Configuration in Cisco Unified Communications Manager Administration 3-1

Cisco Unified Communications Manager Administration Basics 3-2
Using the Cisco Unified Communications Manager Administration Graphical User Interface 3-2
Using Cisco Unified Communications Manager Administration Help 3-3
Finding and Deleting Records 3-3
Adding and Copying Records 3-5
Cisco IME Configuration Checklist 3-6
Configuring Cisco IME Server Connections 3-14
Setting Up TLS Connections Between the Cisco Unified Communications Manager and Cisco Intercompany Media Engine Servers 3-16
Generating and Uploading a Self-Signed Certificate on the Cisco Intercompany Media Engine Server 3-17
Generating and Uploading Third Party Certificates for Cisco Intercompany Media Engine 3-18
Configuring a Cisco IME Enrolled Group 3-19
Configuring a Cisco IME Enrolled Pattern 3-21
Configuring a Cisco IME Exclusion Group 3-22
Configuring a Cisco IME Exclusion Number 3-23
Configuring a Cisco IME Trust Group 3-24
Configuring a Cisco IME Trust Element 3-25
Configuring a Cisco IME Service 3-26
Configuring External IP Address and Port Information 3-28
Configuring Transformation Patterns for Cisco IME 3-29
Configuring a Cisco IME Transformation Profile 3-30
Configuring Cisco IME E.164 Transformations 3-35
Configuring PSTN Access Trunks 3-36
Configuring a Cisco IME Feature Configuration 3-37
Verifying Connectivity 3-40
Registration Status 3-41
Vservice Publication 3-42
DID Publication 3-42
Configuring a Fallback Profile 3-43
Configuring Fallback Feature Parameters 3-47
Configuring Intercompany Media Services Firewall Information 3-49
Cisco Intercompany Media Engine Learned Routes 3-49

Related Topics 3-50

Cisco ASA Configuration 4-1

Proxy Configuration Guidelines and Limits 4-1

Proxy CLI configuration 4-2

Task Flow for Configuring Cisco Intercompany Media Engine 4-3

Configuring NAT for Cisco Intercompany Media Engine Proxy 4-4

Configuring PAT for the Cisco UCM Server 4-5

Creating Access Lists for Cisco Intercompany Media Engine Proxy 4-7

Creating the Media Termination Instance 4-8

Creating the Cisco Intercompany Media Engine Proxy 4-10

Creating Trustpoints and Generating Certificates 4-13

Creating the TLS Proxy 4-16

Enabling SIP Inspection for the Cisco Intercompany Media Engine Proxy 4-17

(Optional) Configuring TLS within the Local Enterprise 4-19

(Optional) Configuring Off Path Signaling 4-22

Proxy Configuration using ASDM 4-24

Configuring the Cisco UC-IMC Proxy by using the UC-IME Proxy Pane 4-24

Configuring the Cisco UC-IMC Proxy by using the Unified Communications Wizard 4-26

Backing up and Restoring the Cisco IME Server 5-1

Quick-Reference Tables for Backup and Restore Procedures 5-2

Backup Quick Reference 5-2

Restore Quick Reference 5-2

System Requirements 5-3

How to Access the Disaster Recovery System 5-3

Master Agent Duties and Activation 5-4

Local Agents 5-4

Managing Backup Devices 5-4

Creating Backup Schedules 5-5

Enabling, Disabling, and Deleting Schedules 5-6

Starting a Manual Backup 5-6

Checking Backup Status 5-7

Displaying Backup Files 5-7

Restoring a Server 5-8

Viewing the Restore Status 5-9

Trace Files 5-10

Error Messages 5-10

Managing Services on the Cisco Intercompany Media Engine Server 6-1

Services 6-1

Service Descriptions 6-1

Performance and Monitoring Services 6-2

Backup and Restore Services 6-2

System Services 6-3

Platform Services 6-3

Service Configuration Checklist 6-4

Working with Services 6-5

Alarms 6-6

Traces 6-8

Configuring Trace 6-9

Collecting Traces 6-10

Related Topics 6-11

Using RTMT with Cisco Intercompany Media Engine 7-1

Installing RTMT 7-1

Uninstalling RTMT 7-3

Launching RTMT 7-3

Navigating RTMT 7-4

Monitoring Predefined Cisco Intercompany Media Engine Objects in RTMT 7-5

Monitoring the Intercompany Media Services Predefined Object on the Cisco Unified Communications Manager Server 7-6

Monitoring Objects on the Cisco IME Server 7-7

Monitoring IME Service 7-7

Monitoring IME System Performance 7-8

Working with Trace and Log Central 7-8

Related Topics 7-8

Generating the Cisco IME Client Call Activity Report 8-1

Configuring SNMP on the Cisco IME Server 9-1

SNMP Configuration Checklist 9-1

SNMP Users 9-3

SNMP Trap Notification Destinations 9-4

SNMP Inform Notification Destination 9-5

MIB2 System Group 9-7

SNMP Management Information Base (MIB) 9-8

Related Topics 9-11

Troubleshooting 10-1

System History Log 10-1

System History Log Overview 10-1

System History Log Fields 10-2

Accessing the System History Log 10-3

Audit Logging 10-4

Configuring Audit Logging 10-6

Netdump Utility 10-8

Configuring a Netdump Server 10-8

Configuring a Netdump Client 10-9

Working with Files That Are Collected by the Netdump Server 10-9

Monitoring Netdump Status 10-9

Cisco Intercompany Media Engine Performance Objects and Counters 11-1

IME Configuration Manager 11-2

IME Server 11-2

IME Server System Performance 11-4

IME Client 11-5

IME Client Instance 11-7

Related Topics 11-7

Cisco Intercompany Media Engine Alert Descriptions and Default Settings 12-1

BannedFromNetwork 12-2

IMEDistributedCacheCertificateExpiring 12-2

IMEDistributedCacheFailure 12-3

IMESdlLinkOutOfService 12-4

InvalidCertificate 12-5

InvalidCredentials 12-5

MessageOfTheDay 12-6

SWUpdateRequired 12-6

TicketPasswordChanged 12-7

ValidationsPendingExceeded 12-8

IMEDistributedCacheInactive 12-9

IMEQualityAlert 12-10

InsufficientFallbackIdentifiers 12-11

IMEServiceStatus 12-12

InvalidCredentials 12-13

TCPSetupToIMEFailed 12-13

TLSConnectionToIMEFailed 12-14

Related Topics 12-15

INDEX

Preface

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

Note The PDF of the entire book represents a snapshot of the information that is available when the book is first published. The book PDF does not necessarily reflect subsequent updates to the content.

Chapters that contain updates use a (Revised mm/dd/yyyy) indicator that follows the chapter title. Consult the HTML and PDF versions of those chapters for the latest content.

You can obtain the most current version of this book at this URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/ime/8_0_2/ime802.html or
http://www.cisco.com/en/US/docs/voice_ip_comm/cucmbe/ime/8_0_2/ime802.html

The preface covers these topics:

- Purpose, page ix
- Audience, page x
- Organization, page x
- Related Documentation, page xi
- Conventions, page xi
- Obtaining Documentation and Submitting a Service Request, page xiii

Purpose

This document provides instructions for installing and administering the Cisco Intercompany Media Engine (Cisco IME). This guide includes descriptions of procedural tasks that you complete by using Cisco Unified Communications Manager Administration and the Cisco IME command line interface.

Audience

This guide provides information for network administrators who are responsible for managing the Cisco Unified Communications Manager system. This guide requires knowledge of telephony and IP networking technology.

Organization

The following table provides the organization of this guide.

Chapter	Description
Chapter 1	"Overview" Contains general information about the Cisco Intercompany Media Engine feature and describes how the feature establishes direct IP connectivity between enterprises.
Chapter 2	"Installation and Cisco IME Server Configuration" Contains information on installing and configuring the Cisco Intercompany Media Engine server.
Chapter 3	"Cisco IME Configuration in Cisco Unified Communications Manager Administration" Contains information on how to configure the Cisco Intercompany Media Engine feature in Cisco Unified Communications Manager Administration.
Chapter 4	"Cisco ASA Configuration" Contains information on configuring ASA using the command-line interface, as well as the ASDM, a web-based GUI application.
Chapter 5	"Backing up and Restoring the Cisco IME Server" Contains information on performing backup- and restore-related tasks on the Cisco Intercompany Media Engine server.
Chapter 6	"Managing Services on the Cisco Intercompany Media Engine Server" Contains information on the available services on the Cisco Intercompany Media Engine server.
Chapter 7	"Using RTMT with Cisco Intercompany Media Engine" Contains descriptions and step-by-step instructions for installing and using the Real Time Monitoring Tool.
Chapter 8	"Generating the Cisco IME Client Call Activity Report" Contains information on how to generate the Cisco IME Client Call Activity Report in Cisco Unified Serviceability.
Chapter 9	"Configuring SNMP on the Cisco IME Server" Contains procedures for configuring SNMP version 3, configuring SNMP trap and inform parameters, and configuring the system contact and system location objects for the MIB-II system group. Administrators use SNMP to troubleshoot and to perform diagnostics and network management tasks.

Chapter	Description
Chapter 10	"Troubleshooting" Contains information on tools to help you to troubleshoot the Cisco Intercompany Media Engine server.
Chapter 11	"Cisco Intercompany Media Engine Performance Objects and Counters" Contains a list of performance objects and their associated counters for Cisco Intercompany Media Engine.
Chapter 12	"Cisco Intercompany Media Engine Alert Descriptions and Default Settings" Contains descriptions and default configurations of Cisco Intercompany Media Engine alerts.

Related Documentation

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

- *Cisco Unified Communications Manager Documentation Guide*
- *Release Notes for Cisco Unified Communications Manager*
- *Release Notes for Cisco Intercompany Media Engine*
- *Cisco Intercompany Media Engine Release 8.5(1) TCP and UDP Port Usage*
- *Cisco Intercompany Media Engine Command Line Interface Reference Guide*
- *Cisco Unified Communications Manager System Guide*
- *Cisco Unified Communications Manager Features and Services Guide*
- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Serviceability Administration Guide*
- *Cisco Unified Real-Time Monitoring Tool Administration Guide*
- *Cisco Unified Communications Manager Bulk Administration Guide*
- *Cisco Unified Communications Solution Reference Network Design (SRND)*

Conventions

This document uses the following conventions.

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

Convention	Description
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.
italic screen font	Arguments for which you supply values are in *italic screen* 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 and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

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

Cisco Product Security Overview

This product contains cryptographic features and is subject to 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.

CHAPTER 1

Overview

Cisco Intercompany Media Engine (Cisco IME) provides a technique for establishing direct IP connectivity between enterprises by combining peer-to-peer technologies with the existing public switched telephone network (PSTN) infrastructure. Cisco IME allows companies that have deployed Cisco Unified Communications Manager to communicate securely over the Internet rather than the PSTN by creating dynamic Session Initiation Protocol (SIP) trunks between the enterprises. By enabling traffic outside of the enterprise to travel over the Internet, Cisco IME extends features and functionality to external calls that have previously worked exclusively within the enterprise, such as video enabled calls, wideband audio support, rich caller ID, presence, and others.

Cisco IME allows you to more effectively communicate with external partners that you rely on to run your business, including consultants, manufacturers, suppliers, outsourcing firms, distributors, and supply chain partners.

This section contains the following information:

- Features and Benefits, page 1-1
- How It Works, page 1-2
- Components, page 1-6
- Deployment Models, page 1-8

Features and Benefits

Cisco Intercompany Media Engine (Cisco IME) gradually creates dynamic SIP trunks between businesses, so that a collection of enterprises that work together appears to be one large business with intercluster trunks between the enterprises. Cisco IME allows companies to interconnect on demand over the Internet. This feature has many important properties for the customer:

- Works with phone numbers—Cisco IME works with the phone numbers customers have today. Cisco IME does not require customers to learn new numbers nor change providers.
- Works with existing phones—Cisco IME works with the existing phones within an enterprise. No need to change phones unless you want a more feature-rich phone.
- No new services to purchase—Cisco IME does not require any new services from any service providers. You continue to use your current PSTN and Internet connectivity. Cisco IME gradually moves calls off the PSTN and onto the Internet.
- Brings full Unified Communications experience—Because Cisco IME creates intercluster SIP trunks between businesses, any feature that works over the SIP trunk and only requires a SIP trunk will now work between businesses.

- Works on the Internet—Cisco IME allows you to send calls over the Internet or on managed extranets.
- Worldwide reach—Cisco IME can connect to any enterprise in the world, as long as the enterprise is running Cisco IME technology.
- Unlimited Scale—Cisco IME can work with any number of enterprises.
- Self-learning—After you configure information about your own networks, Cisco IME learns IP routes to other businesses automatically. You never have to enter information about other businesses, including phone prefixes, IP addresses, ports, domain names, and certificates.
- QoS Management—Cisco IME provides features that help you manage the quality of service (QoS) of the Internet connections. Cisco IME monitors the QoS of the Real-Time Transport Protocol (RTP) traffic in real time and fallback to PSTN automatically if problems arise.

How It Works

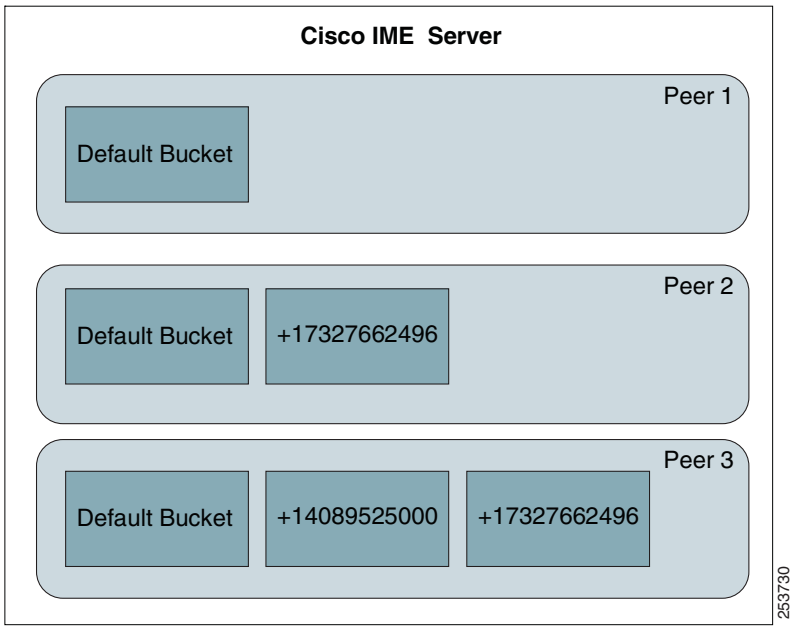
Cisco Intercompany Media Engine (Cisco IME) allows companies that have deployed Cisco Unified Communications Manager to communicate securely over the Internet rather than the PSTN by creating dynamic SIP trunks between the enterprises.

To use Cisco IME, you must deploy the Cisco IME solution, including configuring the direct inward dialing numbers (DIDs) in Cisco Unified Communications Manager that you want to participate in Cisco IME. Cisco Unified Communications Manager publishes these numbers to the Cisco IME server that, in turn, publishes the numbers to a server in the IME distributed cache ring. All Cisco IME (peer) servers participate in the IME distributed cache ring and store data in encrypted form.

Note Cisco IME requires that the system transform the numbers that a user dials to E.164 format numbers that include the international "+" prefix; for example, "+14085551212". This format will be referred to as "+E.164" format throughout this document.

Figure 1-1 provides an illustration of the IME distributed cache ring:

Figure 1-1 IME Distributed Cache Ring



To communicate with another enterprise that has stored numbers in the IME distributed cache ring over the Internet, you must first complete a configurable number of public switched telephone network (PSTN) calls to a number within that enterprise. After each PSTN call terminates, the enterprises that were involved in the call send information about the call to their Cisco IME servers in a voice call record (VCR). The VCR specifies some information about the call, including the start time, stop time, called party number, and calling party number. A validation process begins. The Cisco IME server on the originating side tries to locate the enterprise that claims ownership of the dialed number and begins a validation process to ensure that the terminating enterprise actually owns that phone number. The terminating party verifies that this domain name has not been placed into a set of blacklisted domains.

Once validated, the originating Cisco IME server sends a message to the Cisco Unified Communications Manager server and provides a VoIP route for this number. The originating Cisco Unified Communications Manager learns the route and stores the route and a validation ticket in its database for subsequent use. The ticket specifies the enterprise is authorized to call specific phone numbers at the target enterprise. The route and ticket remains valid for a year. The next time a user places a call to the same number from any number in the originating enterprise, the call travels over the Internet via a dynamic SIP trunk. When the call arrives at the Cisco Intercompany Media Engine-enabled ASA of the terminating enterprise, the Cisco Intercompany Media Engine-enabled ASA verifies the ticket that the SIP message contains. The domain in the ticket must match the domain of the calling enterprise, and the called number must match the number that the ticket permits.

Cisco IME provides security to ensure that only valid routes get sent to the Cisco Unified Communications Manager and methods to preserve quality of service if the Internet connection degrades. For more information on these features, see the following sections:

- Validation Rules, page 1-4
- PSTN Fallback, page 1-5

Validation Rules

To ensure security of the Cisco Unified Communications Manager server, the Cisco Intercompany Media Engine (Cisco IME) feature imposes a set of validation rules to ensure that it passes only valid routes to Cisco Unified Communications Manager.

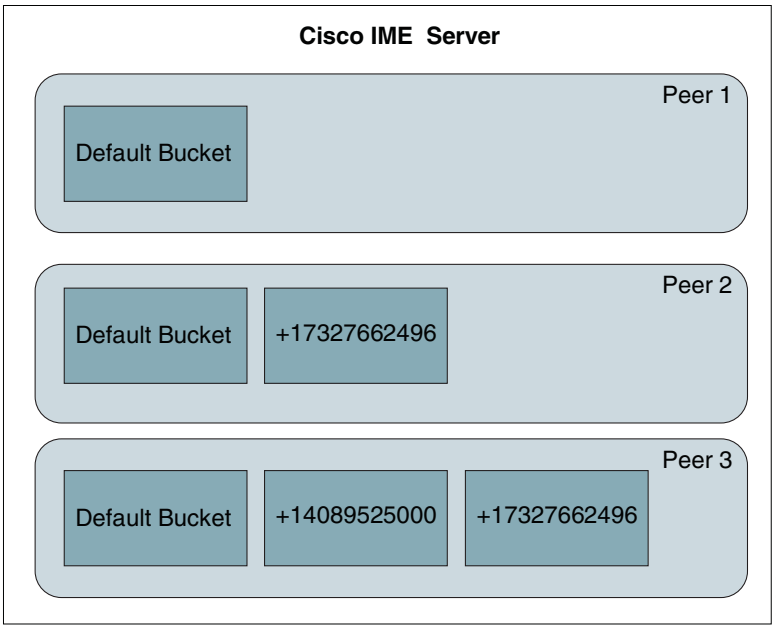
The following list summarizes the validation criteria:

- A number of consecutive successful validations against DIDs owned by a given enterprise (or Cisco IME server) must occur before Cisco Unified Communications Manager receives the learned routes from the Cisco IME server. By default, Cisco Intercompany Media Engine requires 3 validations. The validations can be against different destination numbers. Once three consecutive validations occur, the Cisco IME server passes all three learned routes to the Cisco Unified Communications Manager. You can increase or decrease the number of successful validations required for Cisco Unified Communications Manager to learn a route, depending on your security requirements.
- If validation fails against a particular number, the system requires consecutive validations against that specific number before Cisco IME passes the learned routes to Cisco Unified Communications Manager.
- To ensure that voice call records (VCRs) are uncorrelated, Cisco Unified Communications Manager never validates two VCRs for the same called number that occur within one hour of each other. You can configure the minimum time between validation attempts to the same number, depending on your security requirements.

To track the validation results, the Cisco IME server uses pools, a collection of buckets that are associated with a particular Cisco IME (or peer). Default buckets track successful validations against a Cisco IME server, and the number buckets track successful validations against the same DID.

Figure 1-2 illustrates a Cisco IME server with pools for three different peers.

Figure 1-2 Pools and Buckets



In this example, each pool contains a default bucket. Peer 2 also contains a number-specific bucket for +17327662496. Peer 3 contains two number-specific buckets: one for +1408952500 and one for +17327662496. Because the number +17327662496 exists on two different Cisco IME servers (or peers), a number-specific bucket for that number exists in two different pools, but those buckets have no relation to one another.

Each bucket holds successful validation results. When a validation succeeds against a particular peer, Cisco IME places that validation result into the number-specific bucket that matches the validated number, if one exists; else, into the default bucket. Each validation result also gets associated with a particular value, depending on the method that the Cisco IME server used to validate the call. When a validation result gets placed into a bucket, the value of the bucket increases by the value of that validation result, either 8 or 12.

Each bucket has a configured threshold. The configured threshold applies to both default buckets and number-specific bucket. Once the bucket contains validation result values that exceed the threshold, the validation results in that bucket get removed (or emptied), and the results get passed to Cisco Unified Communications Manager.

Note You can modify the threshold value of the buckets on your Cisco IME server with the set ime validator local bucketentropy CLI command.

When a validation towards a particular peer fails, Cisco IME empties all buckets in the pool that corresponds to that peer and creates a number-specific bucket to the pool for the destination number, if one does not exist. To learn a route after a validation failure, a peer must perform consecutive successful validations to the same number.

The number-specific buckets represent a penalty box. Peers that always have successful validation results never have number-specific buckets and can learn routes after the configured number of consecutive validations against different numbers. Peers that fail validation have number-specific buckets and require the configured number of consecutive validations against the same number.

PSTN Fallback

The Cisco IME feature provides mechanisms to allow calls to fallback to the PSTN, if the quality of service (QoS) degrades below an acceptable level. The Cisco Intercompany Media Engine-enabled ASA on the originating and terminating sides monitor the quality of the traffic. Based on the observed loss and jitter properties, the Cisco Intercompany Media Engine-enabled ASA determines whether the call should fallback to the PSTN. The voice call continues on the PSTN without impacting the call or alerting the users.

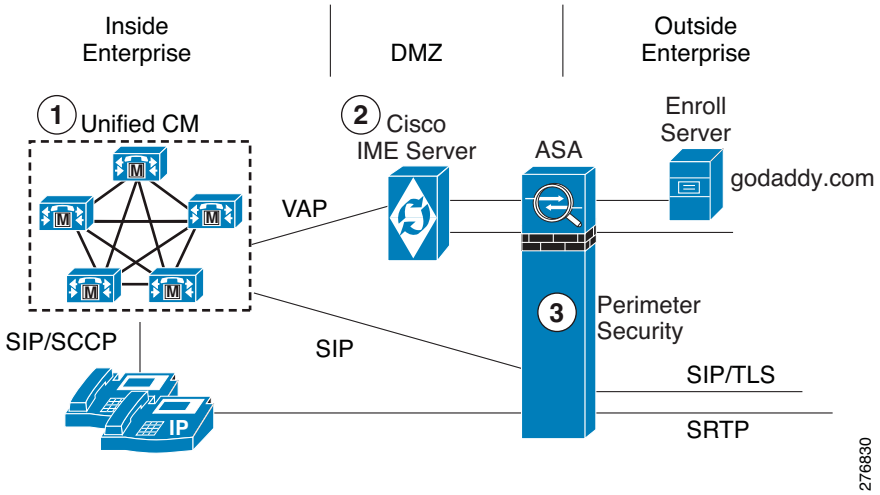
If the call needs to fallback to the PSTN, the originating Cisco Unified Communications Manager sets up a PSTN call in the background while the Cisco IME call remains active. After the Cisco Unified Communications Manager establishes the PSTN call, Cisco Unified Communications Manager seamlessly switches the Internet/RTP stream from the Internet to the PSTN. Any advanced features such as video are lost, but the audio portion of the call remains intact.

Components

Cisco Intercompany Media Engine (Cisco IME) solution consists of several components to allow for the dynamic learning of routes and the secure encryption of call signaling and media between organizations. These components include the Cisco IME server, the Cisco Unified Communications Manager server, the Cisco Intercompany Media Engine-enabled ASA, and certificates from the GoDaddy.com website. The Cisco IME server resides in the demilitarized zone (DMZ) at the customer premise and functions as an automated provisioning service. The server learns VoIP (or Cisco IME) routes to particular phone numbers and pushes those routes to the Cisco Unified Communications Manager. The Cisco Unified Communications Manager server connects to the Cisco IME server through a proprietary protocol called the Validation Access Protocol (VAP). The Cisco Unified Communications Manager performs all call processing functions as in a standard Cisco Unified Communications Manager deployment. The Cisco Intercompany Media Engine-enabled ASA provides perimeter security for the Cisco Intercompany Media Engine solution. The GoDaddy.com website allows you to obtain certificates that are needed to participate in the peer-to-peer network that the ring of Cisco IME servers create.

Figure 1-3 shows the components of the Cisco Intercompany Media Engine network:

Figure 1-3 Cisco Intercompany Media Engine Components



The following sections describe the Cisco IME components in more detail.

Cisco Intercompany Media Engine (Peer) Server

Located in the DMZ, the Cisco IME server communicates with the Cisco Unified Communications Manager server over the Validation Access Protocol (VAP) and communicates with other Cisco IME servers across the Internet. The Cisco IME servers work together to form a peer-to-peer network that creates an IME distributed cache ring across the public Internet.

Each Cisco IME server in the IME distributed cache ring stores a portion of the data owned by the ring. The data gets encrypted so that the Cisco IME server storing the data cannot read the content. Each Cisco IME on the ring can store data into the ring and can fetch data from the ring. The direct inward dialing numbers (DIDs) that get stored in the ring are one-way hashed before they get stored into the DHT. The Cisco IME server does not perform call control. Rather, the Cisco IME server stores direct inward dialing numbers (DIDs) to the IME distributed cache ring and learns routes to remote DIDs that it provides to the Cisco Unified Communications Manager.

You provide local administration and maintenance of the Cisco IME through a command line interface (CLI).

Cisco Intercompany Media Engine (Bootstrap) Server

In order to operate, Cisco IME relies on a set of bootstrap servers that Cisco Systems manages. The bootstrap servers determine which peer servers can join the IME distributed cache ring. Bootstrap servers distribute configuration information. After Cisco makes a configuration change on a bootstrap server, the change propagates around the ring and updates the configuration on all other nodes.

Cisco Unified Communications Manager

Cisco Unified Communications Manager stores the learned VoIP routes from the Cisco IME server and also provides all call processing functions for the Cisco IME solution. Cisco Unified Communications Manager Administration helps you to provision Cisco Unified Communications Manager to use the Cisco IME feature. In Cisco Unified Communications Manager Administration, you identify the Cisco IME servers, the phone numbers that you want to allow to useCisco IME, the domains that you want to trust, and so on. You can also configure parameters to enable Cisco IME calls to fallback to the public switched telephone network (PSTN) if call quality falls below acceptable levels.

ASA

The Cisco Intercompany Media Engine-enabled adaptive security appliance (ASA) plays a key role in the security of the Cisco IME solution. The Cisco Intercompany Media Engine-enabled ASA secures the call control and media interfaces. Enabled with the Cisco Intercompany Media Engine proxy, ASA provides perimeter security functions and inspects SIP signaling between SIP trunks. Specifically, the Cisco Intercompany Media Engine-enabled ASA performs the following functions:

- SIP Application Level Gateway (ALG)—Inspects SIP signaling messages that traverse through the Cisco Intercompany Media Engine-enabled ASA. The Cisco Intercompany Media Engine-enabled ASA patches the SDP and various SIP header fields to handle cases in which network address translation (NAT) is enabled. The SIP ALG also opens pinholes (or create bindings) for media streams so that media can flow in and out of the Cisco Intercompany Media Engine-enabled ASA.
- SIP message verification—Ensures that SIP messages do not crash the Cisco Unified Communications Manager or other components inside the network. The Cisco Intercompany Media Engine-enabled ASA parses and verifies key header fields that allow uniform resource identifiers (URIs). The Cisco Intercompany Media Engine-enabled ASA blocks messages that do not comply with the SIP state diagrams.
- SIP to SIP/TLS—Terminates the SIP/TLS connections towards the Internet and re-initiates a TCP-only connection towards the Cisco Unified Communications Manager when the Cisco Unified Communications Manager is not in secure mode. When the Cisco Unified Communications Manager is in secure mode, the Cisco Intercompany Media Engine-enabled ASA initiates a TLS connection towards the Cisco Unified Communications Manager. The Cisco Intercompany Media Engine-enabled ASA then acts as a TLS proxy, allowing the Cisco Unified Communications Manager to see the SIP messages and process them. The Cisco Intercompany Media Engine-enabled ASA verifies certificates issued from the far-end enterprise against known certificate authorities (CAs.)
- NAT—The ASA frequently provides the NAT and SIP ALG functionality required to work with the Internet.
- RTP/SRTP—Converts RTP on the inside of the Cisco Intercompany Media Engine-enabled ASA to SRTP on the Internet side of the Cisco Intercompany Media Engine-enabled ASA by creating an SRTP key and including the encrypted signaling that gets sent to the other side of the call.
- Ticket Verification—Inspects the Cisco IME ticket header and ensures that all signaling to the Cisco Unified Communications Manager is allowed based on the information in the ticket. The Cisco Intercompany Media Engine-enabled ASA rejects any requests without a valid ticket.
- RTP Monitoring—Inspects the RTP stream for quality of service (QoS).

You can configure your system so that Cisco IME traffic gets sent through a Cisco Intercompany Media Engine-enabled ASA and other corporate traffic gets sent through an existing ASA. For more information, see the "Deployment Models" section on page 1-8.

Enrollment Server (GoDaddy.com)

GoDaddy.com provides certificates to enable Cisco Intercompany Media Engine (Cisco IME) servers to participate in the Cisco IME peer-to-peer network. After you purchase and install the license on the Cisco IME server, go to the GoDaddy.com website to purchase a Cisco IME certificate. During the certificate purchase process, you must provide the Cisco IME server ID to identify the Cisco IME to GoDaddy uniquely. If GoDaddy determines that this server is valid, GoDaddy returns a certificate for the Cisco IME server. The certificates allow for TLS connections between the Cisco IME servers that form the distributed cache ring.

Deployment Models

This section includes the descriptions of the available deployment models for Cisco Intercompany Media Engine:

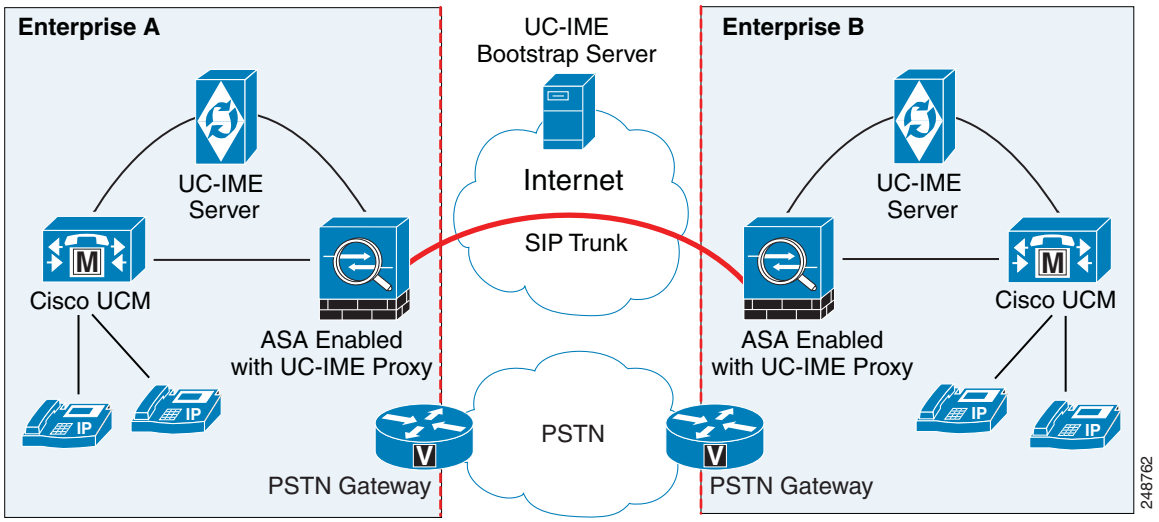
- Basic Deployment, page 1-8
- Off-path Deployment, page 1-9

Basic Deployment

In a basic deployment, the Cisco Intercompany Media Engine proxy resides in-line with the Internet firewall so that all Internet traffic traverses the adaptive security appliance (ASA). In this deployment, a single Cisco Unified Communications Manager or a Cisco Unified Communications Manager cluster is centrally deployed within the enterprise, along with a Cisco Intercompany Media Engine (Cisco IME) server. A single Internet connection traverses the ASA that is enabled with the Cisco Intercompany Media Engine proxy.

As shown in Figure 1-4, the ASA resides on the edge of the enterprise and inspects SIP signaling by creating dynamic SIP trunks between enterprises.

Figure 1-4 Basic Deployment Model



Off-path Deployment

In a typical large enterprise that uses two layers of firewalls between the corporate network, customers may not be able to replace/upgrade the existing Internet firewall with Cisco Intercompany Media Engine-enabled ASA or change the existing security architecture by adding Cisco Intercompany Media Engine-enabled ASA inline with the Internet firewall. To resolve this issue, Cisco allows an off-path ASA model for Cisco Intercompany Media Engine.

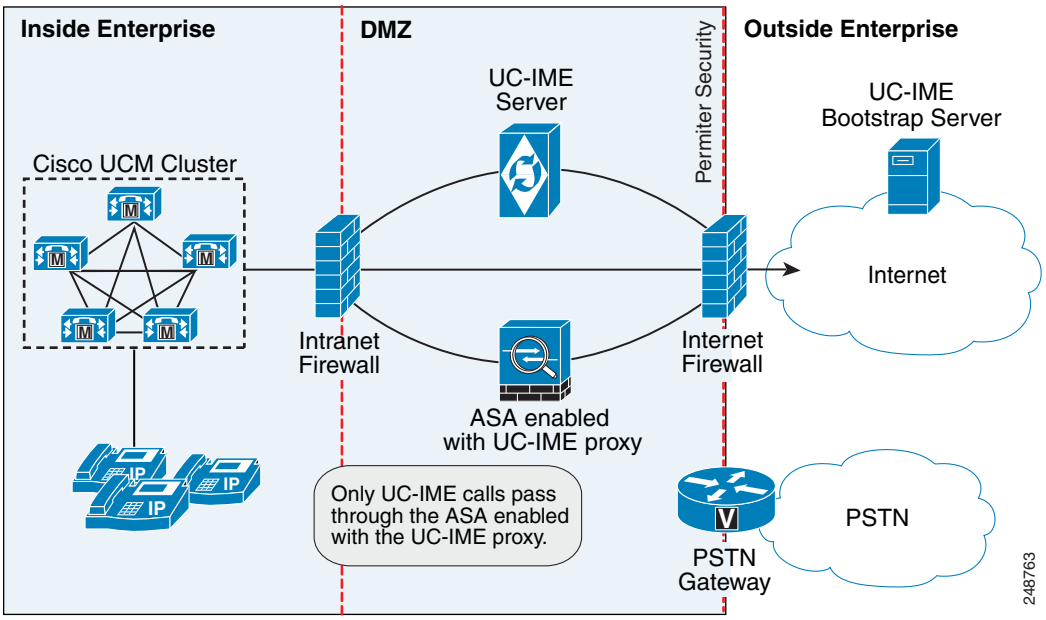
In an off-path deployment, inbound and outbound Cisco Intercompany Media Engine calls pass through an adaptive security appliance (ASA) that is enabled with the Cisco Intercompany Media Engine proxy. You configure the ASA in the DMZ, primarily to provide support for Cisco Intercompany Media Engine. Normal Internet-facing traffic does not flow through this ASA.

For all inbound calls, the signaling gets directed to the ASA because destined Cisco Unified Communications Managers are configured with the global IP address on the ASA. For outbound calls, the called party can specify any IP address on the Internet; therefore, the ASA gets configured with a mapping service that dynamically provides an internal IP address on the ASA for each global IP address of the called party on the Internet.

Cisco Unified Communications Manager sends all outbound calls directly to the mapped internal IP address on the ASA instead of to the global IP address of the called party on the Internet. The ASA then forwards the calls to the global IP address of the called party.

Figure 1-5 illustrates the architecture of the Cisco Intercompany Media Engine in an off-path deployment.

Figure 1-5 Off-path Deployment Model



In the off-path deployment, the Cisco Unified Communications Manager server with the Cisco IME trunk needs to open a TCP connection to the ASA supporting the Cisco IME deployment. This connection exists on a randomly chosen port in the 1024-65535 range. If any firewalls exist between the Cisco Unified Communications Manager server and the ASA supporting Cisco IME, you must open this port range on those firewalls.

The following example shows a sample ACL entry:

access-list SAMPLE extended permit tcp object-group CUCM object-group IME-ASA range 1024 65535

Related Topics

- Features and Benefits, page 1-1
- How It Works, page 1-2
- Deployment Models, page 1-8
- Related Topics, page 1-10

CHAPTER 2

Installation and Cisco IME Server Configuration

This chapter includes information about installing and configuring the Cisco Intercompany Media Engine server. Review all installation instructions carefully before you begin the installation procedures. This chapter covers the following topics:

- Important Considerations, page 2-1
- Frequently Asked Questions About the Installation, page 2-2
- Pre-Installation Tasks, page 2-5
- Starting the Installation, page 2-13
- Post-Installation Tasks, page 2-17
- Resetting Administrator and Security Passwords, page 2-25
- Troubleshooting Installation, page 2-27

Important Considerations

Before you proceed with the installation, consider the following requirements and recommendations:

- Make sure that the Cisco Unified Communications Manager server is running a compatible version of the Cisco Unified Communications Manager software. See the *Cisco Unified Communications Manager Software Compatibility Matrix* at the following URL:

  http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html

- Make sure that you enable NTP on the Cisco Unified Communications Manager server. To verify the NTP status, log into the Cisco Unified Communications Manager Command Line Interface, and enter **utils ntp status**.
- Be aware that when you install on an existing server, the hard drive gets formatted and all existing data on the drive gets overwritten.
- Ensure that you connect the server to an uninterruptible power supply (UPS) to provide backup power and protect your system. Failure to do so may result in damage to physical media and require a new installation of Cisco Intercompany Media Engine (Cisco IME).

  If you want the Cisco IME node to monitor UPS signaling automatically and automatically initiate a graceful shutdown upon power loss, you should use specific UPS and server models. For more information on supported models and configurations, refer to the *Release Notes for Cisco Intercompany Media Engine*.
- Configure the server by using static IP addressing to ensure that the server obtains a fixed IP address.

- You must enable DNS and configure NTP on this server during installation.
- Do not attempt to perform any configuration tasks during the installation.
- Do not install any Cisco-verified applications until you complete the installation.
- Disk mirroring on server model 7825 I3 with 160 GB SATA disk drives takes approximately 3 hours.
- Carefully read the information that follows before you proceed with the installation.

Frequently Asked Questions About the Installation

The following section contains information about commonly asked questions and responses. Review this section carefully before you begin the installation. The section includes the following topics:

- How Much Time Does the Installation Require?, page 2-2
- What User Names and Passwords Do I Need to Specify?, page 2-2
- What is a Strong Password?, page 2-3
- What is the Cisco Unified Communications Answer File Generator?, page 2-3
- Which Servers Does Cisco Support for this Installation?, page 2-4
- May I Install Other Software on the Server?, page 2-4

How Much Time Does the Installation Require?

The entire installation process, excluding pre- and post-installation tasks, takes 20 to 30 minutes, depending on your server type.

What User Names and Passwords Do I Need to Specify?

Note The system checks your passwords for strength. For guidelines on creating a strong passwords, see the "What is a Strong Password?" section on page 2-3.

During the installation, you must specify the following user names and passwords:

- Administrator Account user name and password
- Security password

Administrator Account User Name and Password

You use the Administrator Account user name and password to log in to the following areas:

- Disaster Recovery System
- Command Line Interface

To specify the Administrator Account user name and password, follow these guidelines:

- Administrator Account user name—The Administrator Account user name must start with an alphabetic character and can contain alphanumeric characters, hyphens, and underscores.
- Administrator Account password—The Administrator Account password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

You can change the Administrator Account password or add a new Administrator account by using the command line interface. For more information, see the *Cisco Intercompany Media Engine Command Line Interface Reference Guide*.

Security Password

The Security password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

What is a Strong Password?

The installation wizard checks to ensure that you enter a strong password. To create a strong password, follow these recommendations:

- Mix uppercase and lowercase letters.
- Mix letters and numbers.
- Include hyphens and underscores.
- Remember that longer passwords are stronger and more secure than shorter ones.

Avoid the following types of passwords:

- Do not use recognizable words, such as proper names and dictionary words, even when combined with numbers.
- Do not invert recognizable words.
- Do not use word or number patterns, such as aaabbb, qwerty, zyxwvuts, 123321, and so on.
- Do not use recognizable words from other languages.
- Do not use personal information of any kind, including birthdays, postal codes, names of children or pets, and so on.

What is the Cisco Unified Communications Answer File Generator?

Cisco Unified Communications Answer File Generator, a web application, generates answer files for unattended installations of Cisco Intercompany Media Engine. Individual answer files get copied to the root directory of a USB key or a floppy diskette and are used in addition to the Cisco Intercompany Media Engine DVD during the installation process.

The web application provides

- Syntactical validation of data entries
- Online help and documentation
- Support for fresh installations (but does not support upgrades.)

You can access the Cisco Unified Communications Answer File Generator at the following URL:

http://www.cisco.com/web/cuc_afg/index.html

The Cisco Unified Communications Answer File Generator supports Internet Explorer version 6.0 or higher and Mozilla version 1.5 or higher.

Cisco requires that you use USB keys that are compatible with Linux 2.4. Cisco recommends that you use USB keys that are preformatted to be compatible with Linux 2.4 for the configuration file. These keys use a W95 FAT32 format.

Which Servers Does Cisco Support for this Installation?

For information about supported server models, refer to the release notes for your product release.

Which SFTP Servers Does Cisco Support?

Cisco allows you to use any SFTP server product but recommends SFTP products that have been certified with Cisco through the Cisco Technology Developer Partner program (CTDP). CTDP partners, such as GlobalSCAPE, certify their products with specified versions of Cisco Unified Communications Manager. For information on which vendors have certified their products with your version of Cisco Unified Communications Manager, refer to the following URL:

http://www.cisco.com/pcgi-bin/ctdp/Search.pl

For information on using GlobalSCAPE with supported Cisco Unified Communications versions, refer to the following URL:

http://www.globalscape.com/gsftps/cisco.aspx

Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

- Open SSH (refer to http://sshwindows.sourceforge.net/)
- Cygwin (refer to http://www.cygwin.com/)
- Titan (refer to http://www.titanftp.com/)

Note For issues with third-party products that have not been certified through the CTDP process, contact the third-party vendor for support.

May I Install Other Software on the Server?

You must perform all software installations and upgrades by using the command line interface (CLI). The system can upload and process only software that Cisco Systems approved. You cannot install or use unapproved third-party software applications.

Pre-Installation Tasks

Table 2-1 contains a list of pre-installation tasks that you need to perform to ensure that you can successfully install Cisco Intercompany Media Engine.

Table 2-1 Pre-Installation Tasks

	Task	Important Notes
Step 1	Read this entire document to familiarize yourself with the installation procedure.	
Step 2	Cisco recommends that you complete a site analysis and planning session for Cisco IME that includes the off-path adaptive security appliance (ASA) configuration, IP addressing, pin holes, static network address translation (NAT), and demilitarized zone (DMZ) setup. You must understand the Cisco IME requirements that get imposed on the current network setup.	*Cisco Unified Communications SRND*
Step 3	Enable the necessary traffic on your corporate firewall. You must engage the teams that manage the corporate firewalls and the DMZ, such as your IT and Information Security teams, early in the design and deployment of Cisco Intercompany Media Engine. Ensure that all of the required access control lists (ACLs) on the corporate firewalls are approved and implemented before making Cisco IME calls.	Allowing Network Traffic, page 2-6
Step 4	Verify the integrity of any new server hardware (such as hard drives and memory) by running any manufacturer-provided utilities.	
Step 5	Record the network interface card (NIC) speed and duplex settings of the switch port to which you will connect the new server. You should configure the same NIC settings on the server and on the switch port. For GigE (1000/FULL), you should set NIC and switch port settings to Auto/Auto; do not set hard values.	Enable PortFast on all switch ports that are connected to Cisco servers. With PortFast enabled, the switch immediately brings a port from the blocking state into the forwarding state by eliminating the forwarding delay. [The forwarding delay specifies the amount of time that a port waits before changing from its Spanning-Tree Protocol (STP) learning and listening states to the forwarding state].
Step 6	Verify that all servers on which you plan to install Cisco IME are properly registered in DNS.	You need to be able to resolve and ping the GoDaddy.com server and intercompanymedianetwork.com bootstrap server.
Step 7	Obtain a Cisco IME license file.	See the "Obtaining a License File" section on page 2-8.
Step 8	Record the configuration settings for each server that you plan to install.	To record your configuration settings, see Table 2-4.

Additional Information

Related Topics, page 2-28

Allowing Network Traffic

This section describes the minimum required ports that need to be configured to support IME traffic. Table 2-2 provides a summary of the ports that need to be configured on a corporate firewall. Table 2-3 provides a summary of the ports that need to be configured on the offpath ASA. The port configuration shown in these tables are based on default settings. If you change the default settings, you need to update these configurations.

If you have other servers/ports required on your network, you need to allow for that traffic.

Table 2-2 Corporate Firewall Configuration

Interface	Direction	Source	Destination	Protocol	Port	Description
Inside	Inbound	Cisco Unified CM IP address	Off-path ASA inside signalling address (same as physical)	TCP	8060	Off-path mapping between Cisco Unified CM and ASA signaling address. Require entries for each Cisco Unified CM in the cluster.
Inside	Inbound	Cisco Unified CM IP address	Off-path ASA inside signalling address (same as physical)	TCP	1024-65535	Off-path mapping between Cisco Unified CM and ASA signaling address. Require entries for each Cisco Unified CM in the cluster.
DMZ	Inbound	Offpath ASA inside signaling address (same as physical)	Cisco Unified CM IP address	TCP	5060	SIP Signaling between ASA signaling address and Cisco Unified CM. Require entries for each Cisco Unified CM in the cluster. Port number configurable.
Inside	Inbound	Cisco Unified CM IP address	Cisco IME server DMZ IP address	TCP	5620	VAP communication between Cisco IME and Cisco Unified Communications Manager
Inside	Inbound	All Unified Communication devices, including MeetingPlace, voicemail, softclient IP ranges, voice gateways, and any media device needing to communicate via ASA.	Off-path ASA inside media termination IP	UDP	16384 - 32767	UDP port can be restricted based on Cisco IME enabled ASA media termination address configuration and on the number of simultaneous calls.

Table 2-2 Corporate Firewall Configuration (continued)

Interface	Direction	Source	Destination	Protocol	Port	Description
DMZ	Inbound	Offpath ASA inside media termination IP (Source port range can be restricted based on Cisco IME configuration.)	All Unified Communication devices, including MeetingPlace, voicemail, softclient IP ranges, voice gateways, and any media device needing to communicate via ASA.	UDP	16384 - 32767	UDP ports for media traffic.
Inside	Inbound	Internal network or any management workstation	Cisco IME server DMZ IP address	TCP	22	SFTP access to Cisco IME server for uploading licenses/software, upgrade, and CLI access.
Inside	Inbound	Internal network or any management workstation	Cisco IME server DMZ IP address	HTTPS	443	RTMT download from Cisco IME server
DMZ	Inbound	Cisco IME Server DMZ IP address	GoDaddy website	HTTPS	443	Download certificates from GoDaddy.
DMZ	Inbound	Cisco IME Server DMZ IP address	Any	TLS	6084	IME distributed cache communication outbound from the Cisco IME server towards the Internet
Outside	Inbound	Any	Cisco IME Server DMZ IP address	TLS	6084	IME distributed cache communication inbound from the Internet to the Cisco IME server
DMZ	Inbound	Cisco IME Server DMZ IP address	Any	TLS	8470	IME distributed cache communication outbound from the Cisco IME server towards the Internet
Outside	Inbound	Any	Cisco IME Server DMZ IP address	TLS	8470	IME distributed cache communication inbound from the Internet to the Cisco IME server

Table 2-3 External Cisco IME ASA Firewall (Offpath ASA)

Interface	Direction	Source Description	Destination Description	Protocol	Port	Description
DMZ	Inbound	Cisco Unified CM IP address	Remote Cisco Unified CM	TCP	5560-5590	Internal Cisco Unified CM signaling to remote Cisco Unified CM (remote PAT configuration)
DMZ	Inbound	Cisco Unified CM IP address	Remote Cisco Unified CM	TCP	5060	Internal Cisco Unified CM signaling to remote Cisco Unified CM (remote PAT configuration)
Outside	Inbound	Any	Cisco Unified CM IP address	TCP	5060	Remote Cisco Unified CM signaling to internal Cisco Unified CM

Additional Information

Pre-Installation Tasks, page 2-5

Obtaining a License File

You use the Product Authorization Key (PAK) that came with your product to obtain the necessary license for the Cisco IME server. The license file contains the supported version of Cisco IME, MAC address of the Cisco IME server, number of licensed Cisco IME applications (peercount), and information that you need to obtain a certificate from GoDaddy (tag and signature). The certificate enables the Cisco IME server to establish a TLS connection to other Cisco IME servers on the IME distributed cache ring.

Example 2-1 shows an example of a Cisco IME license file.

Example 2-1 License File Example

```
INCREMENT IME_SERVICE cisco 8.0 permanent uncounted \
    VENDOR_STRING=<ime><peercount>5</peercount><tag>163d18ab727c0fa14fce75c6651b1362</tag>
    <signature>154fe09fdbb012407cbfac8c74c55cb6be460199c813b0af29b83bc3b10824519bef7427f7a
    be7a7b9e6692e9b905e73fa9a1199c90ef7fd269c89f0a9179677bbee34cb1eeb915f03e2372cb1e9d272d
    af907be0077c7fd128ecc0216f036bb9447f06857cdcb4b066e746dc80ebe33fc212117b5c6c95aa404751
    6120e403c320f703a9a94ac7c177a07963dd83aa79b75c1c585250481bce340ef3bf02f86633f245cbfaef
    c2a1851b29c6cf48f580655c8a983b65d5584e316f350a15ff90478cbcb8e39128049edbb6972b33203130
    00f28db28cc51a8eb7666a40184cb5389e216cdfeac7c1d42b0e4fdf2c608bea28faeff807fcc0862497dd
    59ca676</signature></ime><LicFileVersion>1.0</LicFileVersion> \
    HOSTID=00163569b2e0 \
    NOTICE="<LicFileID>20090730162506350</LicFileID><LicLineID>1</LicLineID> \
    <PAK></PAK>" SIGN="0288 1F4A 07D6 0C34 F35B D4D5 0339 C538 \
    AC1E BC65 8697 9D5F 18D3 A57D 27DD 18D2 8C3B 14BA E72F 4932 \
    E27D 7BE9 C410 5477 9B85 AAF7 2F42 8C44 0985 CFF1"
```

Use the following procedure to obtain a license file for a Cisco IME server.

Procedure

Step 1 Enter the Product Authorization Key (PAK) that you received with your Cisco Intercompany Media Engine order in the License Registration web tool at http://www.cisco.com/go/license.

Step 2 Click **Submit**.

Step 3 Follow the system prompts. You must enter the MAC address of the network interface card (NIC) of the server on which you plan to install Cisco Intercompany Media Engine as well as a valid e-mail address. To locate the MAC address, log in to the Cisco IME command line interface (CLI) and enter **show status**. The MAC address displays in the License MAC field.

The system sends the license file to you via e-mail by using the e-mail address that you provided.

The format of a license file specifies IME<timestamp>.lic. If you retain the .lic extension, you can rename the license file. You cannot use the license if you edit the contents of the file in any way.

Step 4 You must upload the license file to the server with the matching MAC address that you provided in Step 3. See the "Uploading a License File" section on page 2-22.

Additional Information

Pre-Installation Tasks, page 2-5

Gathering Information for an Installation

Use Table 2-4 to record the information about your server. You may not need to obtain all the information; gather only the information that is pertinent to your system and network configuration.

Note Because some of the fields are optional, they may not apply to your configuration.

Caution You cannot change some of the fields after installation without reinstalling the software, so be sure to enter the values that you want.

The last column in the table shows whether you can change a field after installation; if so, the appropriate Command Line Interface (CLI) command is shown.

Table 2-4 Server Configuration Data

Parameter	Description	Can Entry Be Changed After Installation?
Administrator ID Your entry:	This field specifies the administrator account user ID that you use for secure shell access to the CLI on the Cisco Intercompany Media Engine server.	No, you cannot change the entry after installation. **Note** After installation, you can create additional administrator accounts, but you cannot change the original administrator account user ID.

Table 2-4 Server Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
Administrator Password Your entry:	This field specifies the password for the Administrator account, which you use for secure shell access to the CLI. You also use this password with the adminsftp user. You use the adminsftp user to access local backup files, upload server licenses, and so on. Ensure the password is at least six characters long; the password can contain alphanumeric characters, hyphens, and underscores.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set password admin**
Country Your entry:	From the list, choose the appropriate country for your installation. **Note** The value that you enter gets used to generate a Certificate Signing Request (CSR).	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**
DHCP Your entry:	Cisco requires that you choose **No** to the DHCP option. After you choose **No**, enter a hostname, IP Address, IP Mask, and Gateway.	No, you should not change the entry after installation.
DNS Enable Your entry:	A DNS server resolves a hostname into an IP address or an IP address into a hostname. Cisco IME requires that you use a DNS server. Choose **Yes** to enable DNS.	No, you should not change the entry after installation.
DNS Primary Your entry:	Enter the IP address of the DNS server that you want to specify as the primary DNS server. Enter the IP address in dotted decimal format as ddd.ddd.ddd.ddd.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network dns** To view DNS and network information, use the following CLI command: CLI > **network eth0 detail**
DNS Secondary (optional) Your entry:	Enter the IP address of the DNS server that you want to specify as the optional secondary DNS server.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network dns**
Gateway Address Your entry:	Enter the IP address of the network gateway. If you do not have a gateway, you must still set this field to 255.255.255.255. Not having a gateway may limit you to being able to communicate only with devices on your subnet.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network gateway**

Table 2-4 Server Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
Hostname Your entry:	Enter a host name that is unique to your server. The host name can comprise up to 64 characters and can contain alphanumeric characters and hyphens. The first character cannot be a hyphen.	Yes, you can change the entry after installation. CLI > **set network hostname**
IP Address Your entry:	Enter the IP address of your server.	Yes, you can change the entry after installation. CLI > **set network ip eth0** **Note** If you have network fault tolerance enabled, you must disable it before changing the IP address by entering set network failover dis. Then, re-enable network fault tolerance after you change the IP address by entering set network failover ena.
IP Mask Your entry:	Enter the IP subnet mask of this machine.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network ip eth0**
Location Your entry:	Enter the location of the server. The system uses this information to generate certificate signing requests (CSRs), which are used to obtain third-party certificates. You can enter any location that is meaningful within your organization. Examples include the state or the city where the server is located.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**
MTU Size Your entry:	The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. Enter the MTU size in bytes for your network. If you are unsure of the MTU setting for your network, use the default value. Default specifies 1500 bytes.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network mtu**
NIC Duplex Your entry:	Choose the duplex mode for the network interface card (NIC), either Full or Half. **Note** This parameter displays only when you choose not to use Automatic Negotiation.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network nic**

Table 2-4 Server Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
NIC Speed Your entry:	Choose the speed for the NIC, either 10 megabits per second or 100 megabits per second. **Note** This parameter displays only when you choose not to use Automatic Negotiation.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network nic**
NTP Server Your entry:	Enter the hostname or IP address of one or more network time protocol (NTP) servers with which you want to synchronize. You can enter up to five NTP servers. **Note** To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers that you specify for the primary node should be NTP v4 (version 4). If you are using IPv6 addressing, external NTP servers must be NTP v4.	Yes, you can change the entry after installation by using the following CLI command: CLI > **utils ntp server**
Organization Your entry:	Enter the name of your organization. **Tip** You can use this field to enter multiple organizational units. To enter more than one organizational unit name, separate the entries with a comma. For entries that already contain a comma, enter a backslash before the comma that is included as part of the entry. **Note** The value you enter gets used to generate a Certificate Signing Request (CSR).	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**
Security Password Your entry:	The password must contain at least six alphanumeric characters. The password can contain hyphens and underscores, but it must start with an alphanumeric character. **Note** Save this password.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set password security**
State Your entry:	Enter the state where the server is located. **Note** The value you enter gets used to generate a Certificate Signing Request (CSR).	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**

Table 2-4 Server Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
Time Zone Your entry:	This field specifies the local time zone and offset from Greenwich Mean Time (GMT). Choose the time zone that most closely matches the location of your machine.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set timezone** To view the current timezone configuration, use the following CLI command: CLI > **show timezone config**
Unit Your entry:	Enter your unit. **Note** The value you enter gets used to generate a Certificate Signing Request (CSR).	Yes, you can change the entry after installation by using the following CLI command: CLI > **set password admin**

Additional Information

Pre-Installation Tasks, page 2-5

Starting the Installation

This section describes how to install the operating system and the Cisco Intercompany Media Engine application. You install the operating system and application by running one installation program.

For information on how to navigate within the installation wizard, see Table 2-5.

Table 2-5 Installation Wizard Navigation

To Do This	Press This
Move to the next field	**Tab**
Move to the previous field	**Alt-Tab**
Choose an option	Space bar or **Enter**
Scroll up or down in a list	Up or down arrow
Go to the previous window	Space bar or **Enter** to choose **Back** (when available)
Get help information on a window	Space bar or **Enter** to choose **Help** (when available)

To start the installation, follow this procedure.

Procedure

Step 1 If you have a USB key with configuration information that the Answer File Generator generated, insert the USB key now.

Note If you have a new server with the software preinstalled, you do not need to install from a DVD, unless you want to reimage the server with a later product release. You can go directly to Step 9.

Step 2 Insert the installation DVD into the tray and restart the server, so that the server boots from the DVD. After the server completes the boot sequence, the DVD Found window displays.

Step 3 To perform the media check, choose **Yes;** or, to skip the media check, choose **No**.

The media check checks the integrity of the DVD. If your DVD passed the media check previously, you may choose to skip the media check.

Step 4 If you choose **Yes** to perform the media check, the Media Check Result window displays. Perform one of these tasks:

a. If the Media Check Result displays Pass, choose **OK** to continue the installation.

b. If the media fails the Media Check, either download another copy from Cisco.com or obtain another DVD directly from Cisco.

Step 5 The system installer performs the following hardware checks to ensure that your system is configured correctly. If the installer makes any changes to your hardware configuration settings, you get prompted to restart your system. Leave the DVD in the drive during the reboot:

- First, the installation process checks for the correct drivers. You may see the following warning:

  ```
  No hard drives have been found. You probably need to manually choose device drivers
  for install to succeed. Would you like to select drivers now?
  ```

  To continue the installation, choose **Yes**.
- The installation next checks whether you have a supported hardware platform. If your server does not meet the exact hardware requirements, the installation process fails with a critical error. If you think this failure is not correct, capture the error and report it Cisco support.
- The installation process next verifies RAID configuration and BIOS settings.

Note If this step repeats, choose **Yes** again.

- If the installation program must install a BIOS update, a notification tells you that the system must reboot. Press any key to continue the installation.

After the hardware checks complete, the Product Deployment Selection window displays.

Step 6 In the Product Deployment Selection window, choose **OK**.

Step 7 If software is currently installed on the server, the Overwrite Hard Drive window opens and displays the current software version on your hard drive and the version on the DVD. Choose **Yes** to continue the installation or **No** to cancel.

Caution If you choose **Yes** on the **Overwrite Hard Drive** window, all existing data on your hard drive gets overwritten and destroyed.

The Platform Installation Wizard window displays.

Step 8 Choose one of the following options:

- To enter your configuration information manually and have the installation program install the configured software on the server, choose **Proceed** and continue with Step 12.
- To do any of the following tasks, choose **Skip** and continue with the Step 9:
  - Manually configure the software that is preinstalled on your server—In this case, you do not need to install the software, but you must configure the preinstalled software.
  - Perform an unattended installation—In this case, you provide preexisting configuration information on a USB key or floppy disk.
  - Install the software before manually configuring it—In this case, the installation program installs the software, then prompts you to configure it manually. You can choose **Skip** if you want to preinstall the application on your server first, then enter the configuration information at a later time. This method may take more time than the other methods.

Step 9 After the system restarts, the Preexisting Installation Configuration window displays.

Step 10 If you have preexisting configuration information that the Answer File Generator created, the information gets stored on a floppy disc or a USB key. Insert the disc or the USB key now and choose **Continue**. The installation wizard reads the configuration information during the installation process.

Note If a popup window states that the system detected new hardware, press any key and then choose **Install** from the next window.

The Platform Installation Wizard window displays.

Step 11 To continue with the Platform Installation Wizard, choose **Proceed**.

Step 12 In the Basic Install window, choose **Continue** to install the software version on the DVD or to configure the preinstalled software.

Step 13 When the Timezone Configuration displays, choose the appropriate time zone for the server; then, choose **OK**.

The Auto Negotiation Configuration window displays.

Step 14 The installation process allows you to set the speed and duplex settings of the Ethernet network interface card (NIC) automatically by using automatic negotiation. You can change this setting after installation.

- To enable automatic negotiation, choose **Yes;** then, continue with Step 17.

  The MTU Configuration window displays.

Note To use this option, your hub or Ethernet switch must support automatic negotiation.

- To disable automatic negotiation, choose **No;** then continue with Step 15.

  The NIC Speed and Duplex Configuration window displays.

Step 15 If you chose to disable automatic negotiation, manually choose the appropriate NIC speed and duplex settings now; then, choose **OK** to continue.

The MTU Configuration window displays.

Step 16 In the MTU Configuration window, you can change the MTU size from the operating system default.

The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. If you are unsure of the MTU setting for your network, use the default value, which specifies 1500 bytes.

Caution If you configure the MTU size incorrectly, your network performance can be affected.

- To accept the default value (1500 bytes), choose **No**.
- To change the MTU size from the operating system default, choose **Yes**. Enter the new MTU size; then, choose **OK**.

The DHCP Configuration window displays.

Step 17 For network configuration, Cisco requires that you set up a static network IP address for the server rather than use Dynamic Host Configuration Protocol (DHCP). When prompted to choose DHCP or not, choose **No**. The Static Network Configuration window displays.

Step 18 Enter your static network configuration values; then, choose **OK**. See Table 2-4 for field descriptions.

The DNS Client Configuration window displays.

Step 19 Cisco requires that you enable DNS. Choose **Yes**. Enter your DNS client information; then, choose **OK**. See Table 2-4 for field descriptions.

The network restarts by using the new configuration information, and the Administrator Login Configuration window displays.

Step 20 Enter your Administrator login and password from Table 2-4.

Note The Administrator login must start with an alphabetic character; must contain at least six characters; and can contain alphanumeric characters, hyphens, and underscores. You need the Administrator login to log in to the command line interface.

The Certificate Information window displays.

Step 21 Enter your certificate signing request information, then, choose **OK**.

The Network Time Protocol Client Configuration window displays.

Step 22 Cisco Systems recommends that you use an external NTP server to ensure accurate system time. Ensure that the external NTP server specifies stratum 9 or higher (that is, stratums 1 through 9).

Choose whether you want to configure an external NTP server or to configure the system time manually:

- To set up an external NTP server, choose **Yes**. Enter the IP address, NTP server name, or NTP server pool name for at least one NTP server. You can configure up to five NTP servers. Cisco Systems recommends that you use at least three NTP servers. Choose **Proceed** to continue with the installation.

The system contacts an NTP server and automatically sets the time on the hardware clock.

Note If the Test button displays, you can choose **Test** to check whether the NTP servers are accessible.

- To configure the system time manually, choose **No**. Enter the appropriate date and time to set the hardware clock. Choose **OK** to continue with the installation.

The Security Configuration window displays.

Step 23 Enter the Security password from Table 2-4.

Note The Security password must start with an alphanumeric character; must contain at least six characters; and can contain alphanumeric characters, hyphens, and underscores.

The Platform Configuration Confirmation window displays.

Step 24 To continue with the installation, choose **OK**; or, to modify the platform configuration, choose **Back**.

The system installs and configures the software. The DVD drive ejects, and the server reboots. Do not reinsert the DVD.

Step 25 When the installation process completes, you get prompted to log in by using the Administrator account and password.

Step 26 Complete the post-installation tasks in the "Post-Installation Tasks" section on page 2-17.

Additional Information

Related Topics, page 2-28

Post-Installation Tasks

After installing the software on your server, you must complete the post-installation tasks listed in Table 2-6.

Table 2-6 Post-Installation Tasks

Configuration Steps		Related Procedures and Topics
Step 1	Install the Real Time Monitoring Tool on a client machine.	You can use the Real Time Monitoring Tool to monitor system health, and to view and collect logs. For installation instructions and more information about the Real Time Monitoring Tool, see "Installing RTMT" section on page 7-1.
Step 2	Upload your Cisco Intercompany Media Engine license file to the server.	See the "Uploading a License File" section on page 2-22.
Step 3	Obtain the Cisco Intercompany Media Engine certificates from GoDaddy.com.	See the "Certificate Purchase and Enrollment" section on page 2-22 and the "Manually Renewing a Cisco Intercompany Media Engine Certificate" section on page 2-24.

Table 2-6 Post-Installation Tasks (continued)

Configuration Steps		Related Procedures and Topics
Step 4	For secure communication between Cisco Unified Communications Manager and Cisco Intercompany Media Engine, access and install a self-signed or third-party certificate.	See the following topics: • Generating and Uploading a Self-Signed Certificate on the Cisco Intercompany Media Engine Server, page 3-17 • Generating and Uploading Third Party Certificates for Cisco Intercompany Media Engine, page 3-18
Step 5	Configure the backup settings. Remember to back up your Cisco Intercompany Media Engine data daily.	See the "Backing up and Restoring the Cisco IME Server" section on page 5-1.
Step 6	On the Cisco IME server, you must create settings that allow the Cisco Unified Communications Manager and Cisco IME servers to connect and exchange VAP signaling. First, you must set up a vapserver name and port.	Log into the Cisco IME CLI and enter the following command: add ime vapserver You will be prompted for the vapserver name, port, and authentication mode. The name the you enter represents a unique identifier for this instance. The name does not need to match the Cisco Unified Communications Manager name. You need to be sure that the authentication mode that you choose matches that of the Cisco Unified Communications Manager (encrypted or authenticated). **Note** If you have more than one Cisco Unified Communications Manager that uses the same Cisco IME server, you need to add a vapserver entry for each cluster. Make sure to specify a unique port number for each vapserver name. You can have multiple vapserver instances, where one instance is for authenticated mode and another is for encrypted and authenticated mode. These instances should use different ports. For more details on the command options, see the *Cisco Intercompany Media Engine Command Line Interface Reference Guide*.
Step 7	View all of the vapservers that you have administered.	Log into the Cisco IME CLI and enter the following command: show ime vapserver all

Table 2-6 Post-Installation Tasks (continued)

Configuration Steps		Related Procedures and Topics
Step 8	(Optional) Set the necessary options for each vapserver instance that you configured, if desired.	Log into the Cisco IME CLI and enter the following commands: • set ime vapserver authenticationmode • set ime vapserver enabled • set ime vapserver keepaliveinterval • set ime vapserver maxconnectionsallowed • set ime vapserver port **Note** Cisco highly recommends that you set the authentication mode to *Encrypted*. For more details on the command options, see the *Cisco Intercompany Media Engine Command Line Interface Reference Guide*.
Step 9	Configure VAP user credentials on the Cisco IME server.	Log into the Cisco IME CLI and enter the following command: add ime vapusercredentials The command prompts you for a username and password. **Note** The application username and password that you enter must match those that you enter for the application user in Cisco Unified Communications Manager Administration in Step 3 in Table 3-1. **Note** The ticket password and Epoch must match those configured on the Cisco IME ASA. Cisco recommends that you create a password containing at least 20 characters. For more details on the command options, see the *Cisco Intercompany Media Engine Command Line Interface Reference Guide*.

Table 2-6 Post-Installation Tasks (continued)

Configuration Steps		Related Procedures and Topics

Step 10	If the Cisco IME Server resides behind a firewall and Network Address Translation (NAT) is required to reach the server from the public internet, you must configure the external address on the Cisco IME server before the server can join the IME Distributed Cache.	1. Log into the Cisco IME CLI and enter the following command:
		set ime addressing publicipaddrv4 *external ip addr*
		For example, if the public IP address of the Cisco IME equals 65.65.65.65, enter
		set ime addressing publicipaddrv4 65.65.65.65
		2. Then, verify the settings by entering the following command:
		show ime addressing
		The following example shows the Public and Private IP addresses of a Cisco IME server:
		`admin: show ime addressing`
		`====================================`
		`Public IP Address = 65.65.65.65`
		`Private IP Address = 10.10.10.10`
		`DHT Port = 6084`
		`Validator Port = 8470`
		`====================================`

Step 11	Make sure that you can display a list of peer IDs of your Cisco IME servers and the IP address of the bootstrap server.	Log into the Cisco IME CLI and enter the following commands: • show ime peerid If you do not see a peer ID, you may have an issue with your Cisco IME certificate. You should fix the problem before continuing the configuration. • show ime bootstrap ip Make sure that at least one IP address displays. If no IP addresses displays, this indicates that the Cisco IME cannot reach the bootstrap severs via DNS.

Table 2-6 Post-Installation Tasks (continued)

Configuration Steps		Related Procedures and Topics

Step 12	Verify the status of the Cisco IME server on the IME distributed cache.
	Note The server may take 20 minutes to join the ring and for the status to turn green.
		Log into the Cisco IME CLI and enter the following command:
		show ime dht summary
		The DHT Health field shows the status of the server in the Peer ID field. Green indicates a functional status.
		`Peer ID = 514dd001c7553593ebefee2b076ad9d4`
		`DHT Health..... = GREEN`
		`BootStrap: 5619e12c7a647e1d3364c8a46c9e58f7`
		`Last Contact (sec)..... = 48`
		`Current Sequence..... = 1250036323`
		`Num. Tokens Received..... = 3`
		`Delay from BootStrap..... = 1`
		`Peer Count Distance..... = 5`
		If the peer ID status does not display as green, verify that you installed Cisco IME certificates correctly and check the Cisco IME ports and the Cisco IME-enabled ASA.
		You may also need to use the show ime addressing command to verify that you set the public IP address correctly.

Step 13	Cisco highly recommends that you configure customer contact information. This information gets stored on your Cisco IME server and can be used by Cisco Technical Support to contact your company, if they detect a misconfiguration on your Cisco IME server.	Log into the Cisco IME CLI and enter the following command: set ime customerinfo The system prompts you for the following information: • Company Name—The name of the company using this Cisco IME server • Unit Name—Unit within the company (city name or department) • State—State where this server is located • Country—Country where this server is located • Support Contact Name—Person that should be contacted, if Cisco detects a misconfiguration on your Cisco IME server • Support Contact Email—Email of the support contact for your company • Support Contact Phone—Phone number of your support contact After you have set your customer information, you can use the show ime customerinfo command to view this information.

Additional Information

Related Topics, page 2-28

Uploading a License File

Use the following procedure to upload a license file to the Cisco IME server with the matching MAC address that is provided when a license file is requested. For information about obtaining a license file, see the "Obtaining a License File" section on page 2-8.

Before You Begin

Make sure that the Cisco IME server software has been installed on the server.

Procedure

Step 1 Save the Cisco IME license file (.lic) to a temporary directory on your local hard drive.

Step 2 Open an SFTP client and connect to the Cisco IME server by using the adminsftp user and the administrator password that you set up during installation.

Step 3 Navigate to the license directory by entering **cd license** and copy the license file to that directory.

Step 4 Type **put** <*license filename*>, where <*license filename*> specifies the license file name that you received via email.

Step 5 Upload the Cisco IME license by logging into the Cisco IME command line interface (CLI) and entering **utils ime license file install <license filename>**.

Note The format of the license file that you receive specifies IME<timestamp>.lic. If you retain the .lic extension, you can rename the license file. You cannot use the license if you edit the contents of the file in any way.

After installation, the server stores license files in /usr/local/ime/conf/licfiles. The server stores license logs at /active/cm/trace/ime/licensing/log4j.

Additional Information

Post-Installation Tasks, page 2-17

Certificate Purchase and Enrollment

Cisco IME encrypts communications between servers and needs certificates on each server that are trusted by the same group. The certificates cannot be self-signed. The certificate enables the Cisco IME server to establish a TLS connection other Cisco IME servers on the IME distributed cache ring.

GoDaddy provides certificates for the IME distributed cache ring. GoDaddy uses information in the Cisco IME license, including the tag, peerIDCount, and signature, to identify each server uniquely and to generate certificates.

You purchase a certificate for Cisco IME server on the GoDaddy website. After you purchase the certificate, you enroll the certificate with GoDaddy. During the enrollment process, you provide information that indicates that you have a valid server that can obtain a certificate. Certificates remain valid for one year from the date of purchase.

The Cisco IME server attempts to renew the certificate before the expiration date. If the auto-enrollment fails, the server generates an EnrollFailure alarm. You must manually renew the certificate. For more information on renewing certificates, see the "Manually Renewing a Cisco Intercompany Media Engine Certificate" section on page 2-24.

Use the following procedure to purchase and enroll a new certificate.

Before You Begin

Install the license on the Cisco IME server, as described in the "Uploading a License File" section on page 2-22.

Procedure

Step 1 Go to http://www.godaddy.com.

Step 2 Log in to your Account Manager.

Step 3 In the My Products section, choose **SSL Certificates**.

Step 4 Purchase a certificate for the Cisco IME server.

Note For more detailed instructions on purchasing a certificate, refer to the support topic on the GoDaddy website for requesting and installing a Cisco Intercompany Media Engine certificate at http://help.godaddy.com/article/5414.

During the purchase process, you must enter the server ID of your server. To obtain this ID, log in to the CLI on the Cisco IME server and type **show ime certenrollment server ID**.

Step 5 When prompted, install the certificate on the Cisco IME server by typing **utils ime certenrollment enroll** in the Cisco IME server CLI.

Step 6 The Cisco IME server generates the SuccessfulEnrollment alert upon successful enrollment and generates the EnrollFailure alert upon a failed enrollment.

Step 7 To view the certificate on the Cisco IME server, go to the CLI and type **show cert own intercompanymedianetwork**.

Note The system stores manual enrollment and auto-enrollment log files in the following directories, respectively: /active/platform/log/cli*.log and /active/platform/log/certm.log.

Additional Information

Post-Installation Tasks, page 2-17

Manually Renewing a Cisco Intercompany Media Engine Certificate

When you install the Cisco IME server for the first time, you have to purchase and enroll the certificate with GoDaddy, as described in "Certificate Purchase and Enrollment" section on page 2-22. Certificates remain valid for one year from the date of purchase. The Cisco IME server attempts to renew the certificate before the expiration date. If the auto-enrollment fails, the server generates an EnrollFailure alert. You must use this procedure to manually renew the certificate.

Procedure

Step 1 Go to http://www.godaddy.com.

Step 2 Log in to your Account Manager.

Step 3 In the My Products section, choose **SSL Certificates** and find the certificate that you want to renew.

Note For more detailed instructions on renewing a certificate, refer to the support topic on the GoDaddy website for renewing a Cisco Intercompany Media Engine certificate at http://help.godaddy.com/article/5415.

Step 4 After GoDaddy receives your payment, one of the following events occurs:

- If GoDaddy receives your payment before the old certificate expires, the certificate renews without further action from you.
- If GoDaddy receives your payment after the old certificate expires, type **utils ime certenrollment enroll** in the Cisco IME server CLI.

Step 5 The Cisco IME server generates the SuccessfulEnrollment alert upon successful enrollment and generates the EnrollFailure alert upon a failed enrollment.

Step 6 To view the certificate on the Cisco IME server, go to the CLI and type **show cert own intercompanymedianetwork**.

Note The system stores manual enrollment and auto-enrollment log files in the following directories, respectively: /active/platform/log/cli*.log and /active/platform/log/certm.log.

Additional Information

Post-Installation Tasks, page 2-17

Resetting Administrator and Security Passwords

If you lose the administrator password or security password, use the following procedure to reset these passwords.

To perform the password reset process, you must connect to the system through the system console; that is, you must connect to the server with a keyboard and monitor. You cannot reset a password when you connect to the system through a secure shell session.

Note During this procedure, you must remove and then insert a valid CD or DVD in the disk drive to prove that you have physical access to the system.

Procedure

Step 1 Log in to the system with the following username and password:

- Username: pwrecovery
- Password: pwreset

The Welcome to platform password reset window displays.

Step 2 Press any key to continue.

Step 3 If you have a CD or DVD in the disk drive, remove it now.

Step 4 Press any key to continue.

The system tests to ensure that you have removed the CD or DVD from the disk drive.

Step 5 Insert a valid CD or DVD into the disk drive.

Note For this test, you must use a data CD, not a music CD.

The system tests to ensure that you have inserted the disk.

Step 6 After the system verifies that you have inserted the disk, you get prompted to enter one of the following options to continue:

- Enter **a** to reset the administrator password.
- Enter **s** to reset the security password.
- Enter **q** to quit.

Step 7 Enter a new password of the type that you chose.

Step 8 Reenter the new password.

The password must contain at least six characters. The system checks the new password for strength. If the password does not pass the strength check, you get prompted to enter a new password.

Step 9 After the system verifies the strength of the new password, the password gets reset. You get prompted to press any key to exit the password reset utility.

Additional Information

Related Topics, page 2-28

Upgrading Cisco Intercompany Media Engine Software

Before you begin the upgrade process, you must obtain the appropriate upgrade file from Cisco.com.

Use the following procedure to upgrade the Cisco Intercompany Media Engine (Cisco IME) server software:

Note When you upgrade the Cisco IME, the services that communicate with the Cisco IME service on the Cisco Unified Communications Manager get stopped. This stoppage causes the Cisco Unified Communications Manager to temporarily stop learning routes until the upgrade completes and the Cisco IME server gets switched to the new release. During this time, an alert that indicates that Cisco IME service is down will be seen on the Cisco Unified Communications Manager server. To minimize impact on the Cisco Unified Communications Manager, Cisco highly recommends that you upgrade the Cisco IME server during an inactive period. The upgrade procedure takes approximately 20 to 30 minutes.

Procedure

Step 1 Obtain the upgrade media to upgrade the Cisco Intercompany Media Engine server.

If you downloaded the software executable from Cisco.com, do one of the following:

- Prepare to upgrade from a local directory by performing the following steps:
  - Copy the Cisco IME upgrade file to a temporary directory on your local hard drive.
  - Create an upgrade disk by burning the upgrade file that you downloaded onto a DVD as an ISO image.

    Note If you copy the .iso file to the DVD but do not create an ISO image, you cannot upgrade your server from that DVD. Most commercial disk burning applications can create ISO image disks.

  - Open an SFTP client and connect to the Cisco IME server by using the adminsftp user and the administrator password that you set up during installation.
  - Navigate to the upgrade directory by entering **cd upgrade** and copy the license file to that directory.
  - Type **put** <*upgrade filename*>, where <*upgrade filename*> specifies the upgrade file name that you downloaded from Cisco.com or obtained on a DVD.
- Put the upgrade file on an FTP or SFTP server that the server that you are upgrading can access.

  If you have a Cisco-provided upgrade disk, copy the contents of the disk to the remote server.

  If you downloaded the upgrade files, copy the files you downloaded to the remote server.

Step 2 After you have inserted the DVD into the server or uploaded the upgrade file to the remote server or local directory, log into the Cisco IME CLI and enter **utils system upgrade initiate**.

Step 3 Choose the source from which you want to upgrade:

- 1—Remote Filesystem via SFTP
- 2—Remote Filesystem via FTP
- 3—Local DVD/CD
- 4—Local Upload Directory

Step 4 Follow the system prompts for the upgrade option that you chose.

Step 5 The system prompts you when the upgrade process completes. If you did not choose the option to automatically switch versions, enter **utils system switch-version** and enter **yes** to confirm that you want to reboot the server and switch to the new software version.

Step 6 After the installation completes, log into the Cisco IME CLI and verify the following:

- Make sure that the DHT displays a green health status by logging into the Cisco IME CLI and entering **show ime dht summary**. The server may take 20 minutes to join the ring and for the status to turn green.
- Make sure that the Registration Status equals *Registered*, and the Client IP ADDR equals the IP address of the Cisco Unified Communications Manager server by entering **show ime vapstatus summary**.

Additional Information

Related Topics, page 2-28

Troubleshooting Installation

Use the following sections to troubleshoot problems that occur during installation of the Cisco Intercompany Media Engine software:

- Handling Network Errors During Installation, page 2-27
- Examining Log Files, page 2-28

Handling Network Errors During Installation

During the installation process, the installation program verifies that the server can successfully connect to the network by using the network configuration that you enter. If the server cannot connect, a message displays; you get prompted to select one of the following options:

- **RETRY** —The installation program tries to validate networking again. If validation fails again, the error dialog box displays again.
- **REVIEW (Check Install)**—This option allows you to review and modify the networking configuration. When detected, the installation program returns to the network configuration windows.

  Networking gets validated after you complete each networking window, so the message may display multiple times.
- **HALT**— The installation halts. You can copy the installation log files to a USB disk to aid troubleshooting of your network configuration.
- **IGNORE** —The installation continues. The networking error gets logged. In some cases, the installation program validates networking multiple times, so this error dialog box may display multiple times. If you choose to ignore network errors, the installation may fail.

Additional Information

Related Topics, page 2-28

Examining Log Files

If you encounter problems with the installation, you may be able to examine the install log files by entering the following commands in Command Line Interface.

To obtain a list of install log files from the command line, enter

```
CLI>file list install *
```

To view the log file from the command line, enter

```
CLI>file view install log_file
```

where *log_file* specifies the log file name.

You can also view logs by using the Real Time Monitoring Tool. For more information on using and installing the Real Time Monitoring Tool, refer to the*Cisco Unified Real Time Monitoring Tool Administration Guide*.

You can get more information about installation events by viewing or downloading the System History log. Refer to the following for more information:

- System History Log, page 10-1
- "Working with Trace and Log Central" chapter in the *Cisco Unified Real Time Monitoring Tool Administration Guide*

Additional Information

Related Topics, page 2-28

Related Topics

- Important Considerations, page 2-1
- Frequently Asked Questions About the Installation, page 2-2
- Pre-Installation Tasks, page 2-5
- Starting the Installation, page 2-13
- Post-Installation Tasks, page 2-17
- Resetting Administrator and Security Passwords, page 2-25
- Troubleshooting Installation, page 2-27

CHAPTER 3

Cisco IME Configuration in Cisco Unified Communications Manager Administration

Cisco Intercompany Media Engine (Cisco IME) allows customer to establish direct IP connectivity between enterprises. After you install the software on the Cisco IME server and perform the post-installation tasks, you must configure the Cisco Unified Communications Manager server to enable the Cisco Intercompany Media Engine feature.

This chapter contains information on using the Cisco Unified Communications Manager Administration user interface and provides detailed steps on configuring the Cisco Unified Communications Manager server for the Cisco Intercompany Media Engine feature. The chapter covers the following topics:

- Cisco Unified Communications Manager Administration Basics, page 3-2
- Cisco IME Configuration Checklist, page 3-6
- Configuring Cisco IME Server Connections, page 3-14
- Setting Up TLS Connections Between the Cisco Unified Communications Manager and Cisco Intercompany Media Engine Servers, page 3-16
- Configuring a Cisco IME Enrolled Group, page 3-19
- Configuring a Cisco IME Enrolled Pattern, page 3-21
- Configuring a Cisco IME Exclusion Group, page 3-22
- Configuring a Cisco IME Exclusion Number, page 3-23
- Configuring a Cisco IME Trust Group, page 3-24
- Configuring a Cisco IME Trust Element, page 3-25
- Configuring a Cisco IME Service, page 3-26
- Configuring External IP Address and Port Information, page 3-28
- Configuring Transformation Patterns for Cisco IME, page 3-29
- Configuring a Cisco IME Transformation Profile, page 3-30
- Configuring Cisco IME E.164 Transformations, page 3-35
- Configuring PSTN Access Trunks, page 3-36
- Configuring a Cisco IME Feature Configuration, page 3-37
- Verifying Connectivity, page 3-40
- Configuring a Fallback Profile, page 3-43
- Configuring Fallback Feature Parameters, page 3-47

- Configuring Intercompany Media Services Firewall Information, page 3-49
- Cisco Intercompany Media Engine Learned Routes, page 3-49
- Related Topics, page 3-50

Cisco Unified Communications Manager Administration Basics

You use Cisco Unified Communications Manager Administration, a web-based application, to perform configuration tasks for Cisco Unified Communications Manager servers. This section describes basic elements of the graphical user interface, including the navigation menus and the documentation search feature that allows you to search Cisco Unified Communications Manager documentation on Cisco.com.

For more information, see the following topics:

- Using the Cisco Unified Communications Manager Administration Graphical User Interface, page 3-2
- Using Cisco Unified Communications Manager Administration Help, page 3-3
- Finding and Deleting Records, page 3-3
- Adding and Copying Records, page 3-5

Using the Cisco Unified Communications Manager Administration Graphical User Interface

The Cisco Unified Communications Manager Administration interface contains the following options.

Note For information on logging into Cisco Unified Communications Manager Administration, refer to the *Cisco Unified Communications Manager Administration Guide*.

- Navigation—After you log on, the main Cisco Unified Communications Manager Administration window redisplays. The window includes the drop-down list box in the upper, right corner called **Navigation**. To access the applications in the drop-down list box, choose the program that you want and click **Go**. The choices in the drop-down list box include the following Cisco Unified Communications Manager applications:
  - Cisco Unified Communications Manager Administration—Shows as default when you access Cisco Unified Communications Manager. Use Cisco Unified Communications Manager Administration to configure system parameters, route plans, devices, and much more.
  - Cisco Unified Serviceability—Takes you to the main Cisco Unified Serviceability window. Use Cisco Unified Serviceability to configure trace files and alarms and to activate and deactivate services.
  - Cisco Unified OS Administration—Takes you to the main Cisco Unified Operating System Administration window, so you can configure and administer the Cisco Unified Communications Manager platform. You must log off from any other application before you can log in to this application.
  - Disaster Recovery System—Takes you to the Cisco Disaster Recovery System, a program that provides full data backup and restore capabilities for all servers in a Cisco Unified Communications Manager cluster. You must log off from any other application before you can log in to this application.

- Search Documentation—Click this link to search Cisco Unified Communications Manager documentation on Cisco.com for the current release. The Cisco Unified CM Documentation Search window displays. Type the word or words for which you want to search and click the **Search** button. The search results display. You can narrow the search results by choosing a documentation type modifier button that displays above your search result; for example, Unified CM Install/Upgrade or Unified CM Business Edition Release Notes.
- About—Displays the Cisco Unified Communications Manager Administration main window and allows you to view the system software version.
- Logout—Allows you to log out of Cisco Unified Communications Manager Administration application. The window redisplays with the login fields.
- Menu Bar—The horizontal bar located across the top of the interface contains the names of the menus. Click the menu options to display the Cisco Unified Communications Manager Administration windows. Menu items in this document appear in **boldface** font. A **>** (greater than) symbol separates menu item selections. In the browser, this indicates a menu item selection; for example: Choose **Advanced Features > Intercompany Media Services > Service**.

Additional Information

Cisco Unified Communications Manager Administration Basics, page 3-2

Using Cisco Unified Communications Manager Administration Help

To access Help, click the Help menu in the Cisco Unified Communications Manager Administration navigation bar, and choose one of the following options:

- Contents—Opens a new browser window and displays the home page for the Cisco Unified Communications Manager Administration Help system. The links in the left pane of the Help window allow you to access all topics in the Help system.
- This Page—Opens a new browser window for the Cisco Unified Communications Manager Administration Help system. The right pane of the window contains definitions for each field in the current window in Cisco Unified Communications Manager Administration. In most cases, cross-references point to additional topics that relate to the current window.
- About—Displays the Cisco Unified Communications Manager Administration main window and allows you to view the system software version.

The left pane of the Help system provides a table of contents for all of the product guides that the Help system includes. The table of contents expands to show the location within the hierarchy of the Help topic that displays on the right.

To learn more about the Cisco Unified Communications Manager Administration system, including instructions on how to search Help, click the Using Help link at the top of any Help window.

Additional Information

Cisco Unified Communications Manager Administration Basics, page 3-2

Finding and Deleting Records

You can search Cisco Unified Communications Manager for any records that you have added to the database through the Cisco Unified Communications Manager Administration windows or for records that exist as default entries. To find records, you navigate to the Find and List window for the record that you want to locate, such as Find and List Phones (**Device > Phone**). You can search for all records or

enter search criteria to narrow your search. The search parameters vary, depending on the records for which you are searching. For example, when searching for a phone, you can search for phones with certain digits in the directory number or certain characters in the device name. When searching for an end user, you can search for first or last names that contain certain letters.

Once you have found records, you can delete them from the Find and List window that contains your records. You can delete individual records or delete all records that display in the window.

Use the following procedure to find and delete records from Cisco Unified Communications Manager Administration.

Procedure

Step 1 Navigate to the Find and List window in Cisco Unified Communications Manager Administration for the component that you want to find. For example, if you want to find a phone, choose **Device > Phone** to display the Find and List Phones window.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

Step 3 To filter or search records

- From the first drop-down list box, select a search parameter. The search parameter represents the field on which you want to search. The search parameters vary, depending on the records type.
- From the second drop-down list box, select a search pattern. The search pattern defines how the system searches the records. For example, you might want to search for records (or search parameters) that contain a certain value that you specify in the search text field.
- Specify the appropriate search text, if applicable. The search text allows you to specify values for which you want to search. Use this field with the search parameter and search pattern fields. For example, if you choose “Directory Number” from the search parameter drop-down list box, choose “contains” from the search pattern drop-down list box, and enter 5551212 as the search text, the system searches for a directory number that contains the digits 5551212.

Note To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the - button to remove the last added criterion or click the **Clear Filter** button to remove all added search criteria.

Step 4 Click **Find**.

All matching records 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.

You can reverse the sort order, by clicking the up or down arrow, if available, in the list header.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record(s) and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking the check box at the top of the column of check boxes and then clicking **Delete Selected**.

Step 5 From the list of records that display, click the link for the record that you want to view.

The window displays the item that you choose.

Additional Information

Cisco Unified Communications Manager Administration Basics, page 3-2

Adding and Copying Records

You can add items to the Cisco Unified Communications Manager by creating new records in Cisco Unified Communications Manager Administration and sometimes by copying existing records. Use the following procedure to add or copy records to the database.

Procedure

Step 1 Navigate to the Find and List window in Cisco Unified Communications Manager Administration for the component that you want to add (or copy). For example, if you want to add a trust element, choose **Advanced Services > Intercompany Media Services > Trust Element** to display the Find and List Trust Elements window.

Step 2 To add a new record, click the **Add New** button.

The window refreshes with a new record. Make the necessary changes, and click **Save**.

Step 3 To copy an existing record, do one of the following:

- In the Find and List window, click the **Copy** button, if available.
- Locate the record that you want to copy, as described in "Finding and Deleting Records" section on page 3-3. Choose the record, and click the **Copy** button in the configuration window. For example, find the trust element record that you want to copy, and click the **Copy** button in the Trust Element Configuration window.

The window refreshes with a new record. Make the necessary changes, and click **Save**.

Step 4 To copy an existing record and populate a new record with all of the associated information from the existing record:

- In the Find and List window, click the **Super Copy** button, if available.
- Locate the record that you want to copy, as described in "Finding and Deleting Records" section on page 3-3. Choose the record, and click the **Super Copy** button in the configuration window. For example, find the phone record that you want to copy, and click the **Super Copy** button in the Phone Configuration window.

The window refreshes with a new Device Name field. Make the necessary changes, and click **Save**.

Additional Information

Cisco Unified Communications Manager Administration Basics, page 3-2

Cisco IME Configuration Checklist

Table 3-1 provides an overview of the steps for configuring the Cisco Intercompany Media Engine (Cisco IME) feature in Cisco Unified Communications Manager Administration.

Note Before you begin, make sure that you have installed the Cisco Intercompany Media Engine software on the server and performed the post-installation tasks, including uploading the license file and enrolling the certificates. See the "Installation and Cisco IME Server Configuration" section on page 2-1.

Table 3-1 Cisco IME Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Make sure that you have the appropriate adaptive security appliance (ASA) license.	For information, refer to the *Cisco Unified Communications Manager Software Compatibility Matrix* at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html.
Step 2	To allow calls to get rerouted to the ingress gateway device immediately if the Cisco IME trunks fail for any reason, set the Retry Count for SIP Invite service parameter to a small value. Reasons include TCP connection timeouts occur or the off-path ASA goes offline. Cisco Systems recommends setting the parameter to a value of 2. **Tip** To determine if you have UDP trunks, check the transport type of the SIP security profile (**System > Security > SIP Trunk Security Profile**.) If you keep the default value of 6 and an ASA outage occurs, Cisco Unified Communications Manager takes up to a minute to revert a Cisco IME call to the PSTN. **Note** The Retry Count for SIP Invite service parameter applies to all SIP trunks that you configure on the Cisco Unified Communications Manager server.	1. Choose **System > Service Parameters**. 2. Choose the appropriate server from the Server drop-down list box. 3. Choose the Cisco CallManager service from the Service drop-down list box. 4. Set the value of the Retry Count for SIP Invite service parameter to the appropriate value. 5. Click **Save**.

Table 3-1 Cisco IME Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 3	Create an application user in Cisco Unified Communications Manager Administration. Cisco Unified Communications Manager uses the application user name and password configuration when you activate the Cisco IME service on the Cisco Unified Communications Manager. Cisco Unified Communications Manager obtains the IP address and port of the Cisco IME server and checks the application user name and password configuration for that server. Cisco Unified Communications Manager also checks the security setting and the application user information for the Cisco IME service. Cisco Unified Communications Manager initiates a connection to the Cisco IME server over TCP. If the security mode specifies encrypted, a TLS connection gets established. That TLS connection uses the self-signed certificate that is created for Cisco Unified Communications Manager upon installation. The certificate for the Cisco IME server must exist in the trust store on the Cisco Unified Communications Manager server. The Cisco Unified Communications Manager node accepts any certificate from the Cisco IME server that exists in the trust store. Once the connection gets established, Cisco Unified Communications Manager sends a Register message that contains the user ID and password that associate with the application user for the Cisco IME service. The Cisco IME server checks the credentials against its configured username and password.	From Cisco Unified Communications Manager Administration, choose **User Management > Application User** and click **Add New**. In the User ID and Password fields in the Application User Configuration window, enter the VAP username and password that you configured on the Cisco IME server by using the add vapusercredentials CLI command, as described in Step 9 of Table 2-6. Leave the other fields in the Application User Configuration window set to the default values. If the username and password values that you enter in the Application User window do not match those of the VAP username and password on the Cisco IME server, the Cisco Unified Communications Manager server cannot register with the Cisco IME server. **Note** You associate the application user to the server in the Intercompany Media Engine Server Connection Configuration window, as described subsequently in this checklist.

Table 3-1 Cisco IME Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 4	Ensure that the SIP security profile specifies the correct SIP listening port and the security mode to connect to the Cisco Intercompany Media Engine-enabled ASA. Check the Accept Out-of-Dialog REFER check box. **Note** You must check the Accept Out-of-Dialog REFER check box to allow mid-call fallback to the PSTN.	1. Choose **System > Security > SIP Trunk Security Profile**. 2. Ensure that the value that is selected from Device Security Mode drop-down list box enables you to connect to the ASA. The value must match what you have configured on the ASA. 3. Ensure that the Incoming Port field contains the correct value of the port that Cisco Unified Communications Manager uses to communicate with the ASA. By default, Cisco Unified Communications Manager uses port 5060. If you are using a non-default port, you need to enter that port here. 4. Check the Accept Out-of-Dialog REFER check box. 5. To allow the Cisco IME trunk to accept unsolicited notification, replaces header, presence subscription, and to transmit security status, choose the corresponding check boxes in the SIP Trunk Security Profile Configuration window.

Table 3-1 Cisco IME Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 5	Configure a SIP trunk to use with Cisco Intercompany Media Engine. The IME SIP trunk does not have a fixed destination IP address and port. Instead, the trunk obtains the remote IP address and port from the routing information that Cisco Unified Communications Manager learns through the Cisco IME network. IME SIP trunks do not support IPv6, so ensure that the IME trunk specifies IPv4 only. If you do not have IPv6 enabled on your system, this issue does not apply. **Note** You associate this trunk with an IME service later in this checklist.	1. Choose **Device > Trunk** and click **Add New**. 2. From the Trunk Type drop down list box, choose **SIP Trunk**. 3. From the Trunk Service Type drop-down list box, choose **Cisco Intercompany Media Engine**. 4. Click the **Next** button. 5. Configure the trunk by following these considerations: For Cisco IME calls, the incoming calling and called numbers always specify an +E.164 number format; that is, globalized numbers preceded by "+". Based on the Cisco Unified Communications Manager dial plan and the routing architecture, you may also need to define calling and called party number transformations or translation patterns to allow the called number to route within Cisco Unified Communications Manager. Otherwise, incoming Cisco IME calls will fail with a digit analysis error. For example, you may need to remove a leading "+" from the calling party number at the gateway level to allow the call to get routed in Cisco Unified Communications Manager. To configure the necessary transformations, configure the fields in the Inbound Calls group box. 6. Restart the trunk. For more information on configuring trunks, refer to the *Cisco Unified Communications Manager Administration Guide*.
Step 6	To enable music on hold for Cisco IME calls, you must set the Cisco CallManager service parameter Duplex Streaming Enabled to true. This parameter determines whether music on hold and Annunciator use duplex streaming.	1. Choose **System > Service Parameters**. 2. From the Server drop-down list box, choose a server. 3. From the Service drop-down list box, choose the Cisco CallManager service. 4. Set the Duplex Streaming Enabled parameter to True.
Step 7	Specify information about the Cisco IME server to which Cisco Unified Communications Manager connects, including the IP address and the port that VAP communications use.	Configuring Cisco IME Server Connections, page 3-14.

Table 3-1 Cisco IME Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 8	If you choose the Encrypted and Authenticated security mode for the Cisco IME server in Step 7, you must set up the TLS connection between the Cisco Intercompany Media Engine server and the into the Cisco IME server using third-party certificates or self-signed certificates.	Setting Up TLS Connections Between the Cisco Unified Communications Manager and Cisco Intercompany Media Engine Servers, page 3-16
Step 9	Create the enrolled groups to which you can assign enrolled patterns. The enrolled patterns specify which numbers can participate in Cisco IME calls. The enrolled groups specify a collection of enrolled patterns. After you create the enrolled group, create the enrolled patterns and assign the patterns to a group, as described in Step 10. **Tip** For information on configuring enrolled groups in bulk, refer to the refer to the *Cisco Unified Communications Manager Bulk Administration Guide*.	Configuring a Cisco IME Enrolled Group, page 3-19
Step 10	Specify the set of +E.164 numbers that you will allow to make and receive Cisco IME calls by creating enrolled patterns.	Configuring a Cisco IME Enrolled Pattern, page 3-21
Step 11	Create an exclusion group to associate to numbers that you will prevent from using Cisco IME. (Optional) **Tip** For information on configuring exclusion groups in bulk, refer to the refer to the *Cisco Unified Communications Manager Bulk Administration Guide*.	Configuring a Cisco IME Exclusion Group, page 3-22
Step 12	Specify numbers that you will prevent from using Cisco IME, including numbers of analog devices and fax machines. Associate the exclusion numbers with an exclusion group that you created in Step 11.	Configuring a Cisco IME Exclusion Number, page 3-23
Step 13	Create trust groups to which you can assign domains and prefixes, or trust elements, that the Cisco IME trusts (or does not trust). (Optional) **Note** If you do not configure trust groups, Cisco IME trusts all prefixes and domains. **Tip** For information on configuring trust groups in bulk, refer to the refer to the *Cisco Unified Communications Manager Bulk Administration Guide*.	Configuring a Cisco IME Trust Group, page 3-24

Table 3-1 Cisco IME Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 14	Specify the prefixes or domains that you want to trust or not trust and associate these trust elements with a trust group. You can only make Cisco IME calls to trusted elements. **Tip** For information on configuring trust elements in bulk, refer to the refer to the *Cisco Unified Communications Manager Bulk Administration Guide*.	Configuring a Cisco IME Trust Element, page 3-25
Step 15	Configure the Cisco IME service. This service defines the elements that you want this instance of Cisco IME to use, such as SIP trunk, trust group, exclusion group, and enrolled groups.	Configuring a Cisco IME Service, page 3-26
Step 16	Define external IP addresses and ports for each Cisco Unified Communications Manager in the cluster, and associate the addresses with the Cisco IME service.	Configuring External IP Address and Port Information, page 3-28
Step 17	Configure calling party and called party transformation patterns. **Note** Make sure to apply transformations and reset your trunks during a maintenance window.	Configuring Transformation Patterns for Cisco IME, page 3-29
Step 18	Configure two transformation profiles: one for incoming calling party numbers and one for incoming called party numbers. Transformation profiles allow the system to convert the calling and called party numbers for incoming calls to a fully qualified +E.164 number format. You associate the profiles with the Cisco IME transformations that are described in Step 19. The system includes the transformed numbers in the voice call records (VCRs) that Cisco IME uses to validate PSTN calls.	Configuring a Cisco IME Transformation Profile, page 3-30
Step 19	Configure Cisco IME +E.164 transformations. The transformations convert calling and called numbers on both the originating and terminating (incoming and outgoing) sides to +E.164 format after a PSTN call terminates. You associate this transformation with all of the PSTN access trunks in your system in Step 20.	Configuring Cisco IME E.164 Transformations, page 3-35
Step 20	Configure trunks to enable them to send VCRs to the Cisco IME server. You must configure any trunk that handles calls that might reach the PSTN.	Configuring PSTN Access Trunks, page 3-36

Table 3-1 Cisco IME Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 21	Review the feature parameters that apply to Cisco IME and make the appropriate changes. For instance, you may want to change the default value of the Enable Intradomain IME feature parameter. The default values of other feature parameters work for most configurations.	Configuring a Cisco IME Feature Configuration, page 3-37
Step 22	(Optional) If you want to prevent certain devices or trunks from making Cisco IME calls, set up a common device configuration with Cisco IME turned off for outgoing calls, then associate that common device configuration with a device. **Note** You can also disable Cisco Intercompany Media Engine from the Intercompany Media Services Feature Configuration window (**Advanced Features > Intercompany Media Services > Feature Configuration**) and create a common device configuration to enable Cisco IME for associated devices.	1. Choose **Device > Device Settings > Common Device Configuration**. 2. Create a common device configuration. To disable Cisco IME for devices that associate with this common device configuration, choose **Off** from the Use Intercompany Media (IME) for Outbound Calls drop-down list box. To enable Cisco IME, choose **On** from the drop-down list box. The default value equals the value that you set for the Use IME for Outbound Calls field in the Intercompany Media Services Feature Configuration window (**Advanced Features > Intercompany Media Services > Feature Configuration**). 3. Associate the appropriate devices with this common device configuration. For more information on associating devices with a common device configuration, refer to the *Cisco Unified Communications Manager Administration Guide*
Step 23	Verify the VAP connectivity between the Cisco IME server and the Cisco Unified Communications Manager server.	Verifying Connectivity, page 3-40
Configuring Fallback Information (Optional) If you configure mid-call fallback information, the system detects voice quality issues based on the threshold that you set and switches only the audio path to a different bearer channel, most likely the PSTN. You must configure fallback on both the originating and terminating sides of the call in order for fallback to work.		
Step 24	Ensure that you checked the Accept Out-of-Dialog REFER check box in the SIP Trunk Security Profile window to allow mid-call fallback to the PSTN, as described in Step 4.	
Step 25	To prevent timeouts during PSTN fallback, Cisco recommends that you increase the Media Exchange Stop Streaming Timer to 12 seconds. This parameter specifies the maximum seconds that the Cisco Unified Communications Manager waits to receive a response to a StopStreaming request. If the Cisco Unified Communications Manager does not receive a within the specified time, the Cisco Unified Communications Manager terminates the call.	1. Choose **System > Service Parameters**. 2. From the Server drop-down list box, choose a server. 3. From the Service drop-down list box, choose the Cisco CallManager service. 4. Set the Media Exchange Stop Streaming Timer parameter to 12 seconds.

Table 3-1 Cisco IME Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 26	Configure a fallback profile that defines several values that the Cisco Unified Communications Manager uses to fallback Cisco IME calls to the PSTN. (Optional) **Tip** During the fallback configuration, a device associates with a device pool. The device pool can associate with an enrolled group, and the enrolled group can specify a fallback profile that contains the necessary information to allow the fallback to be set up.	Configuring a Fallback Profile, page 3-43
Step 27	Associate the fallback profile with an enrolled group.	1. Choose **Advanced Features > Intercompany Media Services > IME Enrolled Group**. Find the enrolled group to associate with the fallback profile that you created. 2. From the Fallback Profile drop-down list box, choose the profile to associate with the selected enrolled group. 3. Click **Save**.
Step 28	Associate the enrolled group that you associated with a fallback profile to a device pool. **Tip** Devices associated with this device pool use caller ID for PSTN fallback using the patterns from the enrolled group in the device pool.	1. Choose **System > Device Pool**. 2. Find the device pool to which you want to associate the fallback profile that you configured in Step 27. 3. From the Intercompany Media Services Enrolled Group drop-down list box, choose the enrolled group. 4. Click **Save**.
Step 29	Review the fallback feature parameters that Cisco Unified Communications Manager uses for mid-call fallback of Cisco IME calls to the PSTN. The default settings apply to most configurations.	Configuring Fallback Feature Parameters, page 3-47
Configuring Off-path Settings (Optional) If you establish an off-path deployment in which inbound and outbound Cisco IME calls pass through an adaptive security appliance (ASA) that is enabled with the Cisco Intercompany Media Engine proxy but normal Internet-facing traffic does not flow through this ASA, you must configure the ASA that is enabled with the Cisco Intercompany Media Engine proxy as described in this section.		
Step 30	Configure the IP address and port of the ASA mapping service.	Configuring Intercompany Media Services Firewall Information, page 3-49
Step 31	Configure the following feature parameters that apply to the firewall settings: • Firewall Connection Request Timer for IME Calls • Firewall Mapping Response Timer for IME Calls • Firewall Mapping Connection Idle Timer for IME calls	Configuring a Cisco IME Feature Configuration, page 3-37

Table 3-1 Cisco IME Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
General Information		
Step 32	You can view the routes that the Cisco Intercompany Media Engine learned as well as enable and disable learned routes.	Cisco Intercompany Media Engine Learned Routes, page 3-49

Configuring Cisco IME Server Connections

Use the Intercompany Media Engine Server Connection Configuration window to specify information about the Cisco Intercompany Media Engine (Cisco IME) server to which Cisco Unified Communications Manager connects. The information that you provide enables Cisco Unified Communications Manager to connect to the Cisco IME server to initiate VAP messaging. The interface between servers allows Cisco Unified Communications Manager to publish its configured direct inward dialing (DID) patterns and to learn new routes.

After Cisco Unified Communications Manager establishes a connection, Cisco Unified Communications Manager sends a VAP Register message to the Cisco IME server. This message contains the username that associates with the application user that the Application User field specifies. The Cisco IME server checks the credentials against the configured VAP username and password that you configured in Step 9 of the "Post-Installation Tasks" section on page 2-17. If the values do not match, validation does not occur and the Cisco IME server cannot communicate with the Cisco Unified Communications Manager server.

Note Cisco recommends that you install the Cisco IME server and ensure that the server is functional before configuring the Cisco IME server in Cisco Unified Communications Manager Administration.

If you configure the Cisco IME server in Cisco Unified Communications Manager Administration, make sure to deactivate the Cisco Intercompany Media Engine service in the Intercompany Media Service Configuration window (**Advanced Features > Intercompany Media Services > Service**) until the Cisco Intercompany Media Engine servers become available.

If the Cisco IME servers are not available when you configure Cisco Unified Communications Manager Administration, Cisco Unified Communications Manager continues to attempt to connect to the Cisco Intercompany Media Engine server based on the reconnect interval that you configure for the Cisco Intercompany Media Engine service.

To access the Intercompany Media Engine Server Connection Configuration window, choose **Advanced Features > Intercompany Media Services > Server Connections**.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the "Cisco Unified Communications Manager Administration Basics" section on page 3-2 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 3-2 describes the Cisco IME server configuration settings.

For related procedures, see the "Cisco IME Configuration Checklist" section on page 3-6.

Table 3-2 Cisco IME Server Configuration Settings

Field	Description
Server Information	
Name	Name of the Cisco IME server, up to 50 characters. Specify a name that is unique in the cluster. Valid values include alphanumeric (a-z, A-Z, 0-9), period (.), dash (-), underscore (_), space ( ).
Description	Enter a descriptive name of the Cisco IME server. The description can comprise up to 128 characters. (Optional)
IP Address	Enter the IP address of the Cisco IME server to which Cisco Unified Communications Manager connects. You must enter an IPv4 address.
Port	Specify the port that the Cisco Unified Communications Manager server uses for Validation Access Protocol (VAP) communications to the Cisco IME server. The default specifies 5620. Valid values range from 0 to 65535. The port number that you enter must match the port number that you configured on the Cisco IME server, as described in Step 6 of Table 2-6.
Authentication Information	
Application User	Choose the application user that you configured in Step 3 of Table 3-1. The application user ID must match the vapusername that you configured in Step 6 of Table 2-6.

Table 3-2 Cisco IME Server Configuration Settings (continued)

Field	Description
Server Security Mode	Choose the appropriate security mode for communications between the Cisco Unified Communications Manager server and the Cisco IME server, either Authenticated or Encrypted and Authenticated. The security mode that you choose must match the security mode that you configured on the Cisco Intercompany Media Engine server, as described in Step 6 of Table 2-6. The Authenticated mode uses a digest-based authentication between the servers but does not encrypt the data. The Encrypted and Authenticated mode uses digest authentication that must run over a TLS connection between the Cisco Unified Communications Manager server and the Cisco IME server. If you choose Encrypted and Authenticated, you must upload the Cisco Intercompany Media Engine certificate into the Cisco Unified Communications Manager trust store by using the Cisco Unified Communications Operating System (**Security > Certificate Management**.). The default specifies Authenticated. Cisco strongly recommends that you choose the Encrypted and Authenticated mode. **Note** If you change the server security mode, the Cisco Unified Communications Manager closes the connections to the Cisco IME server.
Server Reconnect/VAP Retry Interval	Indicate the frequency (in seconds) with which you want the Cisco Unified Communications Manager server to try to connect to the Cisco IME server after losing connectivity. The Cisco Unified Communications Manager server tries to connect to the Cisco IME server indefinitely at this interval. Valid values include 60 through 600 seconds. The default specifies 120 seconds.

Additional Information

Cisco IME Configuration Checklist, page 3-6

Setting Up TLS Connections Between the Cisco Unified Communications Manager and Cisco Intercompany Media Engine Servers

You can set up TLS connections between the Cisco Unified Communications Manager and Cisco Intercompany Media Engine (Cisco IME) servers using self-signed certificates or third-party certificates. See the following procedures:

- Generating and Uploading a Self-Signed Certificate on the Cisco Intercompany Media Engine Server, page 3-17
- Generating and Uploading Third Party Certificates for Cisco Intercompany Media Engine, page 3-18

Generating and Uploading a Self-Signed Certificate on the Cisco Intercompany Media Engine Server

If you want to set up a TLS connection between the Cisco Unified Communications Manager and Cisco Intercompany Media Engine (Cisco IME) servers using self-signed certificates, you must generate the self-signed certificate and upload the certificate to the appropriate trust store.

Use this procedure to use self-signed certificates.

Procedure

Step 1 On the Cisco IME server, log into the Cisco IME command line interface (CLI) and enter the **show cert own IME** command.

The Cisco IME certificate displays.

Step 2 Copy the contents of the certificate from "-----BEGIN CERTIFICATE-----" to "-----END CERTIFICATE-----", and paste it to a file named IME_Cert.pem that you store on your PC.

Step 3 On the Cisco Unified Communications Manager server that is going to connect to the Cisco IME server, login to Cisco Unified Communications Operating System, and choose **Security > Certificate Management**.

Step 4 Click **Upload Certificate**.

The Upload Certificate dialog box opens.

Step 5 Choose **CallManager-trust** from the **Certificate Name** drop down list.

Step 6 Choose the file to upload by doing one of the following steps:

- In the **Upload File** text box, enter the path to the file.
- Click the **Browse** button and navigate to the file; then, click **Open**.

Step 7 To upload the file to the Cisco Unified Communications Manager server, click the **Upload File** button.

Uploading the Cisco Unified Communications Manager Signed Certificate to the Cisco IME Server

Step 8 On the Cisco Unified Communications Manager server, display the certificates. To do this, choose **Security >Certificate Management** from the in the Cisco Unified Communications Operating Systemand click **Find**.

Step 9 Choose the CallManager.pem certificate. The description of this certificate indicates that it is a self-signed certificate generated by the system.

Step 10 Save the file to you PC by choosing the **Download** button.

Step 11 Open the file on your PC using a text editor, and copy the contents of the file from "-----BEGIN CERTIFICATE-----" to "-----END CERTIFICATE-----".

Step 12 Log into the Cisco IME CLI and enter the **set cert import trust IME** command.

Step 13 Paste the previously copied certificate.

Step 14 Make sure that the authentication mode on the Cisco IME specifies "encrypted" by entering the CLI command **show ime vapserver** *vapservername*, where *vapservername* is the name of the VAP server instance that you created on the Cisco IME server.

Step 15 On the Cisco Unified Communications Manager server, make sure that you set the authentication mode to *Encrypted and Authenticated.* To do this, log into Cisco Unified Communications Manager Administration, and display the Intercompany Media Engine Server Connection Configuration window

(**Advanced Features > Intercompany Media Services > Server Connections**). Verify that the Server Security Mode for the corresponding Cisco IME Server equals *Encrypted and Authenticated*.

Verifying the Cisco Unified Communications Manager Signed Certificate Uploaded to the Cisco IME Server

Step 16 On the Cisco Unified Communications Manager server, display the CallManager.pem self-signed certificate by logging into the Cisco Unified Communications Operating System and choosing **Security > Certificate Management**. Click the **Find** button, and choose the CallManager.pem self-signed certificate from the list of certificates. The contents of the certificate displays.

Step 17 On the Cisco IME server, log into the Cisco IME CLI, locate the Cisco IME trust name by entering the **show cert list trust** command, and then enter the **show cert trust** *trust name* command.

Step 18 Compare the certificate content from the Cisco Unified Communications Manager server and the Cisco IME server and make sure that they match.

Note You must repeat this procedure for each Cisco Unified Communications Manager server that connects to the Cisco IME server.

Additional Information

Cisco IME Configuration Checklist, page 3-6

Generating and Uploading Third Party Certificates for Cisco Intercompany Media Engine

If you want to set up a TLS connection between the Cisco Unified Communications Manager and Cisco IME servers using third-party certificates, you must generate a Certificate Signing Request (CSR) and upload the certificates to the Cisco IME server. Then, generate the CSR and upload the third party certificate to the Cisco Unified Communications Manager server.

Use this procedure to generate the Certificate Signing Requests (CSRs) for the third party certificates and upload the certificates to the Cisco Unified Communications Manager and Cisco IME servers.

Procedure

Step 1 Generate the CSR for Cisco IME by logging into the Cisco IME command line interface (CLI) and entering the **set csr gen IME** command and then the **show csr own IME** command.

Step 2 Copy the CSR to the third party certificate agent (CA).

Step 3 Obtain and download the signed application certificate for Cisco IME and the root certificate from the CA.

Step 4 Import the root certificate to the Cisco IME server, by logging into the Cisco IME CLI and entering the **set cert import trust IME** command. Make note of the newly generated Cisco IME trust.

Step 5 Import the signed application certificate to the Cisco IME server by entering the **set cert import own IME** ***IME CA Cert*** command.

Step 6 Make sure that the authentication mode on the Cisco IME specifies encrypted by entering the **show ime vapserver** *vapservername* command, where *vapservername* is the name of the VAP server instance that you created on the Cisco IME server.

If you need to change the authentication mode, enter the **set ime vapserver authenticationmode** *vapservername* **encrypted** command.

Generating and Uploading a Third Party Certificate on the Cisco Unified Communications Manager Server

Step 7 Log into the Cisco Unified Communications Operating System, and choose **Security > Certificate Management**.

Step 8 Generate and download a CallManager CSR, as described in the *Cisco Unified Communications Operating System Administration Guide*. Make sure to choose CallManager from the Certificate Name drop-down list box.

Step 9 Obtain and download the third party signed application certificate and the root certificate from the certificate agent (CA) using the generated CSR.

Step 10 From the Cisco Unified Communications Operating System (**Security > Certificate Management**), upload the CallManager-Trust root certificate and CallManager signed certificate.

Step 11 Make sure that you set the authentication mode on the Intercompany Media Engine Server Connection Configuration window in Cisco Unified Communications Manager Administration (**Advanced Features > Intercompany Media Services > Server Connections**) to *Encrypted and Authenticated*.

Verify the certificate between Cisco IME and Cisco Unified Communications Manager

Step 12 In the Cisco Unified Communications Operating System, choose **Security > Certificate Management**.

Step 13 Find and display the CallManager root certificate that you uploaded in Step 10.

Step 14 Log into the Cisco IME server CLI, and use the **show cert trust list command** to obtain the name of the root certificate.

Step 15 Enter the **show cert trust** *filename* command, where filename equals the name of the certificate that you obtained in Step 14.

Step 16 Make sure that the root certificates on the Cisco Unified Communications Manager server and Cisco IME server match.

Note You must repeat Step 7 and Step 16 of this procedure for each Cisco Unified Communications Manager server that connects to the Cisco IME server.

Additional Information

Cisco IME Configuration Checklist, page 3-6

Configuring a Cisco IME Enrolled Group

You specify the numbers that you want to participate in Cisco Intercompany Media Engine (Cisco IME) by creating enrolled groups and patterns. Enrolled groups are a collection of enrolled patterns. These patterns define the set of +E.164 numbers that make and receive Cisco IME calls. Cisco IME publishes these numbers to the IME distributed cache. By doing so, Cisco IME makes these numbers available for other enterprises to learn through Cisco IME. Numbers within your enterprise must also match a pattern

in an enrolled group in order to make Cisco IME calls. You can create an enrolled group for each of your campuses or sites to facilitate incremental deployment of Cisco IME, starting with certain sites or campuses and extending the deployment as usage grows.

After you create the enrolled group, you create the enrolled patterns, assign the patterns to a group, and associate the group with a Cisco IME service. If you want to disable Cisco IME for certain phones in the enterprise, you can unassign the enrolled group for those phones from the Cisco IME service.

To access the IME Enrolled Group Configuration window, choose **Advanced Features > Intercompany Media Services > IME Enrolled Group**.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the "Cisco Unified Communications Manager Administration Basics" section on page 3-2 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 3-3 describes the Cisco IME enrolled group configuration settings.

For related procedures, see the "Cisco IME Configuration Checklist" section on page 3-6.

Table 3-3 Cisco Intercompany Media Engine Enrolled Group Configuration Settings

Field	Description
Group Name	Enter a unique name for the enrolled group. The name must be at least one character and can include up to 32 characters.
Description	Enter a description for the enrolled group. The description can include up to 128 characters. (Optional)
Fallback Profile	Choose the fallback profile that you want to associate to this enrolled group. The fallback profile defines how Cisco Unified Communications Manager handles fallback to the PSTN for numbers that are associated with this enrolled group. If you choose *None*, calls to direct inward dialing numbers (DIDs) in this pattern group do not fallback to the PSTN. Configure fallback profiles in the Fallback Profile Configuration window. For more information, see the "Configuring a Fallback Profile" section on page 3-43. **Note** If you are setting up Cisco IME for the first time, Cisco Systems recommends that you complete the rest of the Cisco Unified Communications Manager Administration configuration before you choose a fallback profile from this field.

Table 3-3 Cisco Intercompany Media Engine Enrolled Group Configuration Settings (continued)

Field	Description
All Patterns in Group Are Aliases	Check this check box if all of the patterns within the group need to be aliases to each other. For example, check this check box if you have 18xx numbers for which you enrolled the +E.164 numbers, but the service provider performs mapping from the 18xx number and provides the DID as the called party number for the 18xx instead. Check this check box only if the patterns specify exact aliases to other patterns in the same group. Only exact patterns can be aliases; no wild cards are allowed.

Additional Information

Cisco IME Configuration Checklist, page 3-6

Configuring a Cisco IME Enrolled Pattern

Cisco Intercompany Media Engine (Cisco IME) enrolled patterns define the set of +E.164 numbers that make and receive Cisco IME calls. Cisco IME publishes these numbers to the IME distributed cache. By doing so, Cisco IME makes these numbers available for other enterprises to learn through Cisco IME. The patterns must specify valid direct inward dialing numbers (DIDs) that the enterprise owns. Numbers within your enterprise must match a pattern that is found in an enrolled group in order to make Cisco IME calls.

To eliminate the need for day-to-day provisioning of specific numbers as individual phones are added to and removed from the system, you can add a pattern that represents a large group of numbers for a given site. The enrolled pattern can include numbers that you have not assigned to a phone. Numbers that are not associated to a phone cannot be validated.

After you create enrolled patterns, you associate them to an enrolled group and assign the enrolled group to a Cisco Intercompany Media Engine service. You can disable or enable Cisco IME from calling certain phones in the enterprise by disassociating or associating the enrolled group to the Cisco IME service.

Note You can exclude specific numbers that fall within the range of an enrolled pattern from participating in Cisco IME by configuring exclusion groups and exclusion numbers. For more information, see the "Configuring a Cisco IME Exclusion Group" section on page 3-22 and "Configuring a Cisco IME Exclusion Number" section on page 3-23.

To access the IME Enrolled Pattern Server Configuration window, choose **Advanced Features > Intercompany Media Services > Enrolled Pattern**.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the "Cisco Unified Communications Manager Administration Basics" section on page 3-2 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 3-4 describes the Cisco IME enrolled pattern configuration settings.

For related procedures, see the "Cisco IME Configuration Checklist" section on page 3-6.

Table 3-4 Cisco Intercompany Media Engine Enrolled Pattern Configuration Settings

Field	Description
Pattern	Create a unique pattern that contains the following characteristics: • Begins with a plus sign (+). • Contains up to 15 digits, including numbers between 0 and 9 and up to 3 wildcard (X) characters at the end of the pattern. • Wildcard characters represent numbers between 0 and 9. The following patterns represent valid enrolled patterns: • +14089021xxx • +191937611xx • +14089523513
Description	Enter a descriptive name for the enrolled pattern. The description can contain up to 128 characters. (Optional)
Enrolled Group	Choose the Cisco IME enrolled group to associate with this enrolled pattern. **Note** To configure more enrolled groups, see the "Configuring a Cisco IME Enrolled Group" section on page 3-19

Additional Information

Cisco IME Configuration Checklist, page 3-6

Configuring a Cisco IME Exclusion Group

Exclusion groups contain a list of numbers that you want to prevent from using Cisco Intercompany Media Engine (Cisco IME), including numbers of analog devices and fax machines. You create the exclusion group first and then you create exclusion numbers that you associate with a particular exclusion group. Then, you associate the exclusion group to the Cisco IME service.

This section describes how to create an exclusion group.

To access the Intercompany Media Services Exclusion Group Configuration window, choose **Advanced Features > Intercompany Media Services > Exclusion Group**.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the "Cisco Unified Communications Manager Administration Basics" section on page 3-2 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 3-5 describes the Cisco IME exclusion group configuration settings.

For related procedures, see the "Cisco IME Configuration Checklist" section on page 3-6.

Table 3-5 Cisco Intercompany Media Engine Exclusion Group Configuration Settings

Field	Description
Name	Enter a unique name for the exclusion group. The name can comprise up to 32 characters in length.
Description	Enter a descriptive name of the exclusion group. The description can comprise up to 128 characters. (Optional)

Additional Information

Cisco IME Configuration Checklist, page 3-6

Configuring a Cisco IME Exclusion Number

Use the Intercompany Media Services Exclusion Number Configuration window to define numbers, sets of numbers, prefixes, or set of prefixes that you do not want to use Cisco Intercompany Media Engine (Cisco IME), even if these numbers occur within a list of numbers that is included in the Cisco IME enrolled pattern.

To access the Intercompany Media Services Exclusion Number Configuration window, choose **Advanced Features > Intercompany Media Services > Exclusion Number**.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the "Cisco Unified Communications Manager Administration Basics" section on page 3-2 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 3-6 describes the Cisco IME exclusion number settings.

For related procedures, see the "Cisco IME Configuration Checklist" section on page 3-6.

Table 3-6 Cisco Intercompany Media Engine Exclusion Number Configuration Settings

Field	Description
Pattern	Specify the +E.164 number that you want to exclude from Cisco IME. You must precede the number by a plus sign (+). The number may contain up to 15 digits. You must enter the exact +E.164 number with no wildcards.
Description	Enter a descriptive name of the exclusion number. The description can comprise up to 128 characters. (Optional)

Table 3-6 Cisco Intercompany Media Engine Exclusion Number Configuration Settings

Field	Description
Exclusion Group	From the drop-down list box, choose the Cisco IME group to associate with this exclusion number. To configure additional exclusion groups, see the "Configuring a Cisco IME Exclusion Group" section on page 3-22.

Additional Information

Cisco IME Configuration Checklist, page 3-6

Configuring a Cisco IME Trust Group

Cisco Intercompany Media Engine (Cisco IME) trust groups contain a list of domains and prefixes that are trusted (or not trusted) by the Cisco IME service that associates with the trust group. Cisco Unified Communications Manager can only place Cisco IME calls to domains or prefixes that are trusted.

Configuration of trust groups is optional. If you do not create trust groups, Cisco IME trusts all calls by default.

This section describes how to configure a trust group. For information on creating domains and prefixes to include in the trust group, see the "Configuring a Cisco IME Trust Element" section on page 3-25.

To access the Intercompany Media Services Trusted Group Configuration window, choose **Advanced Features > Intercompany Media Services > Trust Group**.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the "Cisco Unified Communications Manager Administration Basics" section on page 3-2 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 3-7 describes the intercompany media services trust group configuration settings.

For related procedures, see the "Cisco IME Configuration Checklist" section on page 3-6.

Table 3-7 Intercompany Media Services Trust Group Configuration Settings

Field	Description
Name	Enter a unique name for the trust group. The name can comprise up to 32 characters in length.
Description	Enter a descriptive name of the trust group. The description can comprise up to 128 characters. (Optional)

Table 3-7 Intercompany Media Services Trust Group Configuration Settings (continued)

Field	Description
Trusted	Choose a trust value from the drop-down list box, either Yes (trusted) or No (untrusted). You cannot change this value if any trust elements use this trust group. This limitation prevents you from accidentally changing an untrusted group (or blacklist) to a trusted group (or whitelist) by changing one value. No default value exists. You must select a value.

Additional Information

Cisco IME Configuration Checklist, page 3-6

Configuring a Cisco IME Trust Element

Cisco Intercompany Media Engine (Cisco IME) trust elements specify prefixes or domain that you want to trust or not trust. You include the trust elements in a trust group. Cisco Unified Communications Manager can only place Cisco IME calls to domains or prefixes that are trusted. You cannot receive Cisco IME calls from a number whose prefix or domain is specified in an untrusted element.

This section describes how to create trust elements and how to associate the trust elements with a trust group. After you create the trust elements, you associate trust groups with an Cisco IME service to trust or not trust the prefixes or domains that the trust group specifies.

To access the Intercompany Media Services Trust Element Configuration window, choose **Advanced Features > Intercompany Media Services > Trust Element**.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the "Cisco Unified Communications Manager Administration Basics" section on page 3-2 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 3-8 describes the intercompany media services trust element configuration settings.

For related procedures, see the "Cisco IME Configuration Checklist" section on page 3-6.

Table 3-8 Intercompany Media Services Trust Element Configuration Settings

Field	Description
Name	Enter a domain name or a prefix. Domain names can contain up to 128 characters. You must specify a valid domain name. Prefixes must begin with a "+" sign followed by up to 15 characters or up to 14 characters and a wildcard "!".
Description	Enter a descriptive name for the engine trust element. The description can comprise up to 128 characters. (Optional)

Table 3-8 Intercompany Media Services Trust Element Configuration Settings (continued)

Field	Description
Element Type	Choose the appropriate element type, either “Domain” or “Prefix.”
Trust Group	Choose the appropriate trust group. To include this element in a whitelist (trusted group), choose a trusted group from the drop-down list box. To include this element in a blacklist (untrusted group), choose an untrusted group from the drop-down list box. For information on configuring trust groups, see the “Configuring a Cisco IME Trust Group” section on page 3-24

Additional Information

Cisco IME Configuration Checklist, page 3-6

Configuring a Cisco IME Service

Use the Intercompany Media Service Configuration window to configure and activate the Cisco Intercompany Media Engine (Cisco IME) service. To configure the Cisco IME service in Cisco Unified Communications Manager Administration, you associate various components that you have already configured, including trusted groups, enrolled groups, and exclusion groups. You indicate the Cisco IME server with which you want Cisco Unified Communications Manager to communicate. Communications between the Cisco Unified Communications Manager and the Cisco IME servers begin after you configure and activate the Cisco IME service.

To begin load balancing so that the system work spreads across multiple Cisco Intercompany Media Engine servers, create more than one Cisco Intercompany Media Engine service with different Cisco Intercompany Media Engine servers and move some of the enrolled groups from the old Cisco Intercompany Media Engine service to the new service.

To access the Intercompany Media Service Configuration window, choose **Advanced Features > Intercompany Media Services > Service**.

For information about the CUCM External Address List pop-up window, see the “Configuring External IP Address and Port Information” section on page 3-28.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the “Cisco Unified Communications Manager Administration Basics” section on page 3-2 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 3-9 describes the intercompany media service configuration settings.

For related procedures, see the "Cisco IME Configuration Checklist" section on page 3-6.

Table 3-9 Intercompany Media Service Configuration Settings

Field	Description
Intercompany Media Service Information	
Name	Enter a unique name for the Cisco IME service. The name can comprise up to 50 characters in length.
Description	Enter a descriptive name for the Cisco IME service. The description can comprise up to 128 characters in length. (Optional)
Domain	Enter the domain name to use with Cisco IME. Typically, you specify the domain name of your enterprise, such as cisco.com. The domain name must match the domain name that is contained in the SSL certificate from GoDaddy.com for the ASA.
SIP Trunk	Choose the SIP trunk that you want to use with this service. The drop-down list box populates with trunks that specify the Cisco Intercompany Media Engine trunk service type. The trunk that you select runs on a specific set of nodes in the cluster, as defined by the Cisco Unified Communications Manager group that associates with the trunk. The Cisco IME service also runs on that same set of nodes. **Tip** You configured Cisco Intercompany Media Engine trunks in Step 5 of the "Cisco IME Configuration Checklist" section on page 3-6.
Trust Group	If desired, choose a trust group. Trust groups contain a list of domains and prefixes that are trusted (or untrusted) by the Cisco IME service with which the group associates. Cisco Unified Communications Manager can only place Cisco IME calls to domains or prefixes that are trusted. The drop-down list box populates with servers that you configured in the Intercompany Media Services Trust Group Configuration window (**Advanced Features > Intercompany Media Services > IME Trusted Group**). If you do not choose a trust group, Cisco IME trusts all prefixes and domains.
Exclusion Group	If desired, choose an exclusion group. Exclusion groups contain numbers that you want to prevent from using Cisco Intercompany Media Engine. The drop-down list box populates with servers that you configured in the Intercompany Media Services Exclusion Group Configuration window (**Advanced Features > Intercompany Media Services > IME Exclusion Group**).
Firewall	If you are using an off-path ASA deployment model, choose the firewall to associate with this service.

Table 3-9 Intercompany Media Service Configuration Settings (continued)

Field	Description
Available Enrolled Groups	This list box displays the enrolled groups that are available for association with this Cisco IME service. Enrolled groups specify the set of +E.164 numbers that make and receive Cisco IME calls. To associate an enrolled group with this Cisco IME service, select the enrolled group and click the Down arrow below this list box.
Selected Enrolled Groups	This list box displays the enrolled groups that associate with this Cisco IME service. To remove an enrolled group, select the enrolled group name and click the Up arrow above this list box. To add an enrolled group, select an enrolled group in the Available Enrolled Groups list box and click the Down arrow between the list group boxes. You can reorder the enrolled groups by clicking the Up and Down arrows to the right of the list box.
Activated	Check the Activated check box to activate the Cisco IME service. If you do not activate the service, you cannot make and receive Cisco IME calls.
Server Information	
Primary IME Server	Choose a primary Cisco IME server. The drop-down list box populates with servers that you configure in the Intercompany Media Server Connection Configuration window (**Advanced Features > Intercompany Media Services > Server Connections**). You can use the selected server in more than one service. If you define multiple Cisco IME services but you have only one Cisco IME server, you can associated multiple Cisco IME services with a single server.
Secondary IME Server	(Optional) Choose a secondary Cisco IME server. The drop-down list box populates with servers that you configure in the Intercompany Media Server Connection Configuration window (**Advanced Features > Intercompany Media Services > Server Connections**). You must choose different servers for the primary and secondary Cisco IME servers. You can use the selected server in more than one service.

Additional Information

Cisco IME Configuration Checklist, page 3-6

Configuring External IP Address and Port Information

Use the CUCM External Address List pop-up window to define an external IP address and port for each Cisco Unified Communications Manager in the cluster. The IP address and port represent the global (or real) address that the Cisco Unified Communications Manager advertises to the Cisco Intercompany

Media Engine (Cisco IME) service. Other enterprises learn this address and use it to route Cisco IME calls. Ensure that all enterprises that use Cisco IME can resolve the IP address or hostname that you provide.

For inbound calls, the Cisco Intercompany Media Engine-enabled ASA utilizes network address translation (NAT). A specific IP/port on one of the ASA interfaces has a static mapping to each Cisco Unified Communications Manager node on the inside. Cisco Unified Communications Manager, through its existing configuration, advertises the IP/port on the ASA instead. As a result, inbound calls arrive at the Cisco Intercompany Media Engine-enabled ASA.

You need to provide external IP addresses or hostnames if your Cisco Unified Communications Manager servers reside behind a firewall or NAT.

To access the CUCM External Address List pop-up window, find the Cisco IME service to which you want to associate the IP Address and port by choosing **Advanced Features > Intercompany Media Services > Service**. From the Related Links drop-down list box in the Intercompany Media Service Configuration window, choose the **Add/Update CUCM External Address List** option and click **Go**.

Table 3-10 describes the address list configuration settings.

For related procedures, see the "Cisco IME Configuration Checklist" section on page 3-6.

Table 3-10 CUCM External Address List Configuration Settings

Field	Description
CUCM External Address List	
Cisco Unified CM	Displays the Cisco Unified Communications Manager servers in your system.
IP Address/Host	Enter the IP address or hostname that you want other enterprises to use to route calls to your enterprise. You must provide an IP address or hostname that all enterprises that use Cisco IME can resolve.
Port	Enter the port to use for external Cisco IME traffic.

Additional Information

Cisco IME Configuration Checklist, page 3-6

Configuring Transformation Patterns for Cisco IME

Configure transformation patterns of called and calling party numbers so that the transformations provide +E.164 numbers. You may need to add or remove digits as well as prefix digits including the "+" sign to get the numbers in +E.164 format.

To access the Calling Party Transformation Pattern Configuration window, choose **Call Routing > Transformation > Transformation Pattern > Calling Party Transformation Pattern**.

To access the Called Party Transformation Pattern Configuration window, choose **Call Routing > Transformation > Transformation Pattern > Called Party Transformation Pattern**.

For calling and called party transformation pattern configuration settings, refer to the *Cisco Unified Communications Manager Administration Guide* or choose **Help > This Page** in the respective window in Cisco Unified Communications Manager Administration.

For related procedures, see the "Cisco IME Configuration Checklist" section on page 3-6.

Additional Information

Cisco IME Configuration Checklist, page 3-6

Configuring a Cisco IME Transformation Profile

Transformation profiles allow the system to convert the calling and called party numbers for outgoing calls to a fully qualified +E.164 number format. The system includes the transformed numbers in the voice call records (VCRs) that Cisco Intercompany Media Engine (Cisco IME) uses to validate PSTN calls. The number transformation takes place after normal call routing processing. Cisco Unified Communications Manager does not use transformation profiles for call routing.

You must create one profile for the incoming called number and one for the incoming calling number. You associate the transformation profiles with the Cisco IME transformation as described in "Configuring Cisco IME E.164 Transformations" section on page 3-35.

Note Cisco IME does not upload VCRs that do not contain numbers in +E.164 format.

To access the Transformation Profile Configuration window, choose **Call Routing > Transformation > Transformation Profile**.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the "Cisco Unified Communications Manager Administration Basics" section on page 3-2 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 3-11 describes the transformation profile configuration settings.

For related procedures, see the "Cisco IME Configuration Checklist" section on page 3-6.

Table 3-11 Cisco Intercompany Media Engine Transformation Profile Configuration Settings

Field	Description
Transformation Profile Information	
Name	Enter a unique name for the transformation profile. The name can comprise up to 50 characters in length.
Description	Enter a descriptive name for the transformation profile. The description can comprise up to 128 characters in length. (Optional)
Incoming Party Setting	
Clear Prefix Settings	To delete prefixes for all calling party number types, click the **Clear Prefix Settings** button.
Default Prefix Settings	To reset prefixes for all calling party number types to the default values, click the **Default Prefix Settings** button.

Table 3-11 Cisco Intercompany Media Engine Transformation Profile Configuration Settings

Field	Description
National Number	Configure the following settings to globalize calling party numbers that use National for the Number Type. The National number type gets used for calls within your country. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use National for the Calling Party Number Type. You can enter up to eight characters, which include digits, the international escape character (+), asterisk (*), or the octothorpe (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field in the Gateway Configuration or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway Configuration or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that applies to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip-digit functionalities. **Tip** To configure the Strip Digits field in the Device Pool Configuration, Gateway Configuration, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of National number type before Cisco Unified Communications Manager applies the prefixes. • Calling Search Space—This setting allows you to globalize the calling party number of National calling party number type on the device. Make sure that the calling search space that you choose contains the calling party transformation pattern that you want to assign to this device.

Table 3-11 Cisco Intercompany Media Engine Transformation Profile Configuration Settings

Field	Description
International Number	Configure the following settings to globalize calling party numbers that use International for the Number Type. The International number type gets used for calls outside the dialing plan for your country. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use International for the Calling Party Numbering Type. You can enter up to eight characters, which include digits, the international escape character (+), asterisk (*), or the octothorpe (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field in the Gateway Configuration or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway Configuration or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that applies to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip-digit functionalities. **Tip** To configure the Strip Digits field in the Device Pool Configuration, Gateway Configuration, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of International type before Cisco Unified Communications Manager applies the prefixes. • Calling Search Space—This setting allows you to globalize the calling party number of International calling party number type on the device. Make sure that the calling party transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. **Tip** Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing.

Table 3-11 Cisco Intercompany Media Engine Transformation Profile Configuration Settings

Field	Description
Unknown Number	Configure the following settings to globalize calling party numbers that use Unknown for the Number Type. The Unknown number type gets used when the dialing plan is unknown. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use Unknown for the Calling Party Numbering Type. You can enter up to eight characters, which include digits, the international escape character (+), asterisk (*), or the octothorpe (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field in the Gateway Configuration or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway Configuration or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that applies to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip-digit functionalities. **Tip** To configure the Strip Digits field in the Device Pool Configuration, Gateway Configuration, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of Unknown type before Cisco Unified Communications Manager applies the prefixes. • Calling Search Space—This setting allows you to globalize the calling party number of Unknown calling party number type on the device. Make sure that the calling party transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. **Tip** Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing.

Table 3-11 Cisco Intercompany Media Engine Transformation Profile Configuration Settings

Field	Description
Subscriber Number	Configure the following settings to globalize calling party numbers that use Subscriber for the Number Type. The Subscriber number type gets used when you are dialing a subscriber by using a shortened subscriber number. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use Subscriber for the Calling Party Numbering Type. You can enter up to eight characters, which include digits, the international escape character (+), asterisk (*), or the octothorpe (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field in the Gateway Configuration or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway Configuration or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that applies to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip-digit functionalities. **Tip** To configure the Strip Digits field in the Device Pool Configuration, Gateway Configuration, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of Subscriber type before Cisco Unified Communications Manager applies the prefixes. • Calling Search Space—This setting allows you to globalize the calling party number of Subscriber calling party number type on the device. Make sure that the CSS that you choose contains the calling party transformation pattern that you want to assign to this device. **Tip** Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing.

Additional Information

Cisco IME Configuration Checklist, page 3-6

Configuring Cisco IME E.164 Transformations

Cisco Intercompany Media Engine (Cisco IME) E.164 transformations convert calling numbers and called numbers on both the originating and terminating (incoming and outgoing) sides to +E.164 format after a PSTN call terminates. Cisco IME E.164 transformations do not impact call routing or digit analysis in Cisco Unified Communications Manager. The transformations allow the following actions to occur:

- Send UploadVCRs to the Cisco Intercompany Media Engine server for unlearned direct inward dialing numbers (DIDs).
- Reroute calls to the Cisco IME trunk if the DID exists in the learned table.

You associate Cisco IME E.164 transformations with a PSTN access trunk. If the transformation does not yield valid calling and called numbers on the incoming and outgoing sides of the call, no VCR upload takes place, and Cisco IME processing stops for that call.

To access the Intercompany Media Services E.164 Transformation Configuration window, choose **Advanced Features > Intercompany Media Services > E.164 Transformation**.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the "Cisco Unified Communications Manager Administration Basics" section on page 3-2 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 3-12 describes the transformation configuration settings.

For related procedures, see the "Cisco IME Configuration Checklist" section on page 3-6.

Table 3-12 Cisco Intercompany Media Engine E.164 Transformation Configuration Settings

Field	Description
E.164 Transformation	
Name	Enter a unique name for the transformation profile. This name can comprise up to 50 characters in length.
Description	Enter a descriptive name for the transformation profile. The description can comprise up to 128 characters in length. (Optional)
Outgoing Calling Party Settings	
Outgoing Party E.164 Transformation CSS	From the drop-down list box, choose the appropriate calling search space for the calling party on outgoing calls. Choose a calling search space that contains the partitions used by the calling party transformation pattern that you configured on the Calling Party Transformation window (**Call Routing > Transformation > Transformation Pattern > Calling Party Transformation Pattern**).

Table 3-12 Cisco Intercompany Media Engine E.164 Transformation Configuration Settings (continued)

Field	Description
Apply On	Choose whether you want to apply the calling search space to the original number or to the routing transformed number.
Outgoing Called Party Settings	
Outgoing Party E.164 Transformation CSS	From the drop-down list box, choose the appropriate calling search space for the called party on outgoing calls. Choose a calling search space that contains the partitions used by the called party transformation pattern that you configured on the Called Party Transformation window (**Call Routing > Transformation > Transformation Pattern > Called Party Transformation Pattern**).
Apply On	Choose whether you want to apply the calling search space to the original number or to the routing transformed number.
Incoming Transformation Profile Settings	
Incoming Calling Party Transformation Profile	Choose the appropriate incoming calling party transformation profile that you configured in the Transformation Profile Configuration window (**Call Routing > Transformation > Transformation Profile**), as described in the "Configuring a Cisco IME Transformation Profile" section on page 3-30.
Incoming Called Party Transformation Profile	Choose the appropriate incoming called party transformation profile that you configured in the Transformation Profile Configuration window (**Call Routing > Transformation > Transformation Profile**), as described in the "Configuring a Cisco IME Transformation Profile" section on page 3-30.

Additional Information

Cisco IME Configuration Checklist, page 3-6

Configuring PSTN Access Trunks

Configure any SIP, MGCP, or H.323 trunk that handles calls that might reach the PSTN as a PSTN trunk. PSTN access trunks enable the system to send voice call records (VCRs) to the Cisco Intercompany Media Engine (Cisco IME) server. To configure PSTN access trunks, check the PSTN Access check box in the Trunk Configuration window and choose the appropriate E.164 transformation. If you do not configure a PSTN access trunk, Cisco Unified Communications Manager does not upload VCRs after calls terminate.

If a SIP trunk in your network connects to a SIP gateway that connects to the PSTN, you can configure this SIP trunk as a PSTN access trunk. If another SIP trunk that is an intercluster trunk connects to another cluster in your network, you do not have to configure this SIP trunk as a PSTN access trunk, because calls from this trunk will never go to the PSTN.

Procedure

Step 1 Choose **Device > Trunk**, and find a trunk that you want to configure as a PSTN access trunk.

Step 2 Check the PSTN Access check box.

Step 3 From the E.164 Transformation Profile drop-down list box, choose the appropriate E.164 transformation profile that you configured in the E.164 Transformation Configuration window (**Advanced Features > Intercompany Media Services > E.164 Transformation**). The profile transforms the called party and calling party numbers to +E.164 format. Numbers must use +E.164 format for call validation.

If you do not choose a profile from this drop-down list box, Cisco Unified Communications Manager does not upload VCRs to the Cisco Intercompany Media Engine server.

Additional Information

Cisco IME Configuration Checklist, page 3-6

Configuring a Cisco IME Feature Configuration

Use the Intercompany Media Services Feature Configuration window to configure feature parameters that apply to Cisco Intercompany Media Engine (Cisco IME).

To access the Intercompany Media Services Feature Configuration window, choose **Advanced Features > Intercompany Media Services > Feature Configuration**.

Configuration Settings Table

Table 3-13 describes the Intercompany Media Services feature configuration settings.

For related procedures, see the "Cisco IME Configuration Checklist" section on page 3-6.

Table 3-13 Intercompany Media Services Feature Configuration Settings

Field	Description
Intercompany Media Services Parameters	
Allow IME Calls through MGCP FXS/FXOs	Indicate whether Cisco IME allows MGCP FXS/FXO analog gateway devices, such as those used to connect to fax machines, to make Cisco IME calls. Choose *True* to allow MGCP FXO/FXS gateways to make Cisco IME calls. Choose *False* to prevent MGCP FXO/FXS gateways from making Cisco IME calls. The default value specifies False.
Enable Intradomain IME	Indicate whether you want to enable Cisco IME for calls to another cluster within your enterprise. Generally, intercluster trunks manage calls between clusters; however, if you are using the PSTN between clusters within the same domain, you can use Cisco IME to learn the patterns between those clusters by enabling this field. Choose *True* to enable Cisco IME between clusters in the same enterprise domain. Choose *False* to disable Cisco IME between clusters in the same enterprise domain The default value specifies False.

Table 3-13 Intercompany Media Services Feature Configuration Settings (continued)

Field	Description
Allow MWI via IME Learned Routes	Indicate whether Cisco Unified Communications Manager can use Cisco IME learned routes for message waiting indicator (MWI) notifications. Choose True to allow Cisco Unified Communications Manager to use Cisco IME learned routes for MWI messages. Choose False to prevent Cisco Unified Communications Manager from using Cisco IME learned routes for MWI messages. The default value specifies True.
SIP Trunk IME Connection Timer for Destination Enterprise	Specify the amount of time in seconds that a Cisco IME SIP trunk attempts to establish a connection to a SIP uniform resource identifier (URI) that exists for a learned route to a destination enterprise. When this timer expires, the SIP trunk attempts to establish a connection to the next URI, if available, for that learned route to the destination enterprise. The default value specifies 2 seconds. Valid values range from 1 to 5.
Firewall Connection Request Timer for IME Calls	Specify the amount of time, in seconds, that the Cisco Unified Communications Manager waits to establish a TCP connection with the Cisco IME firewall. If the firewall does not send a connection response to the Cisco Unified Communications Manager connection request before the timer expires, Cisco Unified Communications Manager continues the call without going through the Cisco IME firewall. In other words, Cisco Unified Communications Manager makes a PSTN call. The default value specifies 2 seconds. Valid values range from 1 to 5.
Firewall Mapping Response Timer for IME Calls	Specify the amount of time, in seconds, that the Cisco Unified Communications Manager waits to complete a mapping transaction (request and response) with the Cisco IME firewall. If the firewall does not send a mapped address response to the Cisco Unified Communications Manager mapped address request before the timer expires, Cisco Unified Communications Manager continues the call without going through the Cisco IME firewall. In other words, Cisco Unified Communications Manager makes a PSTN call. The default value specifies 2 seconds. Valid values range from 1 to 5.

Table 3-13 Intercompany Media Services Feature Configuration Settings (continued)

Field	Description
Firewall Mapping Connection Idle Timer for IME calls	Specify the amount of time, in minutes, that the connection between the Cisco Unified Communications Manager and the Cisco IME firewall can remain idle before Cisco IME firewall tears down the connection with the Cisco Unified Communications Manager. This timer begins when Cisco Unified Communications Manager stops sending new call requests to the Cisco IME firewall. You can choose a higher value in this field to decrease delay in establishing new calls through the Cisco IME firewall, or you can choose a lower value to close the connection sooner. A lower value enhances security but may cause a minor delay in establishment of new calls. The default value specifies 10. Valid values range from 5 to 60.
ICM Failed Call Attempt Threshold	Specify the percentage of failed Cisco IME call attempts to exceed before Cisco Unified Communications Manager generates the IMEQualityAlertEntry alarm. When the percentage of failed Cisco IME call setup attempts falls below the threshold defined in this field and the system does not exceed the fallback threshold that the IME Call Fallback Attempt Threshold field specifies, Cisco Unified Communications Manager triggers the IMEQualityAlertExit alarm, which clears the IMEQualityAlertEntry alarm. Entering a higher threshold value makes the system more tolerant of failed Cisco IME call attempts, so that more calls fail before Cisco Unified Communications Manager triggers an alarm. A higher value may be useful during minor network outages. Entering a lower threshold value makes the system less tolerant of Cisco IME call setup failures, so fewer calls fail before Cisco Unified Communications Manager triggers an IMEQualityAlertEntry alarm. The default value specifies 50 percent. Valid values range from 10 to 100.

Table 3-13 Intercompany Media Services Feature Configuration Settings (continued)

Field	Description
ICM Call Fallback Attempt Threshold	Specify the percentage of active Cisco IME calls that fallback to the PSTN to exceed before Cisco Unified Communications Manager generates the IMEQualityAlertEntry alarm. When the percentage of Cisco IME calls that experience mid-call fallback to the PSTN falls below the threshold defined in this field and the percentage of failed Cisco IME call setup attempts falls below the value specified in the IME Failed Call Attempt Threshold field, Cisco Unified Communications Manager generates the IMEQualityAlertExit alarm, which clears the IMEQualityAlertEntry alarm. Entering a higher threshold value makes the system more tolerant of Cisco IME calls that experience mid-call fallback to the PSTN, so that more calls fallback to the PSTN before Cisco Unified Communications Manager triggers an alarm. A higher value may be useful during minor network outages. Entering a lower threshold value makes the system less tolerant of Cisco IME calls that experience mid-call fallback to the PSTN, so fewer calls fallback before Cisco Unified Communications Manager triggers an IMEQualityAlertEntry alarm. The default value specifies 50. Valid values range from 10 to 100.
ICM Quality Alert Evaluation Interval	Specify the time interval in seconds that Cisco Unified Communications Manager uses to check the status of the ICM Failed Call Attempt Threshold and ICM Call Fallback Attempt Threshold parameters to determine whether to continue generating the IMEQualityAlertEntry alarm. The default value specifies 120. Valid values range from 30 to 1800.
Use IME for Outbound Calls	Specify whether to allow devices to make calls using the Cisco Intercompany Media Engine feature. Choose *True* to allow devices to make Cisco IME calls. Choose *False* to prevent devices from making Cisco IME calls. The default value specifies True.

Additional Information

Cisco IME Configuration Checklist, page 3-6

Verifying Connectivity

The Cisco Unified Communications Manager server and the Cisco Intercompany Media Engine (Cisco IME) server communicate using the Validation Access Protocol (VAP). Without the communication between the servers, Cisco Unified Communications Manager cannot learn Cisco IME routes, and users cannot make Cisco IME calls. To determine if the VAP connection exists, you must verify that the Cisco Unified Communications Manager server registers with the Cisco IME server and that the Cisco Unified Communications Manager server has published Vservices with the Cisco IME server.

See the following sections:

- Registration Status, page 3-41
- Vservice Publication, page 3-42
- DID Publication, page 3-42

Additional Information

Cisco IME Configuration Checklist, page 3-6

Registration Status

You can monitor the status of the connection between the Cisco Unified Communications Manager server and the Cisco Intercompany Media Engine (Cisco IME) server using one of the following methods.

Note After you verify the registration status, you can continue to verify connectivity between the Cisco Unified Communications Manager server and the Cisco IME server by verifying that the Cisco Unified Communications Manager server has published the Cisco IME service (or Vservice) to the Cisco IME server. as described in the "Vservice Publication" section on page 3-42.

From the CLI

From the Cisco Intercompany Media Engine CLI, enter the following command:

```
show ime vapstatus summary
```

This command displays the registration status for the client specified by port number. Make sure that the Registration Status equals *Registered*, and the Client IP ADDR equals the IP address of the Cisco Unified Communications Manager server.

The following example shows the output of the show ime vapstatus summary command in which the Cisco Unified Communications Manager registered with the Cisco IME server:

```
admin:show ime vapstatus summary
    VAP Client Connection Details
        Registration Status ...... Registered
        Client IP ADDR............ 10.94.150.96
        Client Handle ............ 1
        Packets Sent ............. 106
        Packets Rcvd ............. 106
        VAPServer Name ........... vapuser
        Missed Keep Alive Count .. 0
        Connection Up Time ....... 3 hours 7 min 0 sec
```

From RTMT

Access the Cisco Unified Communications Manager server using RTMT, and choose the following menu and counter:

System > Performance > Open Performance Monitoring > IME Client Instance > VAPStatus

If a connection between the Cisco IME server and Cisco Unified Communications Manager server exists, the counter should equal 1 (healthy). The valid values equal: 0=unknown; 1=healthy; 2=unhealthy.

Note This counter monitors connections to primary and secondary Cisco IME servers.

Additional Information

Cisco IME Configuration Checklist, page 3-6

Vservice Publication

Once you have verified the registration status of the Cisco Unified Communications Manager server to the Cisco Intercompany Media Engine (Cisco IME) server, you can continue to verify the connectivity between servers by verifying that the Cisco Unified Communications Manager server has published the Cisco IME service (or Vservice) to the Cisco IME server.

Cisco Unified Communications Manager publishes the Vservice after you check the Activated checkbox on the Intercompany Media Service Configuration window (**Advanced Features > Intercompany Media Services > Service**.)

Published Vservices indicate that an active service exists on the Cisco Unified Communications Manager and that it has connectivity into the Cisco IME server.

To verify Vservice publication, enter the **show ime vservice details** command on the Cisco IME command line.

The following example shows the output of the command in which Cisco Unified Communications Manager has published a Vservice. The VServiceProfiles field matches the Cisco IME service name that you entered on the Intercompany Media Service Configuration window.

```
admin: show ime vservice details
    VServiceProfiles: Vservice12-ccm18
    VServiceId = 3834353762636435
    overlay = intercompanymedianetwork
    domain  = cisco.com
    DiDCount (max) = 100
    SIPURI =
    sip:d954c46b-51b4-ea2d-cda4-8a20134279f6@cisco.com:5082;maddr=10.94.150.96;transport=t
    cp
```

Note After you verify the Vservice publication, you can continue to verify connectivity between the Cisco Unified Communications Manager server and the Cisco IME server by verifying that the Cisco Unified Communications Manager server has published DIDs to the IME distributed cache as described in the "DID Publication" section on page 3-42.

Additional Information

Cisco IME Configuration Checklist, page 3-6

DID Publication

After you confirm connectivity between the Cisco Unified Communications Manager and the Cisco Intercompany Media Engine (Cisco IME) servers, you can verify that the Cisco IME server has published the enrolled patterns (DIDs) to the IME distributed cache. Use the following methods to verify DID publication:

From the CLI

From the Cisco Intercompany Media Engine CLI, enter the following command:

utils ime fetch did *E.164 number*

The command output shows whether the Cisco IME server published DIDs to the IME distributed cache and which node owns the number.

Cisco IME RTMT

Access the Cisco Unified Communications Manager server using RTMT, and choose the following menu and counter:

System > Performance > Open Performance Monitoring > IME Client Instance > PublishedRoutes

This counter indicates the total number of DIDs published successfully into the IME distributed cache across all Cisco IME client instances.

Configuring a Fallback Profile

The fallback profile defines several values that the Cisco Unified Communications Manager uses to fallback Cisco Intercompany Media Engine (Cisco IME) calls to the PSTN. The fallback profile defines the quality of service level at which Cisco Unified Communications Manager attempts a mid-call fallback as well as the fallback number that the Cisco Unified Communications Manager uses to invoke the PSTN call.

When a user makes a call to a number that is linked to a fallback profile, the Cisco Unified Communications Manager of the calling party receives a fallback directory number that is configured on the Cisco Unified Communications Manager of the called party. The Cisco Unified Communications Manager uses the fallback number for the PSTN call when the ASA triggers a fallback to the PSTN.

After you configure the fallback profile and set the fallback feature parameters, you associate the fallback profile with an IME enrolled group (**Advanced Features > Intercompany Media Services > Enrolled Group**).

Note If you want calls to fallback to the PSTN, make sure that you Enable Fallback for IME Calls parameter in the Fallback Feature Configuration window (**Advanced Features > Fallback > Fallback Feature Configuration**.)

To access the Fallback Profile Configuration window, choose **Advanced Features > Fallback > Fallback Profile**.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the "Cisco Unified Communications Manager Administration Basics" section on page 3-2 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 3-14 describes the fallback profile configuration settings.

For related procedures, see the "Cisco IME Configuration Checklist" section on page 3-6.

Table 3-14 Fallback Profile Configuration Settings

Field	Description
Fallback Profile Information	
Name	Enter a unique name for the fallback profile. This name can comprise up to 32 characters in length.
Description	Enter a descriptive name for the fallback profile. The description can comprise up to 128 characters in length. (Optional)
Call Setup Fallback Settings	
Advertised Fallback Directory E.164 Number	Specify the +E.164 DID number that Cisco Unified Communications Manager uses to fallback Cisco IME calls to the PSTN. The number that you enter must begin with a **+** and may contain up to 15 digits. The Cisco Unified Communications Manager from the terminating side of the call passes this number to the Cisco Unified Communications Manager on the originating side of the call so that the originating Cisco Unified Communications Manager can initiate fallback to the PSTN when the quality of service falls below the level that this fallback profile specifies. For example, if the originating enterprise receives +14089023232 as a fallback DID, the originating enterprise must have a route pattern or translation pattern that routes that number over the PSTN to the terminating enterprise that sent that fallback DID. You must provide a dedicated +E.164 number that has not been allocated to any device.

Table 3-14 Fallback Profile Configuration Settings (continued)

Field	Description
Call Fallback Trigger Settings	
Fallback QOS Sensitivity Level	Indicate the RTP audio stream sensitivity level that you want the IME-enabled ASA to use to determine when to fallback a call to the PSTN. The Cisco Unified Communications Manager sends this value to the ASA firewall. Choose one of the following options: • Disable Fallback—This option disables the mid-call fallback feature. When you choose this option, no PSTN fallback of Cisco IME VoIP calls occurs. • Utility—This option maintains the lowest quality Cisco IME calls. This option does not provide consistent quality VoIP, but it does allow the greatest number of calls to be maintained on the VoIP network rather than being rerouted over the more costly PSTN. Cisco Systems does not recommend using this option for extended-duration calls. Cisco Systems recommends this option if you want to maintain as many calls as possible via the IP network, regardless of call quality. • Accommodative—Choose this option to accept a basic or low-level quality of audio on Cisco IME VoIP calls. With this level, the IME-enabled ASA attempts to retain calls over the IP network rather than falling back to the PSTN, even if the calls have less than desirable audio quality. • Nominal—Choose this option to maintain Cisco IME VoIP calls that have good or better quality than PSTN calls. Most enterprise deployments qualify based on reasonably high quality and high-speed Internet connectivity. (Default) • Moderate—This option maintains only Cisco IME VoIP calls that have very good QoS. Calls with lesser QoS statistics fallback to the PSTN. For this option, the enterprises at both ends of the call must have Tier 1 or Tier 2 networks. If both enterprises do not meet the network requirement, the system routes the calls over the PSTN. • Aggressive—This option maintains only Cisco IME VoIP calls that have superior QoS quality; that is, calls that are virtually identical to QoS-provisioned VoIP. All calls that do not meet the QoS statistics for calls at this level fallback to the PSTN. For this option, the enterprises at both ends of the call must have Tier 1 or Tier 2 networks. If both enterprises do not meet the network requirement, the system routes the calls over the PSTN. The default specifies the value of the Fallback QOS Sensitivity Level parameter in the Fallback Feature Configuration window (**Advanced Features > Fallback > Fallback Feature Configuration**).

Table 3-14 Fallback Profile Configuration Settings (continued)

Field	Description
Fallback Call Settings	
Fallback Call CSS	Choose which calling search space to use to route a fallback call to the PSTN on the originating Cisco Unified Communications Manager cluster. The default specifies Calling device AAR Calling Search Space. If you have not defined an AAR calling search space, the re-route CSS can be used, depending on your system configuration.
Fallback Call Answer Timer	Do not change this value unless a Cisco TAC engineer instructs you to do so. This field indicates the amount of time in seconds (from 1 to 10) that the originating Cisco Unified Communications Manager waits for a mid-call fallback PSTN call to be answered. The default value equals the value of the Fallback Call Answer Timer in the Fallback Feature Configuration window (**Advanced Features > Fallback > Fallback Feature Configuration**). **Note** If the value of the Fallback Call Answer Time field on the Fallback Feature Configuration window is greater than the value that you configure here, the fallback call uses the value from the Fallback Feature Configuration window when a mid-call fallback takes place.
Fallback Call Handling Settings	
Fallback Directory Number Partition	Choose the partition that Cisco Unified Communications Manager uses in routing fallback calls. This partition should be included in the calling search space used by the gateway devices that receive calls for the fallback number. The default specifies the default partition. For more information on configuring partitions and calling search spaces, refer to the *Cisco Unified Communications Manager Administration Guide*.
Fallback Directory Number	(Optional) Use this field to specify a non-E.164 version of the fallback directory number. For example, if the advertised +E.164 fallback number specifies +14089023092 and you normalize incoming numbers to seven digits before routing, the fallback directory number should specify 9023092. If you do not specify a value in this field, the +E.164 number gets injected into digit analysis. **Tip** If you are using a dial plan that supports an +E.164 backplane, you can leave this field blank.

Table 3-14 Fallback Profile Configuration Settings (continued)

Field	Description
Number of Digits for Caller ID Partial Match	This field specifies the minimum number of digits that must match in an incoming fallback call and a particular Cisco IME call in order to be considered a match. When receiving fallback calls, Cisco Unified Communications Manager uses the caller ID of the incoming call as a key to match the incoming call to a particular Cisco IME call that is falling back. Because caller identification numbers can be transformed in the PSTN, Cisco Unified Communications Manager uses a partial-matching algorithm that allows a caller ID to be considered a match if a subset of the digits matches. The default specifies five digits.

Additional Information

Cisco IME Configuration Checklist, page 3-6

Configuring Fallback Feature Parameters

Use the Fallback Feature Configuration window to configure feature parameters that apply to mid-call fallback of Cisco Intercompany Media Engine (Cisco IME) calls to the PSTN.

To access the Fallback Profile Configuration window, choose **Advanced Features > Fallback > Fallback Feature Configuration**.

Configuration Settings Table

Table 3-2 describes the fallback configuration settings.

For related procedures, see the "Cisco IME Configuration Checklist" section on page 3-6.

Table 3-15 Fallback Feature Configuration Settings

Field	Description
Enable Fallback for IME Calls	Specify whether Cisco Unified Communications Manager uses PSTN fallback. This value overrides any other setting for fallback. This parameter must be enabled on the originating and terminating side of a call in order for PSTN fallback to occur. The default specifies True.

Table 3-15 Fallback Feature Configuration Settings (continued)

Field	Description
Fallback QOS Sensitivity Level	Specify the sensitivity level for the ASA firewall to use to determine when to fallback a call to the PSTN. The Cisco Unified Communications Manager sends this value to the ASA firewall. This parameter populates the default value of the Fallback QOS Sensitivity Level in the Fallback Profile Configuration window (**Advanced Features > Fallback > Fallback Profile**) as well as provides a default sensitivity level if you do not define a fallback profile. This parameter applies to the terminating side during PSTN fallback. The default value specifies Nominal sensitivity.
Fallback Number of DTMF Correlation Digits	Specify the number of DTMF digits that the Cisco Unified Communications Manager uses for a mid-call fallback PSTN call. This parameter applies to the terminating side during PSTN fallback. The default value specifies 4. Valid values range from 4 to 20.
Fallback DTMF Collection Timer	Specify the amount of time (in seconds) that Cisco Unified Communications Manager waits for DTMF digits collection during a mid-call fallback PSTN call. This parameter applies to the terminating side during PSTN fallback. The default value specifies 3. Valid values range from 1 to 10.
Fallback Call Answer Timer	Specify the amount of time (in seconds) that Cisco Unified Communications Manager waits, after receiving alerting indication, for a mid-call fallback PSTN call to be answered before giving up. This parameter applies to the originating side during PSTN fallback. This parameter populates the default values in the fallback profile, as well as provides the default value if a profile is not defined. The default value specifies 3. Valid values range from 1 to 10. **Note** If the value that you enter in the Fallback Call Answer Timer field on this window is greater than the value that you configure in the Fallback Call Answer Timer field on the Fallback Profile Configuration window (Advanced Features Fallback Fallback Profile), the fallback call uses the value from the Fallback Feature Configuration window when a mid-call fallback takes place.
Fallback Call CSS	Specify the calling search space to use to route the fallback calls. This parameter applies to the originating side during PSTN fallback. The default value specifies AAR CSS.

Additional Information

Cisco IME Configuration Checklist, page 3-6

Configuring Intercompany Media Services Firewall Information

Use the Intercompany Media Services Firewall Configuration window to configure the IP address and port of the ASA mapping service. You need to configure this information if you have implemented an off-path deployment model in which normal Internet-facing traffic does not flow through the same adaptive security appliance (ASA) as the Cisco Intercompany Media Engine (Cisco IME) traffic.

During an outbound call attempt, the SIP invite message must be routed to the offpath Cisco IME enabled ASA. Cisco Unified Communications Manager sends a request to the ASA for a mapping of the global IP/port of the remote enterprise (found in the Cisco IME learned route) to an internal IP/port on the Cisco IME enabled ASA. Cisco Unified Communications Manager then initiates a SIP Invite that routes to this internal IP/port. The Cisco IME enabled ASA performs NAT, mapping to the global IP/port of the remote enterprise from the IME learned route. The offpath Cisco IME enabled ASA proxies this signaling session and initiates a TLS session to this global IP/port (the Cisco IME enabled ASA of the remote enterprise).

To access the Intercompany Media Services Firewall Configuration window, choose **Advanced Features > Intercompany Media Services > Firewall**.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the "Cisco Unified Communications Manager Administration Basics" section on page 3-2 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 3-16 describes the Intercompany Media Services firewall configuration settings.

For related procedures, see the "Cisco IME Configuration Checklist" section on page 3-6.

Table 3-16 Intercompany Media Services Firewall Configuration Settings

Field	Description
Name	Specify a unique name for the ASA mapping service.
Description	Specify a description for the ASA mapping service. (Optional)
IP Address	Enter the IP address of the ASA mapping service.
Port	Enter the port of the ASA mapping service.

Cisco Intercompany Media Engine Learned Routes

Learned routes specify lists of all +E.164 numbers that the system has learned through Cisco Intercompany Media Engine (Cisco IME). You can enable or disable a particular route. You can disable if you are having problems with a particular route and you need to disable to troubleshoot.

To access the IME Learned Routes window, choose **Advanced Features > Intercompany Media Services > Learned Route**.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the "Cisco Unified Communications Manager Administration Basics" section on page 3-2 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 3-17 describes the Intercompany Media Services learned route configuration settings.

For related procedures, see the "Cisco IME Configuration Checklist" section on page 3-6.

Table 3-17 Cisco Intercompany Media Engine Learned Route Configuration Settings

Field	Description
E.164	The field specifies +E.164 number that the Cisco Unified Communications Manager has learned.
Domain	This field specifies the domain for the +E.164 number.
Signaling	This field specifies the destination remote IP address and port of the dynamic SIP trunk that the system uses to reach the destination DID.
Learned-On	This field specifies the date that Cisco Unified Communications Manager learned this route.
Expires-On	This field specifies the date that this route expires. Routes expire a year after the learned-on date.
Admin Enabled	This field indicates whether a learned route is in use. To disable a route without deleting it from the database, uncheck the Admin Enabled check box. To enable a route so that Cisco Intercompany Media Engine can use the route, check this check box.

Additional Information

Cisco IME Configuration Checklist, page 3-6

Related Topics

- Cisco Unified Communications Manager Administration Basics, page 3-2
- Cisco IME Configuration Checklist, page 3-6
- Configuring Cisco IME Server Connections, page 3-14
- Setting Up TLS Connections Between the Cisco Unified Communications Manager and Cisco Intercompany Media Engine Servers, page 3-16
- Configuring a Cisco IME Enrolled Group, page 3-19
- Configuring a Cisco IME Enrolled Pattern, page 3-21
- Configuring a Cisco IME Exclusion Group, page 3-22
- Configuring a Cisco IME Exclusion Number, page 3-23
- Configuring a Cisco IME Trust Group, page 3-24
- Configuring a Cisco IME Trust Element, page 3-25

- Configuring a Cisco IME Service, page 3-26
- Configuring External IP Address and Port Information, page 3-28
- Configuring Transformation Patterns for Cisco IME, page 3-29
- Configuring a Cisco IME Transformation Profile, page 3-30
- Configuring Cisco IME E.164 Transformations, page 3-35
- Configuring PSTN Access Trunks, page 3-36
- Configuring a Cisco IME Feature Configuration, page 3-37
- Verifying Connectivity, page 3-40
- Configuring a Fallback Profile, page 3-43
- Configuring Fallback Feature Parameters, page 3-47
- Configuring Intercompany Media Services Firewall Information, page 3-49
- Cisco Intercompany Media Engine Learned Routes, page 3-49

CHAPTER 4

Cisco ASA Configuration

The Cisco Adaptive Security Appliance (ASA) firewall plays a key role in the security of the Cisco Intercompany Media Engine solution. This section contains information on configuring ASA using the command-line interface, as well as the ASDM, a web-based GUI application.

- Proxy Configuration Guidelines and Limits, page 4-1
- Proxy CLI configuration, page 4-2
- Proxy Configuration using ASDM, page 4-24

Proxy Configuration Guidelines and Limits

Context Mode Guidelines

Supported in single context mode only.

Firewall Mode Guidelines

Supported in routed firewall mode only.

IPv6 Guidelines

Does not support IPv6 addresses.

Additional Guidelines and Limitations

Cisco Intercompany Media Engine has the following limitations:

- Fax is not supported. Fax capability needs to be disabled on the SIP trunk.
- Stateful failover of Cisco Unified Intercompany Media Engine is not supported. During failover, existing calls traversing the Cisco Intercompany Media Engine Proxy disconnect; however, new calls successfully traverse the proxy after the failover completes.
- Having Cisco UCMs on more than one of the adaptive security appliance interfaces is not supported with the Cisco Intercompany Media Engine Proxy. Having the Cisco UCMs on one trusted interface is especially necessary in an off path deployment because the adaptive security appliance requires that you specify the listening interface for the mapping service and the Cisco UCMs must be connected on one trusted interface.
- Multipart MIME is not supported.
- Only existing SIP features and messages are supported.

- RTCP is not supported. The adaptive security appliance drops any RTCP traffic sent from the inside interface to the outside interface. The adaptive security appliance does not convert RTCP traffic from the inside interface into SRTP traffic.
- The Cisco Intercompany Media Engine Proxy configured on the adaptive security appliance creates a dynamic SIP trunk for each connection to a remote enterprise. However, you cannot configure a unique subject name for each SIP trunk. The Cisco Intercompany Media Engine Proxy can have only one subject name configured for the proxy.

  Additionally, the subject DN you configure for the Cisco Intercompany Media Engine Proxy match the domain name that has been set for the local Cisco UCM.
- If a service policy rule for the Cisco Intercompany Media Engine Proxy is removed (by using the no service policy command) and reconfigured, the first call traversing the adaptive security appliance will fail. The call fails over to the PSTN because the Cisco UCM does not know the connections are cleared and tries to use the recently cleared IME SIP trunk for the signaling.

  To resolve this issue, you must additionally enter the **clear connection all** command and restart the adaptive security appliance. If the failure is due to failover, the connections from the primary adaptive security appliance are not synchronized to the standby adaptive security appliance.
- After the **clear connection all** command is issued on an adaptive security appliance enabled with a UC-IME Proxy and the IME call fails over to the PSTN, the next IME call between an originating and terminating SCCP IP phone completes but does not have audio and is dropped after the signaling session is established.

  An IME call between SCCP IP phones use the IME SIP trunk in both directions. Namely, the signaling from the calling to called party uses the IME SIP trunk. Then, the called party uses the reverse IME SIP trunk for the return signaling and media exchange. However, this connection is already cleared on the adaptive security appliance, which causes the IME call to fail.

  The next IME call (the third call after the **clear connection all** command is issued), will be completely successful.

  Note This limitation does not apply when the originating and terminating IP phones are configured with SIP.

- The adaptive security appliance must be licensed and configured with enough TLS proxy sessions to handle the IME call volume. See the licensing requirements sections for TLS proxy sessions in the *Cisco ASA 5500 Series Configuration Guide using the CLI*.

  This limitation occurs because an IME call cannot fall back to the PSTN when there are not enough TLS proxy sessions left to complete the IME call. An IME call between two SCCP IP phones requires the adaptive security appliance to use two TLS proxy sessions to successfully complete the TLS handshake.

  Assume for example, the adaptive security appliance is configured to have a maximum of 100 TLS proxy sessions and IME calls between SCCP IP phones establish 101 TLS proxy sessions. In this example, the next IME call is initiated successfully by the originating SCCP IP phone but fails after the call is accepted by the terminating SCCP IP phone. The terminating IP phone rings and on answering the call, the call hangs due to an incomplete TLS handshake. The call does not fall back to the PSTN.

Proxy CLI configuration

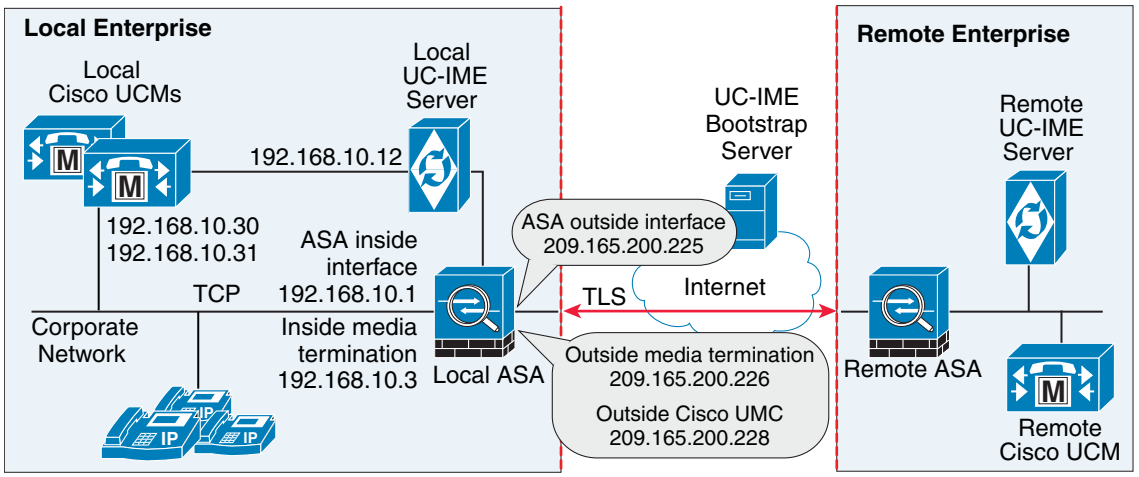
This section contains the following topics:

- Task Flow for Configuring Cisco Intercompany Media Engine, page 4-3
- Configuring NAT for Cisco Intercompany Media Engine Proxy, page 4-4
- Configuring PAT for the Cisco UCM Server, page 4-5
- Creating Access Lists for Cisco Intercompany Media Engine Proxy, page 4-7
- Creating the Media Termination Instance, page 4-8
- Creating the Cisco Intercompany Media Engine Proxy, page 4-10
- Creating Trustpoints and Generating Certificates, page 4-13
- Creating the TLS Proxy, page 4-16
- Enabling SIP Inspection for the Cisco Intercompany Media Engine Proxy, page 4-17
- (Optional) Configuring TLS within the Local Enterprise, page 4-19
- (Optional) Configuring Off Path Signaling, page 4-22

Task Flow for Configuring Cisco Intercompany Media Engine

Figure 4-1 provides an example for a basic deployment of the Cisco Intercompany Media Engine. The following tasks include command line examples based on Figure 4-1.

Figure 4-1 Example for Basic (in-line) Deployment Tasks



Note Step 1 through Step 8 apply to both basic (in-line) and off path deployments and Step 9 applies only to off path deployment.

To configure a Cisco Intercompany Media Engine for a basic deployment, perform the following tasks.

Step 1 Configure static NAT for Cisco UCM. See Configuring NAT for Cisco Intercompany Media Engine Proxy, page 4-4.

Or

Configure PAT for the UCM server. See Configuring PAT for the Cisco UCM Server, page 4-5.

Step 2 Create access lists for Cisco Intercompany Media Engine Proxy. See Creating Access Lists for Cisco Intercompany Media Engine Proxy, page 4-7.

Step 3 Create the media termination address instance for Cisco Intercompany Media Engine Proxy. See Creating the Media Termination Instance, page 4-8.

Step 4 Create the Cisco Intercompany Media Engine Proxy. See Creating the Cisco Intercompany Media Engine Proxy, page 4-10.

Step 5 Create trustpoints and generate certificates for the Cisco Intercompany Media Engine Proxy. See Creating Trustpoints and Generating Certificates, page 4-13.

Step 6 Create the TLS proxy. See Creating the TLS Proxy, page 4-16.

Step 7 Configure SIP inspection for the Cisco Intercompany Media Engine Proxy. See Enabling SIP Inspection for the Cisco Intercompany Media Engine Proxy, page 4-17.

Step 8 (Optional) Configure TLS within the enterprise. See (Optional) Configuring TLS within the Local Enterprise, page 4-19.

Step 9 (Optional) Configure off path signaling. See (Optional) Configuring Off Path Signaling, page 4-22.

Note You only perform Step 9 when you are configuring the Cisco Intercompany Media Engine Proxy in an off path deployment.

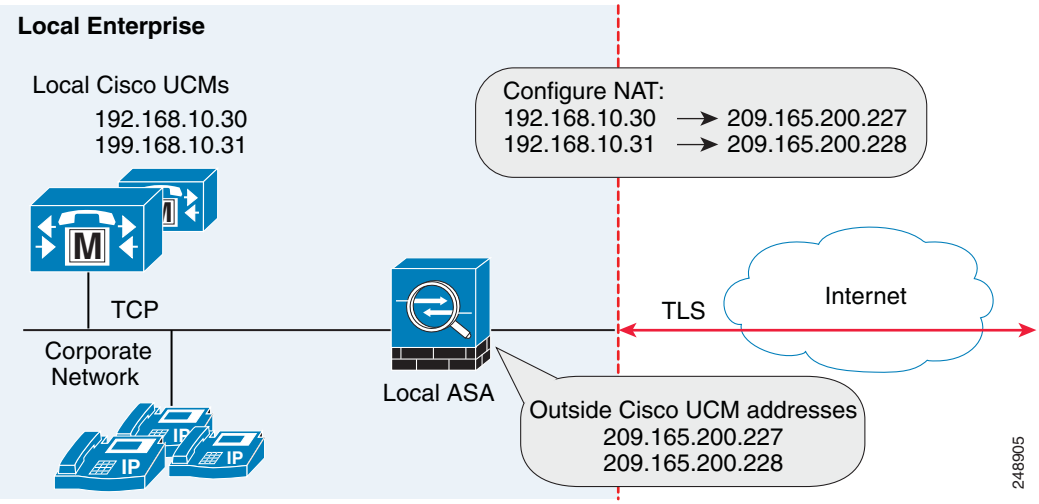
Configuring NAT for Cisco Intercompany Media Engine Proxy

To configure auto NAT, you first configure an object; then use the **nat** command in the object configuration mode.

The example command lines in this task are based on a basic (in-line) deployment. See Figure 4-1 on page 4-3 for an illustration explaining the example command lines in this task.

Alternatively, you can configure PAT for the Cisco Intercompany Media Engine Proxy. See Configuring PAT for the Cisco UCM Server, page 4-5.

Figure 4-2 Example for Configuring NAT for a Deployment



To configure auto NAT rules for the Cisco UCM server, perform the following steps:

	Command	Purpose

Step 1	`hostname(config)# object network name`
	Examples:
	`hostname(config)# object network inside_to_outside`
		Configures a network object for the real address of Cisco UCM that you want to translate.

Step 2	`hostname(config-network-object)# host ip_address`
	Examples:
	`hostname(config-network-object)# host 192.168.10.30`
	`hostname(config-network-object)# host 192.168.10.31`
		Specifies the real IP address of the Cisco UCM host for the network object.

Step 3	(Optional)
	`hostname(config-network-object)# description string`
	Example:
	`hostname(config-network-object)# description "Cisco UCM NAT"`
		Provides a description of the network object.

Step 4	`hostname(config-network-object)# nat (inside,outside) static mapped_inline_ip`
	Examples:
	`hostname(config-network-object)# nat (inside,outside) static 209.165.200.227`
	`hostname(config-network-object)# nat (inside,outside) static 209.165.200.228`
		Specifies the address translation on the network objects created in this procedure.
		Where *mapped_inline_ip* is the outside IP address of the Cisco UCM.

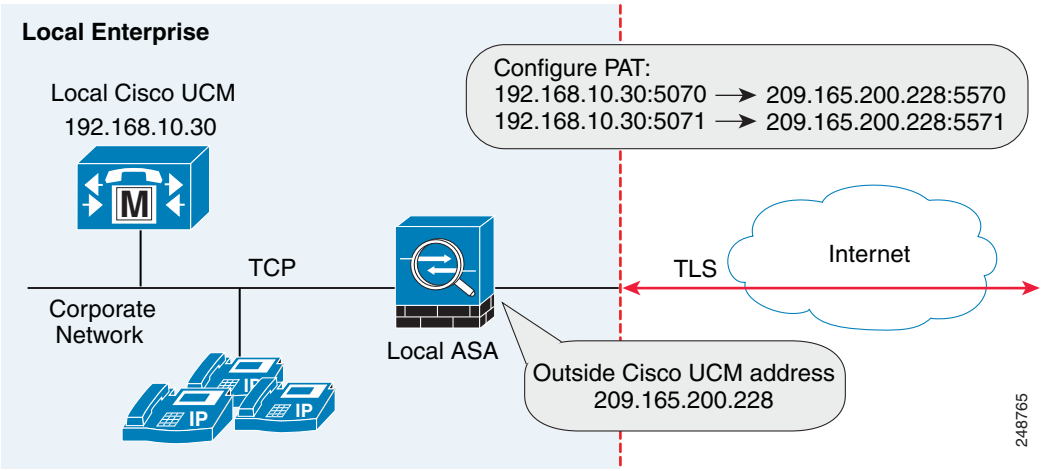
What to Do Next

Create the access lists for the Cisco Intercompany Media Engine Proxy. See Creating Access Lists for Cisco Intercompany Media Engine Proxy, page 4-7.

Configuring PAT for the Cisco UCM Server

Perform this task as an alternative to configuring NAT for the Cisco Intercompany Media Engine Proxy.

Figure 4-3 Example for Configuring PAT for a Deployment



Note You only perform this step when NAT is not configured for the Cisco UCM server.

To configure PAT for the Cisco UCM server, perform the following steps:

	Command	Purpose

Step 1	`hostname(config)# object network name`
	Examples:
	`hostname(config)# object network ucm-pat-config1`
		Configures a network object for inbound Intercompany Media Engine calls.

Step 2	`hostname(config-network-object)# host ip_address`
	Example:
	`hostname(config-network-object)# host 192.168.30`
		Specifies the real IP address of the Cisco UCM host for the network object.

Step 3	(Optional)
	`hostname(config-network-object)# description string`
	Example:
	`hostname(config-network-object)# description "PAT for Inbound Calls"`
		Provides a description of the network object.

Step 4	`hostname(config-network-object)# nat (inside,outside) static mapped_inline_ip service tcp real_port mapped_port`
	Example:
	`hostname(config-network-object)# nat (inside,outside) static 209.165.200.228 service tcp 5570 5571`
		Configures static PAT for inbound Intercompany Media Engine calls from the port configured on the outside network to the specified port on the inside network.

Step 5	`hostname(config-network-object)# exit`	Exits from the object configuration mode.

Step 6	`hostname(config)# object network name`
	Examples:
	`hostname(config)# object network ucm-pat-config2`
		Configures a network object for outbound Intercompany Media Engine calls.

Step 7	`hostname(config-network-object)# subnet ip_address mask`
	Examples:
	`hostname(config-network-object)# host 192.168.10.0 255.255.255.0`
		Specifies the subnet for the network object.

	Command	Purpose

Step 8	(Optional)
	`hostname(config-network-object)# description string`
	Example:
	`hostname(config-network-object)# description "PAT for Outbound Calls"`
		Provides a description of the network object.

Step 9	`hostname(config-network-object)# nat (inside,outside) dynamic ip_address`
	Example:
	`hostname(config-network-object)# nat (inside,outside) dynamic 209.165.200.228`
		Configures dynamic PAT for outbound Intercompany Media Engine calls that hides the inside network behind the outside interface address.

Creating Access Lists for Cisco Intercompany Media Engine Proxy

To configure access lists for the Cisco Intercompany Media Engine Proxy to reach the Cisco UCM server, perform the following steps.

The example command lines in this task are based on a basic (in-line) deployment. See Figure 4-1 on page 4-3 for an illustration explaining the example command lines in this task.

	Command	Purpose

Step 1	`hostname(config)# access-list id extended permit tcp any host ip_address eq port`
	Example:
	`hostname(config)# access-list incoming extended permit tcp any host 192.168.10.30 eq 5070`
		Adds an Access Control Entry (ACE). An access list is made up of one or more ACEs with the same access list ID. This ACE provides access control by allowing incoming access for Cisco Intercompany Media Engine connections on the specified port.
		In the *ip_address* argument, provide the real IP address of Cisco UCM.

Step 2	`hostname(config)# access-group access-list in interface interface_name`
	Example:
	`hostname(config)# access-group incoming in interface outside`
		Binds the access list to an interface.

Step 3	`hostname(config)# access-list id extended permit tcp any host ip_address eq port`
	Example:
	`hostname(config)# access-list ime-inbound-sip extended permit tcp any host 192.168.10.30 eq 5070`
		Adds an ACE. This ACE allows the adaptive security appliance to allow inbound SIP traffic for Cisco Intercompany Media Engine. This entry is used to classify traffic for the class and policy map.
		Note The port that you configure here must match the trunk settings configured on Cisco UCM. See the Cisco Unified Communications Manager documentation for information about this configuration setting.

	Command	Purpose
Step 4	hostname(config)# **access-list** *id* **extended permit tcp** *ip_address mask* **any range** *range* **Example:** hostname(config)# access-list ime-outbound-sip extended permit tcp 192.168.10.30 255.255.255.255 any range 5000 6000	Adds an ACE. This ACE allows the adaptive security appliance to allow outbound SIP traffic for Cisco Intercompany Media Engine (in the example, any TCP traffic with source as 192.168.10.30 and destination port range between 5000 and 6000). This entry is used to classify traffic for the class and policy map. **Note** Ensure that TCP traffic between Cisco UCM and the Cisco Intercompany Media Engine server does not use this port range (if that connection goes through the adaptive security appliance).
Step 5	hostname(config)# **access-list** *id* **permit tcp any host** *ip_address* **eq 6084** **Example:** hostname(config)# access-list ime-traffic permit tcp any host 192.168.10.12 eq 6084	Adds an ACE. This ACE allows the adaptive security appliance to allow traffic from the Cisco Intercompany Media Engine server to remote Cisco Intercompany Media Engine servers.
Step 6	hostname(config)# **access-list** *id* **permit tcp any host** *ip_address* **eq 8470** **Example:** hostname(config)# access-list ime-bootserver-traffic permit tcp any host 192.168.10.12 eq 8470	Adds an ACE. This ACE allows the adaptive security appliance to allow traffic from the Cisco Intercompany Media Engine server to the Bootstrap server for the Cisco Intercompany Media Engine.

What to Do Next

Create the media termination instance on the adaptive security appliance for the Cisco Intercompany Media Engine Proxy. See Creating the Media Termination Instance, page 4-8.

Creating the Media Termination Instance

Guidelines

The media termination address you configure must meet these requirements:

- If you decide to configure a media-termination address on interfaces (rather than using a global interface), you must configure a media-termination address on at least two interfaces (the inside and an outside interface) before applying the service policy for the Cisco Intercompany Media Engine Proxy. Otherwise, you will receive an error message when enabling the proxy with SIP inspection.

Note Cisco recommends that you configure the media-termination address for the Cisco Intercompany Media Engine Proxy on interfaces rather than configuring a global media-termination address.

- The Cisco Intercompany Media Engine Proxy can use only one type of media termination instance at a time; for example, you can configure a global media-termination address for all interfaces or configure a media-termination address for different interfaces. However, you cannot use a global media-termination address and media-termination addresses configured for each interface at the same time.

Note If you change any Cisco Intercompany Media Engine Proxy settings after you create the media-termination address for the proxy, you must reconfigure the media-termination address by using the **no media-termination** command, and then reconfiguring it as described in this procedure.

Procedure

Create the media termination instance to use with the Cisco Intercompany Media Engine Proxy.

The example command lines in this task are based on a basic (in-line) deployment. See Figure 4-1 on page 4-3 for an illustration explaining the example command lines in this task.

To create the media termination instance for the Cisco Intercompany Media Engine Proxy, perform the following steps:

	Command	Purpose

Step 1	`hostname(config)# media-termination instance_name`
	Example:
	`hostname(config)# media-termination uc-ime-media-term`
		Creates the media termination instance that you attach to the Cisco Intercompany Media Engine Proxy.

Step 2	`hostname(config-media-termination)# address ip_address interface intf_name`
	Examples:
	`hostname(config-media-termination)# address 209.165.200.228 interface outside`
		Configures the media-termination address used by the outside interface of the adaptive security appliance.
		The outside IP address must be a publicly routable address that is an unused IP address within the address range on that interface.
		See Creating the Cisco Intercompany Media Engine Proxy, page 4-10 for information about the UC-IME proxy settings. See *Cisco ASA 5500 Series Configuration Guide using the CLI* for information about the **no service-policy** command.

Step 3	`hostname(config-media-termination)# address ip_address interface intf_name`
	Examples:
	`hostname(config-media-termination)# address 192.168.10.3 interface inside`
		Configures a media termination address used by the inside interface of the adaptive security appliance.
		Note The IP address must be an unused IP address within the same subnet on that interface.

Step 4	(Optional)
	`hostname(config-media-termination)# rtp-min-port port1 rtp-maxport port2`
	Examples:
	`hostname(config-media-termination)# rtp-min-port 1000 rtp-maxport 2000`
		Configures the rtp-min-port and rtp-max-port limits for the Cisco Intercompany Media Engine Proxy. Configure the RTP port range for the media termination point when you need to scale the number of calls that the Cisco Intercompany Media Engine supports.
		Where *port1* specifies the minimum value for the RTP port range for the media termination point, where port1 can be a value from 1024 to 65535. By default, the value for *port1* is 16384.
		Where *port2* specifies the maximum value for the RTP port range for the media termination point, where port2 can be a value from 1024 to 65535. By default, the value for *port2* is 32767.

What To Do Next

Once you have created the media termination instance, create the Cisco Intercompany Media Engine Proxy. See Creating the Cisco Intercompany Media Engine Proxy, page 4-10.

Creating the Cisco Intercompany Media Engine Proxy

To create the Cisco Intercompany Media Engine Proxy, perform the following steps.

The example command lines in this task are based on a basic (in-line) deployment. See Figure 4-1 on page 4-3 for an illustration explaining the example command lines in this task.

Note You cannot change any of the configuration settings for the Cisco Intercompany Media Engine Proxy described in this procedure when the proxy is enabled for SIP inspection. Remove the Cisco Intercompany Media Engine Proxy from SIP inspection before changing any of the settings described in this procedure.

	Command	Purpose

Step 1	`hostname(config)# uc-ime uc_ime_name`
	Example:
	`hostname(config)# uc-ime local-ent-ime`
		Configures the Cisco Intercompany Media Engine Proxy.
		Where *uc_ime_name* is the name of the Cisco Intercompany Media Engine Proxy. The name is limited to 64 characters.
		Only one Cisco Intercompany Media Engine Proxy can be configured on the adaptive security appliance.

Step 2	`hostname(config-uc-ime)# media-termination mta_instance_name`
	Example:
	`hostname(config-uc-ime)# media-termination ime-media-term`
		Specifies the media termination instance used by the Cisco Intercompany Media Engine Proxy.
		Note You must create the media termination instance before you specify it in the Cisco Intercompany Media Engine Proxy.
		Where *mta_instance_name* is the *instance_name* that you created in Step 1 of Creating the Media Termination Instance.
		See Creating the Media Termination Instance, page 4-8 for the steps to create the media termination instance.

	Command	Purpose
Step 3	hostname(config-uc-ime)# **ucm address** *ip_address* **trunk-security-mode** [**nonsecure** | **secure**] **Example:** hostname(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure	Specifies the Cisco UCM server in the enterprise. You must specify the real IP address of the Cisco UCM server. Do not specify a mapped IP address for the server. **Note** You must include an entry for each Cisco UCM in the cluster with Cisco Intercompany Media Engine that has a SIP trunk enabled. Where the **nonsecure** and **secure** options specify the security mode of the Cisco UCM or cluster of Cisco UCMs. **Note** Specifying **secure** for Cisco UCM or Cisco UCM cluster indicates that Cisco UCM or Cisco UCM cluster is initiating TLS; therefore, you must configure TLS for components. See (Optional) Configuring TLS within the Local Enterprise, page 4-19. You can specify the **secure** option in this task or you can update it later while configuring TLS for the enterprise. See Step 11 in (Optional) Configuring TLS within the Local Enterprise, page 4-19.

	Command	Purpose
Step 4	hostname(config-uc-ime)# **ticket epoch** *n* **password** *password* **Example:** hostname(config-uc-ime)# ticket epoch 1 password password1234	Configures the ticket epoch and password for Cisco Intercompany Media Engine. Where *n* is an integer from 1-255. The epoch contains an integer that updates each time that the password is changed. When the proxy is configured the first time and a password entered for the first time, enter 1 for the epoch integer. Each time you change the password, increment the epoch to indicate the new password. You must increment the epoch value each time your change the password. Typically, you increment the epoch sequentially; however, the adaptive security appliance allows you to choose any value when you update the epoch. If you change the epoch value, the current password is invalidated and you must enter a new password. Where *password* contains a minimum of 10 and a maximum of 64 printable character from the US-ASCII character set. The allowed characters include 0x21 to 0x73 inclusive, and exclude the space character. We recommend a password of at least 20 characters. Only one password can be configured at a time. The ticket password is stored onto flash. The output of the **show running-config uc-ime** command displays ***** instead of the password string. **Note** The epoch and password that you configure on the adaptive security appliance must match the epoch and password configured on the Cisco Intercompany Media Engine server. See the Cisco Intercompany Media Engine server documentation for information.

	Command	Purpose

Step 5	(Optional)
	`hostname(config-uc-ime)# fallback monitoring timer timer_millisec | hold-down timer timer_sec`
	Examples:
	`hostname(config-uc-ime)# fallback monitoring timer 120`
	`hostname(config-uc-ime)# fallback hold-down timer 30`
		Specifies the fallback timers for Cisco Intercompany Media Engine.
		Specifying **monitoring timer** sets the time between which the adaptive security appliance samples the RTP packets received from the Internet. The adaptive security appliance uses the data sample to determine if fallback to the PSTN is needed for a call.
		Where *timer_millisec* specifies the length of the monitoring timer. By default, the length is 100 milliseconds for the monitoring timer and the allowed range is 10-600 ms.
		Specifying **hold-down timer** sets the amount of time that adaptive security appliance waits before notifying Cisco UCM whether to fall back to PSTN.
		Where *timer_sec* specifies the length of the hold-down timer. By default, the length is 20 seconds for the hold-down timer and the allowed range is 10-360 seconds.
		If you do not use this command to specify fallback timers, the adaptive security appliance uses the default settings for the fallback timers.

Step 6	(Optional)
	`hostname(config-uc-ime)# fallback sensitivity-file file_name`
	Example:
	`hostname(config-uc-ime)# fallback sensitivity-file ime-fallback-sensitvity.fbs`
		Specifies the file to use for mid-call PSTN fallback.
		Where *file_name* must be the name of a file on disk that includes the .fbs file extension.
		The fallback file is used to determine whether the QoS of the call is poor enough for the Cisco Intercompany Media Engine to move the call to the PSTN.

What to Do Next

Install the certificate on the local entity truststore. You could also enroll the certificate with a local CA trusted by the local entity.

Creating Trustpoints and Generating Certificates

You need to generate the keypair for the certificate used by the adaptive security appliance, and configure a trustpoint to identify the certificate sent by the adaptive security appliance in the TLS handshake.

The example command lines in this task are based on a basic (in-line) deployment. See Figure 4-1 on page 4-3 for an illustration explaining the example command lines in this task.

Note This task instructs you on how to create trustpoints for the local enterprise and the remote enterprise and how to exchange certificates between these two enterprises. This task does not provide steps for creating trustpoints and exchanging certificates between the local Cisco UCM and the local adaptive security appliance. However, if you require additional security within the local enterprise, you must perform the

optional task (Optional) Configuring TLS within the Local Enterprise, page 4-19. Performing that task allows for secure TLS connections between the local Cisco UCM and the local adaptive security appliance. The instructions in that task describe how to create trustpoints between the local Cisco UCM and the local adaptive security appliance.

Prerequisites for Installing Certificates

To create a proxy certificate on the adaptive security appliance that is trusted by the remote entity, obtain a certificate from a trusted CA or export it from the remote enterprise adaptive security appliance.

To export the certificate from the remote enterprise, you enter the following command on the remote adaptive security appliance:

hostname(config)# **crypto ca export trustpoint identity-certificate**

The adaptive security appliance prompts displays the certificate in the terminal screen. Copy the certificate from the terminal screen. You will need the certificate text in Step 5 of this task.

Procedure

To create the trustpoints and generate certificates, perform the following steps:

	Command	Purpose
Step 1	`hostname(config)# crypto key generate rsa label` *key-pair-label* `modulus` *size* **Example:** `hostname(config)# crypto key generate rsa label local-ent-key modulus 2048`	On the local adaptive security appliance, creates the RSA keypair that can be used for the trustpoints. This is the keypair and trustpoint for the local entities signed certificate. The modulus key size that you select depends on the level of security that you want to configure and on any limitations imposed by the CA from which you are obtaining the certificate. The larger the number that you select, the higher the security level will be for the certificate. Most CAs recommend 2048 for the key modulus size; however, **Note** GoDaddy requires a key modulus size of 2048.
Step 2	`hostname(config)# crypto ca trustpoint` *trustpoint_name* **Example:** `hostname(config)# crypto ca trustpoint local_ent`	Enters the trustpoint configuration mode for the specified trustpoint so that you can create the trustpoint for the local entity. A trustpoint represents a CA identity and possibly a device identity, based on a certificate issued by the CA. Maximum name length is 128 characters.

	Command	Purpose
Step 3	hostname(config-ca-trustpoint)# **subject-name** *X.500_name* **Example:** hostname(config-ca-trustpoint)# subject-name cn=Ent-local-domain-name**	Includes the indicated subject DN in the certificate during enrollment. **Note** The domain name that you enter here must match the domain name that has been set for the local Cisco UCM. For information about how to configure the domain name for Cisco UCM, see the Cisco Unified Communications Manager documentation for information.
Step 4	hostname(config-ca-trustpoint)# **keypair** *keyname* **Example:** hostname(config-ca-trustpoint)# keypair local-ent-key	Specifies the key pair whose public key is to be certified.
Step 5	hostname(config-ca-trustpoint)# **enroll terminal**	Specifies that you will use the "copy and paste" method of enrollment with this trustpoint (also known as manual enrollment).
Step 6	hostname(config-ca-trustpoint)# **exit**	Exits from the CA Trustpoint configuration mode.
Step 7	hostname(config)# **crypto ca enroll** *trustpoint* **Example:** hostname(config)# crypto ca enroll remote-ent % % Start certificate enrollment ... % The subject name in the certificate will be: % cn=enterpriseA % The fully-qualified domain name in the certificate will @ be: ciscoasa % Include the device serial number in the subject name? [yes/no]: no Display Certificate Request to terminal? [yes/no]: yes	Starts the enrollment process with the CA. Where *trustpoint* is the same as the value you entered for *trustpoint_name* in Step 2. When the trustpoint is configured for manual enrollment (**enroll terminal** command), the adaptive security appliance writes a base-64-encoded PKCS10 certification request to the console and then displays the CLI prompt. Copy the text from the prompt. Submit the certificate request to the CA, for example, by pasting the text displayed at the prompt into the certificate signing request enrollment page on the CA website. When the CA returns the signed identity certificate, proceed to Step 8 in this procedure.
Step 8	hostname(config)# **crypto ca import** *trustpoint* **certificate** **Example:** hostname(config)# crypto ca import remote-ent certificate	Imports the signed certificate received from the CA in response to a manual enrollment request. Where *trustpoint* specifies the trustpoint you created in Step 2. The adaptive security appliance prompts you to paste the base-64 formatted signed certificate onto the terminal.
Step 9	hostname(config)# **crypto ca authenticate** *trustpoint* **Example:** hostname(config)# crypto ca authenticate remote-ent	Authenticates the third-party identity certificate received from the CA. The identity certificate is associated with a trustpoint created for the remote enterprise. The adaptive security appliance prompts you to paste the base-64 formatted identity certificate from the CA onto the terminal.

What to Do Next

Create the TLS proxy for the Cisco Intercompany Media Engine. See the "Creating the TLS Proxy" section on page 4-16.

Creating the TLS Proxy

Because either enterprise, namely the local or remote Cisco UCM servers, can initiate the TLS handshake (unlike IP Telephony or Cisco Mobility Advantage, where only the clients initiate the TLS handshake), you must configure by-directional TLS proxy rules. Each enterprise can have an adaptive security appliance as the TLS proxy.

Create TLS proxy instances for the local and remote entity initiated connections respectively. The entity that initiates the TLS connection is in the role of "TLS client." Because the TLS proxy has a strict definition of "client" and "server" proxy, two TLS proxy instances must be defined if either of the entities could initiate the connection.

The example command lines in this task are based on a basic (in-line) deployment. See Figure 4-1 on page 4-3 for an illustration explaining the example command lines in this task.

To create the TLS proxy, perform the following steps:

	Command	Purpose

Step 1	`hostname(config)# tls-proxy proxy_name`
	Example:
	`hostname(config)# tls-proxy local_to_remote-ent`
		Creates the TLS proxy for the outbound connections.

Step 2	`hostname(config-tlsp)# client trust-point proxy_trustpoint`
	Example:
	`hostname(config-tlsp)# client trust-point local-ent`
		For **outbound** connections, specifies the trustpoint and associated certificate that the adaptive security appliance uses in the TLS handshake when the adaptive security appliance assumes the role of the TLS client. The certificate must be owned by the adaptive security appliance (identity certificate).
		Where *proxy_trustpoint* specifies the trustpoint defined by the **crypto ca trustpoint** command in Step 2 in "Creating Trustpoints and Generating Certificates" section on page 4-13.

Step 3	`hostname(config-tlsp)# client cipher-suite cipher_suite`
	Example:
	`hostname(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1`
		For outbound connections, controls the TLS handshake parameter for the cipher suite.
		Where *cipher_suite* includes des-sha1, 3des-sha1, aes128-sha1, aes256-sha1, or null-sha1.
		For client proxy (the proxy acts as a TLS client to the server), the user-defined cipher suite replaces the default cipher suite, or the one defined by the **ssl encryption** command. Use this command to achieve difference ciphers between the two TLS sessions. You should use AES ciphers with the Cisco UCM server.

Step 4	`hostname(config-tlsp)# exit`	Exits from the TLS proxy configuration mode.

Step 5	`hostname(config)# tls-proxy proxy_name`
	Example:
	`hostname(config)# tls-proxy remote_to_local-ent`
		Create the TLS proxy for inbound connections.

	Command	Purpose

Step 6	`hostname(config-tlsp)# server trust-point proxy_trustpoint`
	Example:
	`hostname(config-tlsp)# server trust-point local-ent`
		For **inbound** connections, specifies the proxy trustpoint certificate presented during TLS handshake. The certificate must be owned by the adaptive security appliance (identity certificate).
		Where *proxy_trustpoint* specifies the trustpoint defined by the **crypto ca trustpoint** command in Step 2 in "Creating Trustpoints and Generating Certificates" section on page 4-13.
		Because the TLS proxy has strict definition of client proxy and server proxy, two TLS proxy instances must be defined if either of the entities could initiate the connection.

Step 7	`hostname(config-tlsp)# client cipher-suite cipher_suite`
	Example:
	`hostname(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1`
		For inbound connections, controls the TLS handshake parameter for the cipher suite.
		Where *cipher_suite* includes des-sha1, 3des-sha1, aes128-sha1, aes256-sha1, or null-sha1.

Step 8	`hostname(config-tlsp)# exit`	Exits from the TSL proxy configuration mode.
Step 9	`hostname(config)# ssl encryption 3des-sha1 aes128-sha1 [algorithms]`	Specifies the encryption algorithms that the SSL/TLS protocol uses. Specifying the 3des-shal and aes128-shal is required. Specifying other algorithms is optional. **Note** The Cisco Intercompany Media Engine Proxy requires that you use strong encryption. You must specify this command when the proxy is licensed using a K9 license.

What to Do Next

Once you have created the TLS proxy, enable it for SIP inspection.

Enabling SIP Inspection for the Cisco Intercompany Media Engine Proxy

Enable the TLS proxy for SIP inspection and define policies for both entities that could initiate the connection.

The example command lines in this task are based on a basic (in-line) deployment. See Figure 4-1 on page 4-3 for an illustration explaining the example command lines in this task.

Note If you want to change any Cisco Intercompany Media Engine Proxy settings after you enable SIP inspection, you must enter the **no service-policy** command, and then reconfigure the service policy as described in this procedure. Removing and reconfiguring the service policy does not affect existing calls; however, the first call traversing the Cisco Intercompany Media Engine Proxy will fail. Enter the **clear connection** command and restart the adaptive security appliance.

To enable SIP inspection for the Cisco Intercompany Media Engine Proxy, perform the following steps:

	Command	Purpose

Step 1	`hostname(config)# class-map class_map_name`
	Examples:
	`hostname(config)# class-map ime-inbound-sip`
		Defines a class for the inbound Cisco Intercompany Media Engine SIP traffic.

Step 2	`hostname(config-cmap)# match access-list access_list_name`
	Examples:
	`hostname(config-cmap)# match access-list ime-inbound-sip`
		Identifies the SIP traffic to inspect.
		Where the *access_list_name* is the access list you created in Step 3, page 4-7 of the task Creating Access Lists for Cisco Intercompany Media Engine Proxy.

Step 3	`hostname(config-cmap)# exit`	Exits from the class map configuration mode.

Step 4	`hostname(config)# class-map class_map_name`
	Examples:
	`hostname(config)# class-map ime-outbound-sip`
		Defines a class for the outbound SIP traffic from Cisco Intercompany Media Engine.

Step 5	`hostname(config)# match access-list access_list_name`
	Examples:
	`hostname(config-cmap)# match access-list ime-outbound-sip`
		Identifies which outbound SIP traffic to inspect.
		Where the *access_list_name* is the access list you created in Step 4, page 4-8 of the task Creating Access Lists for Cisco Intercompany Media Engine Proxy.

Step 6	`hostname(config-cmap)# exit`	Exits from the class map configuration mode.

Step 7	`hostname(config)# policy-map name`
	Examples:
	`hostname(config)# policy-map ime-policy`
		Defines the policy map to which to attach the actions for the class of traffic.

Step 8	`hostname(config-pmap)# class classmap_name`
	Examples:
	`hostname(config-pmap)# class ime-outbound-sip`
		Assigns a class map to the policy map so that you can assign actions to the class map traffic.
		Where *classmap_name* is the name of the SIP class map that you created in Step 1 in this task.

Step 9	`hostname(config-pmap-c)# inspect sip [sip_map] uc-ime uc_ime_map tls-proxy proxy_name`
	Examples:
	`hostname(config-pmap-c)# inspect sip uc-ime local-ent-ime tls-proxy local_to_remote-ent`
		Enables the TLS proxy and Cisco Intercompany Media Engine Proxy for the specified SIP inspection session.

Step 10	`hostname(config-cmap-c)# exit`	Exits from the policy map class configuration mode.

Step 11	`hostname(config-pmap)# class class_map_name`
	Examples:
	`hostname(config-pmap)# class ime-inbound-sip`
		Assigns a class map to the policy map so that you can assign actions to the class map traffic.
		Where *classmap_name* is the name of the SIP class map that you created in Step 4 in this task.

Step 12	`hostname(config-pmap-c)# inspect sip [sip_map] uc-ime uc_ime_map tls-proxy proxy_name`
	Examples:
	`hostname(config-pmap-c)# inspect sip uc-ime local-ent-ime tls-proxy remote_to_local-ent`
		Enables the TLS proxy and Cisco Intercompany Media Engine Proxy for the specified SIP inspection session.

Step 13	`hostname(config-pmap-c)# exit`	Exits from the policy map class configuration mode.

	Command	Purpose
Step 14	`hostname(config-pmap)# exit`	Exits from the policy map configuration mode.

Step 15	`hostname(config)# service-policy policymap_name global`
	Examples:
	`hostname(config)# service-policy ime-policy global`
		Enables the service policy for SIP inspection for all interfaces.
		Where *policymap_name* is the name of the policy map you created in Step 7 of this task.
		See Creating the Cisco Intercompany Media Engine Proxy, page 4-10 for information about the UC-IME proxy settings. See *Cisco ASA 5500 Series Configuration Guide using the CLI* for information about the **no service-policy** command.

What to Do Next

Once you have enabled the TLS proxy for SIP inspection, if necessary, configure TLS within the enterprise. See (Optional) Configuring TLS within the Local Enterprise, page 4-19.

(Optional) Configuring TLS within the Local Enterprise

This task is not required if TCP is allowable within the inside network.

TLS within the enterprise refers to the security status of the Cisco Intercompany Media Engine trunk as seen by the adaptive security appliance.

Note If the transport security for the Cisco Intercompany Media Engine trunk changes on Cisco UCM, it must be changed on the adaptive security appliance as well. A mismatch will result in call failure. The adaptive security appliance does not support SRTP with non-secure IME trunks. The adaptive security appliance assumes SRTP is allowed with secure trunks. So 'SRTP Allowed' must be checked for IME trunks if TLS is used. The adaptive security appliance supports SRTP fallback to RTP for secure IME trunk calls.

Prerequisites

On the local Cisco UCM, download the Cisco UCM certificate. See the Cisco Unified Communications Manager documentation for information. You will need this certificate when performing Step 6 of this procedure.

Procedure

To configure TLS within the local enterprise, perform the following steps on the local adaptive security appliance:

	Commands	Purpose
Step 1	hostname(config)# **crypto key generate rsa label** *key-pair-label* hostname(config)# **crypto ca trustpoint** *trustpoint_name* hostname(config-ca-trustpoint)# **enroll self** hostname(config-ca-trustpoint)# **keypair** *keyname* hostname(config-ca-trustpoint)# **subject-name** *x.500_name* **Example:** hostname(config)# crypto key generate rsa label local-ent-key hostname(config)# crypto ca trustpoint local-asa hostname(config-ca-trustpoint)# enroll self hostname(config-ca-trustpoint)# keypair key-local-asa hostname(config-ca-trustpoint)# subject-name *cn=Ent-local-domain-name***., o="Example Corp"	Creates an RSA key and trustpoint for the self-signed certificate. Where *key-pair-label* is the RSA key for the local adaptive security appliance. Where *trustpoint_name* is the trustpoint for the local adaptive security appliance. Where *keyname* is key pair for the local adaptive security appliance. Where *x.500_name* includes the X.500 distinguished name of the local adaptive security appliance; for example, *cn=Ent-local-domain-name***. **Note** The domain name that you enter here must match the domain name that has been set for the local Cisco UCM. For information about how to configure the domain name for Cisco UCM, see the Cisco Unified Communications Manager documentation for information.
Step 2	hostname(config-ca-trustpoint)# **exit**	Exits from Trustpoint Configuration mode.
Step 3	hostname(config)# **crypto ca export** *trustpoint* **identity-certificate** **Example:** hostname(config)# crypto ca export local-asa identity-certificate	Exports the certificate you created in Step 1. The certificate contents appear on the terminal screen. Copy the certificate from the terminal screen. This certificate enables Cisco UCM to validate the certificate that the adaptive security appliance sends in the TLS handshake. On the local Cisco UCM, upload the certificate into the Cisco UCM trust store. See the Cisco Unified Communications Manager documentation for information. **Note** The subject name you enter while uploading the certificate to the local Cisco UCM is compared with the X.509 Subject Name field entered on the SIP Trunk Security Profile on Cisco UCM. For example, "Ent-local-domain-name" was entered in Step 1 of this task; therefore, "Ent-local-domain-name" should be entered in the Cisco UCM configuration.
Step 4	hostname(config)# **crypto ca trustpoint** *trustpoint_name* hostname(config-ca-trustpoint)# **enroll terminal** **Example:** hostname(config)# crypto ca trustpoint local-ent-ucm hostname(config-ca-trustpoint)# enroll terminal	Creates a trustpoint for local Cisco UCM. Where *trustpoint_name* is the trustpoint for the local Cisco UCM.
Step 5	hostname(config-ca-trustpoint)# **exit**	Exits from Trustpoint Configuration mode.

	Commands	Purpose
Step 6	hostname(config)# **crypto ca authenticate** *trustpoint* **Example:** hostname(config)# crypto ca authenticate local-ent-ucm	Imports the certificate from local Cisco UCM. Where *trustpoint* is the trustpoint for the local Cisco UCM. Paste the certificate downloaded from the local Cisco UCM. This certificate enables the adaptive security appliance to validate the certificate that Cisco UCM sends in the TLS handshake.
Step 7	hostname(config)# **tls-proxy** *proxy_name* hostname(config-tlsp)# **server trust-point** *proxy_trustpoint* hostname(config-tlsp)# **client trust-point** *proxy_trustpoint* hostname(config-tlsp)# **client cipher-suite** aes128-sha1 aes256-sha1 3des-sha1 null-sha1 **Example:** hostname(config)# tls-proxy local_to_remote-ent hostname(config-tlsp)# server trust-point local-asa hostname(config-tlsp)# client trust-point local-ent hostname(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1	Updates the TLS proxy for **outbound** connections. Where *proxy_name* is the name you entered in Step 1 of the task Creating the TLS Proxy. Where *proxy_trustpoint* for the **server trust-point** command is the trustpoint name for the local adaptive security appliance you entered in Step 1 of this procedure. Where *proxy_trustpoint* for the **client trust-point** command is the name you entered in Step 2 of the task Creating Trustpoints and Generating Certificates. **Note** In this step, you are creating different trustpoints for the client and the server.
Step 8	hostname(config-tlsp)# **exit**	Exits from TLS Proxy Configuration mode.
Step 9	hostname(config)# **tls-proxy** proxy_name hostname(config-tlsp)# **server trust-point** *proxy_trustpoint* hostname(config-tlsp)# **client trust-point** *proxy_trustpoint* hostname(config-tlsp)# **client cipher-suite** aes128-sha1 aes256-sha1 3des-sha1 null-sha1 **Example:** hostname(config)# tls-proxy remote_to_local-ent hostname(config-tlsp)# server trust-point local-ent hostname(config-tlsp)# client trust-point local-asa hostname(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1	Updates the TLS proxy for **inbound** connections. Where *proxy_name* is the name you entered in Step 5 of the task Creating the TLS Proxy. Where *proxy_trustpoint* for the **server trust-point** command is the name you entered in Step 2 of the task Creating Trustpoints and Generating Certificates. Where *proxy_trustpoint* for the **client trust-point** command is the trustpoint name for the local adaptive security appliance you entered in Step 1 of this procedure.
Step 10	hostname(config-tlsp)# **exit**	Exits from TLS Proxy Configuration mode.
Step 11	hostname(config)# **uc-ime** *uc_ime_name* hostname(config-uc-ime)# **ucm address** *ip_address* **trunk-security-mode secure** **Example:** hostname(config)# uc-ime local-ent-ime hostname(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode secure	Updates the Cisco Intercompany Media Engine Proxy for trunk-security-mode. Where *uc_ime_name* is the name you entered in Step 1 of the task Creating the Cisco Intercompany Media Engine Proxy. Only perform this step if you entered nonsecure in Step 3 of the task Creating the Cisco Intercompany Media Engine Proxy.

What to Do Next

Once you have configured the TLS within the enterprise, if necessary, configure off path signaling for an off path deployment. See (Optional) Configuring Off Path Signaling, page 4-22.

(Optional) Configuring Off Path Signaling

Perform this task only when you are configuring the Cisco Intercompany Media Engine Proxy as part of an off path deployment. You might choose to have an off path deployment when you want to use the Cisco Intercompany Media Engine but do not want to replace your existing Internet firewall with an adaptive security appliance enabled with the Cisco Intercompany Media Engine Proxy. In an off path deployment, normal Internet facing trafficflows through the existing Internet firewall while the Cisco Intercompany Media Engine traffic flows through the adaptive security appliance enabled with the Cisco Intercompany Media Engine Proxy.

Off path signaling requires that outside IP addresses translate to an inside IP address. For the Cisco Intercompany Media Engine Proxy, the adaptive security appliance creates dynamic mappings for external addresses to the internal IP address. For inbound signaling and outbound signaling, address translation must be configured in the following ways.

For inbound signaling, the outside Cisco UCM address has to be routed to the outside interface of the adaptive security appliance. Therefore, you must configure the adaptive security appliance to translate the real Cisco UCM address to the outside address of the adaptive security appliance. The outside address of the adaptive security appliance must be routable. This ensures that the adaptive security appliance receives packets sent to the Cisco UCM.

Configuring this translation means that the source IP address of an inbound signaling packet is translated to the inside interface of the adaptive security appliance. Based the example in Figure 4-4, an inbound signaling packet from the remote adaptive security appliance:

SOURCE	DESTINATION
10.10.0.24	209.165.200.228

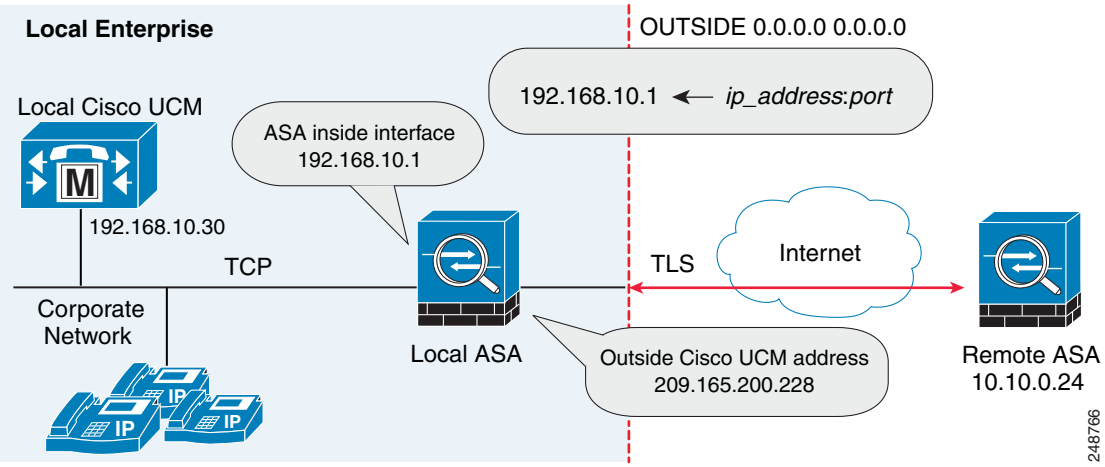
Translates to

SOURCE	DESTINATION
10.10.0.24	192.168.10.30

For outbound signaling, the Cisco UCM does not have an inbound packet with a translated source IP address to which it can reply when the Cisco UCM initiates a connection. To accommodate this situation, you must configure a mapping service on the adaptive security appliance. The mapping service translates the source IP address of future inbound signaling packets.

After you configure off path signaling, the adaptive security appliance mapping service listens on interface “inside” for requests. When it receives a request, it creates a dynamic mapping for the “outside” as the destination address.

Figure 4-4 Example for Configuring Off Path Signaling in an Off Path Deployment



In an off path deployment, inbound media packets and outbound media packets are routed based on the media termination address. For information about how the adaptive security appliance uses the media termination address to route media packets, see Creating the Media Termination Instance, page 4-8.

To configure off path signaling for the Cisco Intercompany Media Engine Proxy, perform the following steps:

	Command	Purpose

Step 1	`hostname(config)# object network name`
	Example:
	`hostname(config)# object network outside-any`
		For the off path adaptive security appliance, creates a network object to represent all outside addresses.

Step 2	`hostname(config-network-object)# subnet ip_address`
	Example:
	`hostname(config-network-object)# subnet 0.0.0.0 0.0.0.0`
		Specifies the IP address of the subnet.

Step 3	`hostname(config-network-object)# nat (outside, inside) dynamic interface`	Creates a mapping for the Cisco UCM of remote enterprises.
Step 4	`hostname(config-network-object)# exit`	Exits from the objects configuration mode.

	Command	Purpose
Step 5	hostname(config)# **uc-ime** *uc_ime_name* **Example:** hostname(config)# uc-ime local-ent-ime	Specifies the Cisco Intercompany Media Engine Proxy that you created in the task Creating the Cisco Intercompany Media Engine Proxy, page 4-10. Where *uc_ime_name* is the name you specified in Step 1 of Creating the Cisco Intercompany Media Engine Proxy, page 4-10.
Step 6	hostname(config-uc-ime)# **mapping-service listening-interface** *interface_name* [**listening-port** *port*] **uc-ime-interface** *uc-ime-interface_name* **Example:** hostname(config-uc-ime)# mapping-service listening-interface inside listening-port 8060 uc-ime-interface outside	For the off path adaptive security appliance, adds the mapping service to the Cisco Intercompany Media Engine Proxy. Specifies the interface and listening port for the adaptive security appliance mapping service. You can only configure one mapping service for the Cisco Intercompany Media Engine Proxy. Where *interface_name* is the name of the interface on which the adaptive security appliance listens for the mapping requests. Where port is the TCP port on which the adaptive security appliance listens for the mapping requests. The port number must be between 1024 and 65535 to avoid conflicts with other services on the device, such as Telnet or SSH. By default, the port number is TCP 8060. Where *uc-ime-interface_name* is the name of the interface that connects to the remote Cisco UCM.

Proxy Configuration using ASDM

This section contains the following sections:

- Configuring the Cisco UC-IMC Proxy by using the UC-IME Proxy Pane, page 4-24
- Configuring the Cisco UC-IMC Proxy by using the Unified Communications Wizard, page 4-26

Configuring the Cisco UC-IMC Proxy by using the UC-IME Proxy Pane

Use the Configure Cisco Intercompany Media Engine (UC-IME) proxy pane to add or edit a Cisco Intercompany Media Engine Proxy instance.

Note The Cisco Intercompany Media Engine Proxy does not appear as an option under the Unified Communications section of the navigation pane unless the license required for this proxy is installed on the adaptive security appliance.

Use this pane to create the proxy instance; however, for the UC-IME proxy to be fully functionally, you must complete additional tasks, such as create the required NAT statements, access lists, and MTA, set up the certificates, create the TLS Proxy, and enable SIP inspection.

Depending on whether the UC-IME proxy is deployed off path or in-line of Internet traffic, you must create the appropriate network objects with embedded NAT/PAT statements for the Cisco UCMs.

This pane is available from the Configuration > Firewall > Unified Communications > UC-IME Proxy.

Step 1 Open the Configuration > Firewall > Unified Communications > UC-IME Proxy pane.

Step 2 Check the Enable Cisco UC-IME proxy check box to enable the feature.

Step 3 In the Unified CM Servers area, enter an IP address or hostname for the Cisco Unified Communications Manager (Cisco UCM) or click the ellipsis to open a dialog and browse for an IP address or hostname.

Step 4 In the Trunk Security Mode field, click a security option. Specifying **secure** for Cisco UCM or Cisco UCM cluster indicates that Cisco UCM or Cisco UCM cluster is initiating TLS.

Step 5 Click **Add** to add the Cisco UCM for the Cisco Intercompany Media Engine Proxy. You must include an entry for each Cisco UCM in the cluster with Cisco Intercompany Media Engine that has a SIP trunk enabled.

Step 6 In the Ticket Epoch field, enter an integer from 1-255.

The epoch contains an integer that updates each time that the password is changed. When the proxy is configured the first time and a password entered for the first time, enter 1 for the epoch integer. Each time you change the password, increment the epoch to indicate the new password. You must increment the epoch value each time your change the password.

Typically, you increment the epoch sequentially; however, the adaptive security appliance allows you to choose any value when you update the epoch.

If you change the epoch value, the current password is invalidated and you must enter a new password.

Note The epoch and password that you configure in this step on the adaptive security appliance must match the epoch and password that you configure on the Cisco Intercompany Media Engine server. See the Cisco Intercompany Media Engine server documentation for information.

Step 7 In the Ticket Password field, enter a minimum of 10 printable character from the US-ASCII character set. The allowed characters include 0x21 to 0x73 inclusive, and exclude the space character. The ticket password can be up to 64 characters. Confirm the password you entered. Only one password can be configured at a time.

Step 8 Check the Apply MTA to UC-IME Link proxy check box to associate the media termination address with the Cisco Intercompany Media Engine Proxy.

Note You must create the media termination instance before you associate it with the Cisco Intercompany Media Engine Proxy. If necessary, click the Configure MTA button to configure a media termination address instance.

Step 9 If the Cisco Intercompany Media Engine Proxy is being configured as part of off path deployment, check the Enable off path address mapping service checkbox and configure the off path deployment settings:

a. From the Listening Interface field, select an adaptive security appliance interface. This is the interface on which the adaptive security appliance listens for the mapping requests.

b. In the Port field, enter a number between 1024 and 65535 as the TCP port on which the adaptive security appliance listens for the mapping requests. The port number must be 1024 or higher to avoid conflicts with other services on the device, such as Telnet or SSH. By default, the port number is TCP 8060.

c. From the UC-IME Interface field, select an interface from the list. This is the interface that the adaptive security appliance uses to connect to the remote Cisco UCM.

Note In an off path deployment any existing adaptive security appliance that you have deployed in your environment are not capable of transmitting Cisco Intercompany Media Engine traffic. Off-path signaling requires that outside addresses are translated (using NAT) to an inside IP address. The inside interface address can be used for this mapping service configuration. For the Cisco Intercompany Media Engine Proxy, the adaptive security appliance creates dynamic mappings for external addresses to the internal IP address.

Step 10 In the Fallback area, configure the fallback timer for the Cisco Intercompany Media Engine by specifying the following settings:

a. In the Fallback Sensitivity File field, enter the path to a file in flash memory that the adaptive security appliance uses for mid-call PSTN fallback. The file name that you enter must be the name of a file on disk that includes the .fbs file extension. Alternatively, click the Browse Flash button to locate and select the file from flash memory.

b. In the Call Quality Evaluation Interval field, enter a number between 10-600 (in milliseconds). This number controls the frequency at which the adaptive security appliance samples the RTP packets received from the Internet. The adaptive security appliance uses the data sample to determine if fallback to the PSTN is needed for a call. By default, the length is 100 milliseconds for the timer.

c. In the Notification Interval field, enter a number between 10-360 (in seconds). This number controls the amount of time that the adaptive security appliance waits before notifying Cisco UCM whether to fall back to PSTN. By default, the length is 20 seconds for this timer.

Note When you change the fallback timer for the Cisco Intercompany Media Engine Proxy, ASDM automatically removes the proxy from SIP inspection and then reapplies SIP inspection when the proxy is re-enabled.

Step 11 Click Apply to save the configuration changes for the Cisco Intercompany Media Engine Proxy.

Configuring the Cisco UC-IMC Proxy by using the Unified Communications Wizard

To configure the Cisco Intercompany Media Engine Proxy by using ASDM, choose Wizards > Unified Communications Wizard from the menu. The Unified Communications Wizard opens. From the first page, select the Cisco Intercompany Media Engine Proxy option under the Business-to-Business section.

The wizard automatically creates the necessary TLS proxy, then guides you through creating the Intercompany Media Engine proxy, importing and installing the required certificates, and finally enables the SIP inspection for the Intercompany Media Engine traffic automatically.

The wizard guides you through these steps to create the Cisco Intercompany Media Engine Proxy:

Step 1 Select the Intercompany Media Engine Proxy option.

Step 2 Select the topology of the Cisco Intercompany Media Engine Proxy, namely whether the adaptive security appliance is an edge firewall with all Internet traffic flowing through it or whether the adaptive security appliance is off the path of the main Internet traffic (referred to as an off path deployment).

Step 3 Specify private network settings such as the Cisco UCM IP addresses and the ticket settings.

Step 4 Specify the public network settings.

Step 5 Specify the media termination address settings of Cisco UCM.

Step 6 Configure the local-side certificate management, namely the certificates that are exchanged between the local Cisco Unified Communications Manager servers and the adaptive security appliance. The identity certificate that the wizard generates in this step needs to be installed on each Cisco Unified Communications Manager (UCM) server in the cluster with the proxy and each identity certificate from the Cisco UCMs need to be installed on the adaptive security appliance. The certificates are used by the adaptive security appliance and the Cisco UCMs to authenticate each other, respectively, during TLS handshakes. The wizard only supports self-signed certificates for this step.

Step 7 Configure the remote-side certificate management, namely the certificates that are exchanged between the remote server and the adaptive security appliance. In this step, the wizard generates a certificate signing request (CSR). After successfully generating the identity certificate request for the proxy, the wizard prompts you to save the file.

You must send the CSR text file to a certificate authority (CA), for example, by pasting the text file into the CSR enrollment page on the CA website. When the CA returns the Identity Certificate, you must install it on the adaptive security appliance. This certificate is presented to remote servers so that they can authenticate the adaptive security appliance as a trusted server.

Finally, this step of the wizard assists you in installing the root certificates of the CA from the remote servers so that the adaptive security appliance can determine that the remote servers are trusted.

The wizard completes by displaying a summary of the configuration created for Cisco Intercompany Media Engine. See the Unified Communications Wizard section in this documentation for more information.

CHAPTER 5

Backing up and Restoring the Cisco IME Server

The Disaster Recovery System (DRS), which can be invoked from the Cisco IME server command line interface (CLI), provides full data backup and restore capabilities for the Cisco IME server. The Disaster Recovery System allows you to perform regularly scheduled automatic or user-invoked data backups.

DRS restores its own settings (backup device settings and schedule settings) as part of the backup/restore process. DRS backs up and restores drfDevice.xml and drfSchedule.xml files. When the server is restored with these files, you do not need to reconfigure DRS backup device and schedule.

You can store the backup files to either a local or network device. You must choose a local device if you do not have outgoing SFTP access to the Cisco IME server. If you store backup files to a local device, DRS stores the backup files in the /common/adminsftp/backup directory. You must manually move local backup files from the Cisco IME server by opening an SFTP client and connecting to the Cisco IME server by using the adminsftp user and the administrator password that you set up during installation

Caution Before you restore Cisco IME, ensure that the Cisco IME version that is installed on the server matches the version of the backup file that you want to restore. The Disaster Recovery System supports only matching versions of Cisco IME for restore. For example, the Disaster Recovery System does not allow a restore from version 8.0.(**1**).1000-1 to version 8.0(**2**).1000-1, or from version 8.0.(1).1000-**1** to version 8.0(1).1000-**2**.

The Disaster Recovery System includes the following capabilities:

- A command line interface for performing backup and restore tasks.
- A distributed system architecture for performing backup and restore functions.
- Scheduled backups.
- Archive backups to a local drive or remote SFTP server. The Disaster Recovery System does not support tape drives for backup and restore on the Cisco IME server.

Note The system automatically deletes local backup files more than one week old. A warning message displays when you perform a backup that indicates that local backup files get deleted after one week.

The Disaster Recovery System contains two key functions, Master Agent (MA) and Local Agent (LA). The Master Agent coordinates backup and restore activity with Local Agents.

Caution Schedule backups during off-peak hours to avoid call-processing interruptions and impact to service.

Quick-Reference Tables for Backup and Restore Procedures

The following tables provide a quick reference for the backup and restore procedures.

Note DRS backs up and restores the drfDevice.xml and drfSchedule.xml files. These backup device settings and schedule settings get restored as a part of the backup/restore process. After the server is restored with these files, you do not need to reconfigure DRS backup device and schedule.

Backup Quick Reference

Table 1 provides a quick, high-level reference to the major steps, in chronological order, that you must perform to do a backup procedure by using the Disaster Recovery System.

Table 1 Major Steps for Performing a Backup Procedure

Action	Reference
Create backup devices on which to back up data.	"Managing Backup Devices" section on page 5-4
Create backup schedules to back up data on a schedule.	"Creating Backup Schedules" section on page 5-5
Enable and disable backup schedules to back up data.	"Enabling, Disabling, and Deleting Schedules" section on page 5-6
Optionally, run a manual backup.	"Starting a Manual Backup" section on page 5-6
Check the Status of the Backup—While a backup is running, you can check the status of the current backup job.	"Checking Backup Status" section on page 5-7

Restore Quick Reference

Table 2 provides a quick, high-level reference to the major steps, in chronological order, that you must perform to do a restore procedure by using the Disaster Recovery System.

Table 2 Major Steps for Performing a Restore Procedure

Action	Reference
Restore a backup file from a local or network directory.	"Restoring a Server" section on page 5-8
Check the Status of the Restore—While the restore process is running, you can check the status of the current restore job.	"Viewing the Restore Status" section on page 5-9

System Requirements

To back up data to a remote device on the network or to move a local backup to another location, you must have an SFTP server that is configured. Cisco allows you to use any SFTP server product but recommends SFTP products that have been certified with Cisco through the Cisco Technology Developer Partner program (CTDP). CTDP partners, such as GlobalSCAPE, certify their products with specified version of Cisco Unified Communications Manager. For information on which vendors have certified their products with your version of Cisco Unified Communications Manager, refer to the following URL:

http://www.cisco.com/pcgi-bin/ctdp/Search.pl

For information on using GlobalSCAPE with supported Cisco Unified Communications versions, refer to the following URL:

http://www.globalscape.com/gsftps/cisco.aspx

Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

- Open SSH (refer to http://sshwindows.sourceforge.net/)
- Cygwin (refer to http://www.cygwin.com/)
- Titan (refer to http://www.titanftp.com/)

Note Note: For issues with third-party products that have not been certified through the CTDP process, contact the third-party vendor for support

Note While a backup or restore is running, you cannot perform any OS Administration tasks because Disaster Recovery System blocks all OS Administration requests by locking the platform API. However, this does not block most CLI commands as only the CLI-based upgrade commands use the Platform API locking package.

Tip Schedule backups during periods when you expect less network traffic.

How to Access the Disaster Recovery System

To access the Disaster Recovery System, log into the Cisco IME CLI remotely or locally using the same Administrator username and password that you use created during installation:

- From a client workstation, you can use SSH to connect securely to the CLI.
- You can access the Cisco IME CLI directly by using the monitor and keyboard that you used during installation or by using a terminal server that is connected to the serial port. Use this method if a problem exists with the IP address.

Note You set the Administrator username and password during the Cisco IME installation, and you can change the Administrator password or set up a new Administrator account by using the CLI. Refer to the *Cisco Intercompany Media Engine Command Line Interface Reference Guide*.

Master Agent Duties and Activation

The system automatically activates the Master Agent (MA) on the server. The Master Agent (MA) performs the following duties:

- The MA stores systemwide component registration information.
- The MA maintains a complete set of scheduled tasks in an XML file. The MA updates this file when it receives updates of schedules from the user interface. The MA sends executable tasks to the applicable Local Agents, as scheduled. (Local Agents execute immediate-backup tasks without delay.)
- You access the MA through the Disaster Recovery System user interface to perform activities such as configuring backup devices, scheduling backups by adding new backup schedules, viewing or updating an existing schedule, displaying status of executed schedules, and performing system restoration.
- The MA stores backup data on a local directory or a remote network location.

Local Agents

The server has a Local Agent to perform backup and restore functions. The Local Agent runs backup and restore scripts on the server.

Managing Backup Devices

Before using the Disaster Recovery System, you must configure the locations where you want the backup files to be stored. You can create local or network backup devices. If you create a local backup device, Disaster Recovery System stores the backup files in the a preconfigured directory on the Cisco IME server. You must manually move local backup files from the Cisco IME server by opening an SFTP client and connecting to the Cisco IME server by using the adminsftp user and the administrator password that you set up during installation.

You can configure up to 10 backup devices. Perform the following steps to configure backup devices.

Procedure

Step 1 To access the Disaster Recovery System, log into the Cisco IME CLI as described in "How to Access the Disaster Recovery System" section on page 5-3.

The CLI admin prompt displays.

Step 2 To create a local device, enter **utils disaster_recovery device local** ***device_name number of backups***

where

device_name equals the name of the backup device. The backup device name may contain only alphanumeric characters, spaces ( ), dashes (-) and underscores (_). Do not use any other characters. By default, DRS stores backup files for local devices in the /common/adminsftp/backup directory.

number of backups equals the number of backups allowed for this device.

Step 3 To create a network device so that you can store backup files on a network drive that is accessed through an SFTP connection, enter **utils disaster_recovery device network** ***device_name path server_name username number of backups***

where

device_name equals the name of the backup device. The backup device name may contain only alphanumeric characters, spaces ( ), dashes (-) and underscores (_). Do not use any other characters.

path equals the path name for the directory where you want to store the backup file

server_name equals the name or IP address of the network server

username equals a valid username for an account on the remote system

number of backups equals the number of backups allowed for this device

Note You must have access to an SFTP server to configure a network storage location. The SFTP path must exist prior to the backup. The account that is used to access the SFTP server must have write permission for the selected path.

Note The DRS Master Agent validates the selected backup device. If the user name, password, server name, or directory path is invalid, the command will fail.

Step 4 To display a list of backup devices, enter **utils disaster_recovery *device list***.

The device name, device type, and device path for each backup device displays.

Step 5 To delete a backup device, enter **utils disaster_recovery device delete *device_name***, where *device_name* equals the name of the device that you want to delete.

Note You cannot delete a backup device that is configured as the backup device in a backup schedule. You must first delete the schedule which uses this devicename, and then delete this device.

Creating Backup Schedules

You can create up to 10 backup schedules. Each backup schedule has its own set of properties, including a schedule for automatic backups, the set of features to back up, and a storage location.

Caution Schedule backups during off-peak hours to avoid call-processing interruptions and impact to service.

Perform the following steps to create backup schedules:

Procedure

Step 1 To access the Disaster Recovery System, log into the Cisco IME CLI as described in "How to Access the Disaster Recovery System" section on page 5-3.

The CLI admin prompt displays.

Step 2 Enter **utils disaster_recovery schedule add *schedulename devicename featurelist datetime frequency***

where

schedulename equals the name of the schedule

devicename equals the location where Disaster Recovery System stores the backup files

featurelist equals IME

datetime specifies the time and date when Disaster Recovery System performs the backup. The formast equals *yyyy/mm/dd-hh:mm* . Enter the time based on a 24- hour clock.

frequency equals how often Disaster Recovery System performs the backup. Options are once, daily, weekly, and monthly.

Step 3 To enable a schedule, enter **utils disaster_recovery schedule enable *schedulename***.

The next backup occurs automatically at the time that you set.

Note To disable or delete schedules, see the "Enabling, Disabling, and Deleting Schedules" section on page 5-6.

Enabling, Disabling, and Deleting Schedules

Follow this procedure to enable, disable, or delete backup schedules.

Procedure

Step 1 To access the Disaster Recovery System, log into the Cisco IME CLI as described in "How to Access the Disaster Recovery System" section on page 5-3.

The CLI admin prompt displays.

Step 2 To view the list of backup schedules, enter **utils disaster_recovery schedule list**.

The CLI displays the device name and status for each schedule. The device name specifies where Disaster Recovery System stores the backup files.

Step 3 Perform one of the following tasks:

- To enable a schedule, enter **utils disaster_recovery schedule enable *schedulename***.
- To disable a schedule, enter **utils disaster_recovery schedule disable *schedulename***.
- To delete a schedule, enter **utils disaster_recovery schedule delete *schedulename***.

The schedules can be enabled, disabled or deleted only one at a time.

Starting a Manual Backup

Follow this procedure to start a manual backup.

Procedure

Step 1 To access the Disaster Recovery System, log into the Cisco IME CLI as described in "How to Access the Disaster Recovery System" section on page 5-3.

The CLI admin prompt displays.

Step 2 Enter **utils disaster_recovery backup** ***type featurelist device_name***

where

type equals the location of the backup, either local or network

featurelist equals IME

device_name equals the name of the backup device.

Step 3 To view the status of the current backup, enter **utils disaster_recovery status backup**.

Step 4 To cancel the current backup, enter **utils disaster_recovery cancel_backup yes**.

Checking Backup Status

You can check the status of the current backup job and cancel the current backup job. To view a list of backup files, see the "Viewing the Restore Status" section on page 5-9.

Caution Be aware that if the backup to the remote server is not completed within 20 hours, the backup session will time out. You will then need to begin a fresh backup.

Perform the following steps to check the status of the current backup job.

Procedure

Step 1 To access the Disaster Recovery System, log into the Cisco IME CLI as described in "How to Access the Disaster Recovery System" section on page 5-3.

The CLI admin prompt displays.

Step 2 To view the status of the current backup, enter **utils disaster_recovery status backup**.

Step 3 To cancel the current backup, enter **utils disaster_recovery cancel_backup yes**.

Note The backup cancels after the current component completes its backup operation.

Displaying Backup Files

Using the following procedures, you can see the list of backup files that are stored to the localor network drives:

Procedure

Step 1 To access the Disaster Recovery System, log into the Cisco IME CLI as described in "How to Access the Disaster Recovery System" section on page 5-3.

The CLI admin prompt displays.

Step 2 To view backup files, do one of the following:

- To view the list of backup files in the local directory (/common/adminsftp/backup), enter **utils disaster_recovery show_backupfiles local backup**.
- To view the list of backup files in the local restore directory (/common/adminsftp/restore), enter **utils disaster_recovery show_backupfiles local restore**.
- To view the list of backup files on a network drive, enter **utils disaster_recovery show_backupfiles network *path servername userid***

where

path equals the path name for the directory where the backup file is stored

servername equals the name or IP address of the network server

userid equals a valid user ID for an account on the remote system

Restoring a Server

You can restore the Cisco IME server from a backup file in a network directory or in a local directory. Use one of the following procedures to restore the Cisco IME server:

Caution Before you restore Cisco IME, ensure that the Cisco IME version that is installed on the server matches the version of the backup file that you want to restore. The Disaster Recovery System supports only matching versions of Cisco IME for restore. For example, the Disaster Recovery System does not allow a restore from version 8.0.(**1**).1000-1 to version 8.0.(**2**).1000-1, or from version 8.0.(1).1000-**1** to version 8.0.(1).1000-**2**. In essence, the product version needs to match, end-to-end, for the Disaster Recovery System to run a successful Cisco IME restore. Disaster Recovery System adheres to strict version checking and allows restore only between matching versions of Cisco IME.

Caution After you choose the server to which you want the data restored, any existing data on that server gets overwritten.

Procedure 1: Restoring from a Local Directory

Step 1 Copy the backup file to the Cisco IME server by opening an SFTP client, and connecting to the Cisco IME server by using the adminsftp user and the administrator password, that you set up during installation. To do that, navigate to the backup directory by entering **cd backup**, and copy the backup file to the /common/adminsftp/restore directory.

Step 2 Access the Disaster Recovery System by logging into the Cisco IME CLI as described in "How to Access the Disaster Recovery System" section on page 5-3.

The CLI admin prompt displays.

Step 3 Enter **utils disaster_recovery restore local** ***restore_server tarfilename device_name***

where

restore_server hostname of the server to be restored

tarfilename equals the name of the backup file to be restored without extension; for example, 2008-01-21-18-25-03

device_name equals the name of the backup device

Step 4 Your data gets restored on the server that you chose. To view the status of the restore, enter **utils disaster_recovery status restore**..

Step 5 Restart the server.

Procedure2: Restoring from a Network Directory

Step 1 To access the Disaster Recovery System, log into the Cisco IME CLI as described in "How to Access the Disaster Recovery System" section on page 5-3.

The CLI admin prompt displays.

Step 2 Enter **utils disaster_recovery restore network** ***restore_server tarfilename device_name***

where

restore_server hostname of the server to be restored

tarfilename file name to be restored without extension(e.g.2008-01-21-18-25-03)

device_name equals the name of the backup device

Caution After you choose the server to which you want the data restored, any existing data on that server gets overwritten.

Step 3 Your data gets restored on the server that you chose. To view the status of the restore, enter **utils disaster_recovery status restore**..

Step 4 Restart the server.

Viewing the Restore Status

To check the status of the current restore job, perform the following steps:

Procedure

Step 1 To access the Disaster Recovery System, log into the Cisco IME CLI as described in "How to Access the Disaster Recovery System" section on page 5-3.

The CLI admin prompt displays.

Step 2 To view information about the current restore job, enter **utils disaster_recovery status restore**. The status shows the restore percentage, log file location, timestamp, feature name, server name, component name, and component status.

Trace Files

For ViPR, we have following trace files:-

In this release of the Disaster Recovery System, trace files for the Master Agent, the GUI, and each Local Agent get written to the following locations:

- For the Master Agent, find the trace file at *platform/drf/trace/drfMA0**
- For each Local Agent, find the trace file at *platform/drf/trace/drfLA0**

Error Messages

The Disaster Recovery System (DRS) issues alarms for various errors that could occur during a backup or restore procedure. Table 3 provides a list of Cisco DRS alarms.

Table 3 Disaster Recovery System Alarms

Alarm Name	Description	Explanation
DRFBackupDeviceError	DRF backup process has problems accessing device.	DRS backup process encountered errors while it was accessing device.
DRFBackupFailure	Cisco DRF Backup process failed.	DRS backup process encountered errors.
DRFBackupInProgress	New backup cannot start while another backup is still running	DRS cannot start new backup while another backup is still running.
DRFInternalProcessFailure	DRF internal process encountered an error.	DRS internal process encountered an error.
DRFLA2MAFailure	DRF Local Agent cannot connect to Master Agent.	DRS Local Agent cannot connect to Master Agent.
DRFLocalAgentStartFailure	DRF Local Agent does not start.	DRS Local Agent might be down.
DRFLocalDeviceError	DRF has problems accessing local device.	DRS encountered errors while it was accessing local device.
DRFMA2LAFailure	DRF Master Agent does not connect to Local Agent.	DRS Master Agent cannot connect to Local Agent.
DRFMABackupComponent Failure	DRF cannot back up at least one component.	DRS requested a component to back up its data; however, an error occurred during the backup process, and the component did not get backed up.

Table 3 Disaster Recovery System Alarms (continued)

Alarm Name	Description	Explanation
DRFMABackupNodeDisconnect	The node that is being backed up disconnected from the Master Agent prior to being fully backed up.	While the DRS Master Agent was running a backup operation on a Cisco Unified Communications ManagerCisco Unity Connection node, the node disconnected before the backup operation completed.
DRFMARestoreComponent Failure	DRF cannot restore at least one component.	DRS requested a component to restore its data; however, an error occurred during the restore process, and the component did not get restored.
DRFMARestoreNodeDisconnect	The node that is being restored disconnected from the Master Agent prior to being fully restored.	While the DRS Master Agent was running a restore operation on a Cisco Unified Communications ManagerCisco Unity Connection node, the node disconnected before the restore operation completed.
DRFMasterAgentStartFailure	DRF Master Agent did not start.	DRS Master Agent might be down.
DRFNoRegisteredComponent	No registered components are available, so backup failed.	DRS backup failed because no registered components are available.
DRFNoRegisteredFeature	No feature got selected for backup.	No feature got selected for backup.
DRFRestoreDeviceError	DRF restore process has problems accessing device.	DRS restore process cannot read from device.
DRFRestoreFailure	DRF restore process failed.	DRS restore process encountered errors.
DRFSftpFailure	DRF SFTP operation has errors.	Errors exist in DRS SFTP operation.
DRFSecurityViolation	DRF system detected a malicious pattern that could result in a security violation.	The DRF Network Message contains a malicious pattern that could result in a security violation like code injection or directory traversal. DRF Network Message has been blocked.
DRFTruststoreMissing	The IPsec truststore is missing on the node.	The IPsec truststore is missing on the node. DRF Local Agent cannot connect to Master Agent.
DRFUnknownClient	DRF Master Agent on the Pub received a Client connection request from an unknown server outside the cluster. The request has been rejected.	The DRF Master Agent on the Pub received a Client connection request from an unknown server outside the cluster. The request has been rejected.

CHAPTER 6

Managing Services on the Cisco Intercompany Media Engine Server

TheCisco IME server contains network services and servlets that the system requires to function. Since these services are required for basic functionality, they do not require activation. However, you may need to stop and start (or restart) these services for troubleshooting purposes.

If something is wrong with a service or servlet, CriticalServiceDown alert is raised in RTMT. Alarms provide information on runtime status and the state of the system, so you can troubleshoot problems that are associated with your system. After viewing the alarm information, you can run a trace on the service. The trace files can help you further troubleshoot issues with your system.

This section contains information on services and describes how to troubleshoot issues using alarms and traces:

- Services, page 6-1
- Alarms, page 6-6
- Traces, page 6-8

Services

After the installation of the Cisco IME application, network services start on the server automatically. The network services include services that the system requires to function; for example, database and platform services. You can configure these services by setting service parameters for each service. If necessary, for example, for troubleshooting purposes, you may need to stop and start (or restart) a network service. You perform these task by using the command line interface (CLI) on the Cisco IME server.

This section provides descriptions of services/servlets and describes how to start and stop services and configure service parameters from the CLI:

- Service Descriptions, page 6-1
- Service Configuration Checklist, page 6-4
- Working with Services, page 6-5

Service Descriptions

This section describes the network services that exist of the Cisco IME server and are grouped by the following functional areas:

- Performance and Monitoring Services, page 6-2
- Backup and Restore Services, page 6-2
- System Services, page 6-3
- Platform Services, page 6-3

For information on working with services, see the "Service Configuration Checklist" section on page 6-4.

Performance and Monitoring Services

This section describes the Performance and Monitoring Services.

Cisco CallManager Serviceability RTMT

The Cisco CallManager Serviceability RTMT servlet supports the 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, and so on.

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 by using configured thresholds and a polling interval.

Cisco RIS Data Collector

The Real-time Information Server (RIS) maintains real-time 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 the Real Time Monitoring Tool (RTMT), to retrieve the information that is stored in the RIS server.

Cisco AMC Service

Used for the Real Time Monitoring Tool (RTMT), this service, Alert Manager and Collector service, allows RTMT to retrieve real-time information that exists on the server.

Cisco Audit Event Service

The Cisco Audit Event Service monitors and logs any configuration change to the Cisco IME system by a user or as a result of the user action.

Backup and Restore Services

This section describes the Backup and Restore Services.

Cisco DRF Master

The CiscoDRF Master Agent service supports the DRF Master Agent, which works with the Disaster Recovery System 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.

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 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.

System Services

This section describes the System Services.

Cisco CDP

Cisco CDP advertises the voice application to other network management applications, so the network management application, for example, SNMP or CiscoWorks Lan Management Solution, can perform network management tasks for the voice application.

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 RTMT. If you stop this service on a server, you cannot collect or view traces on that server.

For SysLog Viewer and Trace and Log Central to work in RTMT, the Cisco Trace Collection Servlet and the Cisco Trace Collection Service must run on the 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. If you stop this service on a server, you cannot collect or view traces on that server.

For SysLog Viewer and Trace and Log Central to work in RTMT, the Cisco Trace Collection Servlet and the Cisco Trace Collection Service must run on the server.

Tip If necessary, Cisco recommends that, to reduce the initialization time, you restart the Cisco Trace Collection Service before restarting Cisco Trace Collection Servlet.

Platform Services

This section describes the Platform Services.

Cisco Tomcat

The Cisco Tomcat service supports the web server.

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.

Tip After you complete SNMP configuration in the CLI, you must restart the SNMP Master Agent service in the Control Center—Network Features window.

MIB2 Agent

This service provides SNMP access to variables, which are defined in RFC 1213, that 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, and installed software base. This service implements the HOST-RESOURCES-MIB.

Native Agent Adaptor

This service, which supports vendor MIBs, 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 IME server. This service implements the CISCO-CDP-MIB.

Cisco Syslog Agent

This service supports gathering of syslog messages that various components generate. This service implements the CISCO-SYSLOG-MIB.

Cisco Certificate Expiry Monitor

This service periodically checks the expiration status of certificates that the system generates and sends notification when a certificate gets close to its expiration date.

Cisco IME Service

This service provides the primary functionality of the IME server. It manages data of the peer-to-peer network, communication to other nodes in the peer-to-peer network, and the communication to Cisco Unified Communication Manager.

Cisco IME Configuration Manager

This service manages administration and configuration settings used by the other services.

Service Configuration Checklist

Table 6-1 provides an overview of the steps for configuring services.

Table 6-1 Alarm Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Configure the appropriate service parameters.	Working with Services, page 6-5
Step 2	In the CLI, configure the server(s), service(s), destination(s), and event level(s) for the applications (services) alarm information that you want to collect. • All services can go to the SDI log (but must be configured using **`set alarm`** CLI command). • All alarms can go to the SysLog Viewer. • Ensure that Event Log alarm monitor is enabled with the desired severity. Use **`set alarm`** CLI command for this. • To send syslog messages to the Remote Syslog Server, enable the Remote Syslog destination and specify a host name. Use **`set alarm`** CLI command for configuration. If you do not configure the remote server name, the system does not send Syslog messages to the remote syslog server. **Tip** Do not configure a Cisco Unified Communications Manager server as a remote Syslog server.	• Alarms, page 6-6
Step 3	If you chose an SDI trace file as the alarm destination, collect traces and view the information with the Trace and Log Central option in RTMT.	• Traces, page 6-8 • *Cisco Unified Real Time Monitoring Tool Administration Guide*
Step 4	If you chose local syslog as the alarm destination, view the alarm information in the SysLog Viewer in RTMT.	• Traces, page 6-8 • *Cisco Unified Real Time Monitoring Tool Administration Guide*
Step 5	See the corresponding alarm definition for the description and recommended action, in the SysLog Viewer in RTMT.	• *Cisco Unified Real Time Monitoring Tool Administration Guide*

Working with Services

To start, stop, or restart services or to configure service parameters for services on the Cisco IME server, you must use the command line interface (CLI). You can start, stop, or refresh only one service at a time. Be aware that when a service is stopping, you cannot start it until after the service is stopped. Likewise, when a service is starting, you cannot stop it until after the service is started.

Caution Some changes to service parameters may cause system failure. Cisco recommends that you do not make any changes to service parameters unless you fully understand the feature that you are changing or unless the Cisco Technical Assistance Center (TAC) specifies the changes.

Table 6-2 shows the commands that you need to work with services on the Cisco IME server:

Table 6-2 Service CLI Commands

Task	Command
Display a list of services and service status	utils service list
Stop a service	utils service stop *servicename*
Start a service	utils service start *servicename*
Restart a service	utils service restart *servicename*
Show service parameters	show *servicename* serviceparam *serviceparametername* where, *servicename* can be ime, amc, risdc or enterprise. *serviceparametername* is one of the service parameters defined for that service. To see a list of serviceparameters that are defined for a service, use the following command: show *servicename* serviceparam ?
Set service parameters	set *servicename* serviceparam *service parameter name* where *servicename* equals <ime | amc | risdc | enterprise> and *service parameter name* is one of the service parameters defined for that service.

Additional Information

Related Topics, page 6-11

Alarms

Alarms provide information on runtime status and the state of the system, so you can troubleshoot problems that are associated with your system; for example, to identify issues with the Disaster Recovery System. Alarm information, which includes an explanation and recommended action, also includes the application name, machine name, and so on, to help you perform troubleshooting.

You configure the alarm interface to send alarm information to multiple locations, and each location 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, or to all destinations.

When a service issues an alarm, the alarm interface sends the alarm information to the locations that you configure (and that are specified in the routing list in the alarm definition) (for example, SDI trace). The system can either forward the alarm information, as is the case with SNMP traps, or the system can write the alarm information to its final destination (such as a log file).

You use the Trace and Log Central option in the Real Time Monitoring Tool (RTMT) to collect alarms that get sent to an SDI trace log file. You use the SysLog Viewer in RTMT to view alarm information that gets sent to the local syslog.

As soon as you enter the CLI command, the system will prompt you for the required parameters. Enter the values to see the output.

Table 6-2 shows the commands that you need to work with alarms on the Cisco IME server:

Table 6-3 Alarm CLI Commands

Task	Command
Display the alarm configuration for a specific service/list of all services	show alarm Required Parameter(s): *servicename*—Name of the service. It could contain multiple words. Example: Enter the servicename as *all* to show the alarm configurations of all the services. Enter the servicename as *Cisco Tomcat* to show the alarm configuration of Cisco Tomcat service.
Enable/Disable alarms for a particular destination	set alarm *status* Required Parameter(s): *status*—enable or disable. *servicename*—Name of the service. It could contain multiple words. *monitorname*—SDI, SDL, Event_Log, or Sys_Log.
Enable alarms for a remote Syslog server	set alarm remotesyslogserver Required Parameter(s): *servicename*—Name of the service. It could contain multiple words. *servername*—Name of the remote syslog server.

Table 6-3 Alarm CLI Commands (continued)

Task	Command
Set the event level for an alarm	set alarm *severity* Required Parameter(s): *servicename*—Name of the service. It could contain multiple words. *monitorname*—SDI, SDL, Event_Log, or Sys_Log. *severity* equals one of the following: – Emergency—This level designates the system as unusable. – Alert—This level indicates that immediate action is needed. – Critical—The system detects a critical condition. – Error—This level signifies that 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.
Set alarm configuration to default values **Tip** This option is available only for service names beginning with Cisco.	set alarm default Required Parameter(s): *servicename*—Name of the service. It could contain multiple words.

Additional Information

Related Topics, page 6-11

Traces

Traces assist you in troubleshooting issues with your application. You use the CLI to specify the level of information that you want traced as well the type of information that you want to be included in each trace file. You can configure trace parameters for any service on the Cisco IME server.

You can direct alarms to various locations, including SDI trace log files. If you want to do so, you can configure trace for alerts in the Real Time Monitoring Tool (RTMT).

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 Real Time Monitoring Tool. To do this, configure alarms using **set alarm** CLI command.

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)

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 *Cisco Unified Real Time Monitoring Tool Administration Guide*.

Configuring Trace

You use the command line interface (CLI) to enable and disable tracing as well as to configure trace settings for specific services on the Cisco IME server. As soon as you enter the CLI command, the system prompts you for the required parameters. After the system generates trace files, you use RTMT to collect them. For more information regarding trace collection, see the "Collecting Traces" section on page 6-10 and refer to the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

Table 6-4 shows the commands that you need to work with traces on the Cisco IME server:

Table 6-4 Trace CLI Commands

Task	Command
Display the trace configuration for a specified service	show trace Required Parameter(s): *servicename*—Name of the service. It could contain multiple words. Example: Enter the servicename as *all* to show the trace configurations of all the services. Enter the servicename as *Cisco AMC Service* to show the trace configuration of Cisco AMC service.
Display the trace levels available for a specified service	show tracelevels Required Parameter(s): *servicename*—Name of the service. It could contain multiple words.
Enable/Disable trace for a specified service	set trace *status* Required Parameter(s): *status*— enable or disable *servicename*—Name of the service. It could contain multiple words.

Table 6-4 Trace CLI Commands (continued)

Task	Command
Specify the debug trace level settings for a specified service	set trace *tracelevel* Required Parameter(s): *tracelevel*—Use show tracelevels CLI command, to find the tracelevels for a given servicename. *servicename*—Name of the service. It could contain multiple words.
Specify the maximum size of a trace files for a specific service from 1 to 10 megabytes.	set trace maxfilesize Required Parameter(s): *servicename*—Name of the service. It could contain multiple words. *size*—Maximum size of the trace files from 1 to 10 megabytes.
Specify the maximum number of trace files per service. The system automatically appends a sequence number to the file name to indicate which file it is; for example, cus299.txt. When the last file in the sequence is full, the trace data begins writing over the first file.	set trace maxnumfiles Required Parameter(s): *servicename*—Name of the service. It could contain multiple words. *filecount*—Number of trace files from 1 to 10000.
Set the usercategories flag to the value provided, for a specified service. **Tip** This option is available only for service names beginning with Cisco.	set trace usercategories Required Parameter(s): *flagnumber*—Hexadecimal value from 0 to 7FFF. 7FFF means all the flags are enabled. *servicename*—Name of the service. It could contain multiple words.
Set trace configuration to default values for a specified service. **Tip** This option is available only for service names beginning with Cisco.	set trace default Required Parameter(s): *servicename*—Name of the service. It could contain multiple words.

Additional Information

Related Topics, page 6-11

Collecting Traces

The trace and log central feature in the Cisco Unified Real-Time Monitoring Tool (RTMT) allows you to configure on-demand trace collection for a specific date range or an absolute time. You can collect trace files that contain search criteria that you specify and save the trace collection criteria for later use, schedule one recurring trace collection and download the trace files to a SFTP or FTP server on your network, or to the localhost, or collect a crash dump file.

After you collect the files, you can view them in the appropriate viewer within the real-time monitoring tool. You can also view traces on the server without downloading the trace files by using the remote browse feature. You can open the trace files by either selecting the internal viewer that is provided with RTMT or choosing an appropriate program as an external viewer.

Note From RTMT, you can also edit the trace setting for the traces on the server that you have specified. Enabling trace settings decreases system performance; therefore, enable Trace only for troubleshooting purposes.

Note To use the trace and log central feature in the RTMT, make sure that RTMT can directly access the server without Network Access Translation (NAT). If you have set up a NAT to access devices, configure the server(s) with a hostname instead of an IP address and make sure that the host names and their routable IP address are in the DNS server or host file.

Additional Information

Related Topics, page 6-11

Related Topics

- Services, page 6-1
- Service Descriptions, page 6-1
- Service Configuration Checklist, page 6-4
- Working with Services, page 6-5
- Alarms, page 6-6
- Traces, page 6-8
- Configuring Trace, page 6-9
- Collecting Traces, page 6-10

CHAPTER 7

Using RTMT with Cisco Intercompany Media Engine

RTMT provides a set of default monitoring objects that assist you in monitoring the health of the Cisco Intercompany Media Engine product. You monitor the Cisco Intercompany Media Engine product on the Cisco IME server and on the Cisco Unified Communications Manager server. The objects on the Cisco Unified Communications Manager contain information about learned routes and call activities. The objects on the Cisco IME server contain information about network and server activity.

The system logs data every five minutes for predefined counters.

This chapter contains information on the following topics:

- Installing RTMT, page 7-1
- Uninstalling RTMT, page 7-3
- Launching RTMT, page 7-3
- Navigating RTMT, page 7-4
- Monitoring Predefined Cisco Intercompany Media Engine Objects in RTMT, page 7-5
- Working with Trace and Log Central, page 7-8
- Related Topics, page 7-8

Installing RTMT

A single copy of RTMT that is installed on your computer lets you monitor only one server or one cluster at a time. For example, you can monitor either of the following entities:

- A Cisco Unified Communications Manager product on one server
- A server on a cluster to monitor the health of the cluster

To monitor a product on a different server, such as the Cisco Intercompany Media Engine product on the Cisco IME server, you must first log off the server before you can log on to the other server.

Consider the following, before you install RTMT:

- On a client machine, you can install RTMT client downloaded from only one product type such as Cisco Unified Communications Manager or Cisco Intercompany Media Engine. Installing RTMT client from different product types on the same client machine is not supported.

- The current RTMT download may not support earlier releases of Cisco Unified Communications Manager. Some releases of Cisco Unified Communications Manager may require different versions of RTMT to be installed on your computer (one version per Cisco Unified Communications Manager release). Verify that the RTMT version that you install is compatible with the Cisco Unified Communications Manager that you are monitoring. If the RTMT version that you are using is not compatible with the server that you want to monitor, the system prompts you to download the compatible version.
- Your computer stores the user preferences, such as the IP address and RTMT frame size, from the RTMT client that last exits.

To install RTMT from the Cisco IME server, perform the following procedure:

Note When you install RTMT on a Windows Vista platform, the following User Account Control pop-up message displays: "An unidentified program wants to access your computer." Click **Allow** to continue working with RTMT.

Note When you launch RTMT, log into the same product type from which you downloaded the RTMT client application. If you log into a different product type, RTMT will not launch nor work properly.

Procedure

Step 1 Start your preferred operating system browser.

Note Microsoft Internet Explorer has a known bug, which doe not let you download IME RTMT from an IME server. You can use other browsers like FireFox, Safari, and so forth.

Step 2 In the address bar of the web browser, enter the following case-sensitive URL:

https://<Cisco IME-server-name>:{8443}/ast/rtmtinstaller.jsp

where: <Cisco IME-server-name> equals the name or IP address of the Cisco IME server

Note You can optionally specify a port number.

Step 3 A Security Alert dialog box displays. Click the appropriate button.

Step 4 Enter the Administrator username and password that you specified during installation.

Step 5 Do one of the following:

- If you are planning to install the RTMT tool on a computer that is running the Microsoft Windows operating system, click the RTMT Windows Installer link.
- If you are planning to install the RTMT tool on a computer that is running the Linux operating system, click the RTMT Linux Installer link.

Step 6 Download the executable to the preferred location on your client.

Step 7 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 8 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 9 After the RTMT welcome window displays, click **Next**.

Step 10 To accept the license agreement, click **I accept the terms of the license agreement**; then, click **Next**.

Step 11 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**.

Default installation paths specify the following:

- Windows—C:\Program Files\Cisco\Unified-Communications-Manager Serviceability\JRtmt
- Linux—/opt/Cisco/Unified-Communications-Manager_Serviceability/JRtmt

Step 12 To begin the installation, click **Next**.

The Setup Status window displays. Do not click **Cancel**.

Step 13 To complete the installation, click **Finish**.

Uninstalling RTMT

Tip When you use RTMT, it saves user preferences and the module jar files (the cache) locally on the client machine. 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 Hat Linux with KDE and/or Gnome client, choose **Start > Accessories > Uninstall Real-time Monitoring tool** from the task bar.

Note When you uninstall RTMT on a Windows Vista machine, the following User Account Control pop-up message displays: “An unidentified program wants to access your computer.” Click **Allow** to continue working with RTMT.

Launching RTMT

Note When you use RTMT on a Windows Vista machine, the following User Account Control pop-up message displays: “An unidentified program wants to access your computer.” Click **Allow** to continue working with RTMT.

Procedure

Step 1 After you install the plug-in, perform one of the following tasks:

- From your Windows desktop, double-click the **Real-Time Monitoring Tool** icon.
- Choose **Start > Programs > Cisco > Unified-Communications-Manager 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 server or (if applicable) first server in a cluster.

Step 3 In the User Name field, enter the Administrator username for the application.

Step 4 In the Password field, enter the Administrator 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 server, when the local cache does not contain a monitoring module that matches the backend version.

Step 5 Enter the port that the application will use to listen to the server. The default setting specifies 8443.

Note The Trace and Log Central tool in RTMT uses the port number that you specify to communicate with all the nodes in a cluster. If your system uses port mapping and all Cisco Intercompany Media Engine nodes do not map to the same port number, some RTMT tools can not connect to those nodes. The tools that will fail to connect include Trace and Log Central, Job Status, SyslogViewer, Perfmon Log Viewer, and FTP/SFTP Configuration.

Step 6 Check the **Secure Connection** check box.

Step 7 Click **OK**.

Step 8 When prompted, add the certificate store by clicking **Yes**.

Real-Time Monitoring Tool RTMT starts.

Navigating RTMT

The RTMT window comprises the following main components:

- Menu Bar, which includes some or all of the following menu options, depending on your configuration:
  - File—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 Serviceability, log off, or exit RTMT.

Note The RTMT menu option **File > Cisco Unified Reporting** lets you access Cisco Unified Reporting from RTMT. You can use the Cisco Unified Reporting application to snapshot Cisco Unified Communications Manager cluster data for inspection or troubleshooting. Refer to the *Cisco Unified Reporting Administration Guide* for more information.

  - System—Allows you to monitor system summary, monitor server resources, work with performance counters, work with alerts, collect traces, and view syslog messages.
  - Communications Manager—Allows you to view Cisco Unified Communications Manager summary information on the server; monitor call-processing information; and view and search for devices, monitor services, and CTI.
  - Unity Connection—Allows you to view the Port Monitor tool.
  - IME Service—Allows you monitor server and network activity of the Cisco Intercompany Media Engine server.
  - 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.
  - Window—Allows you to close a single RTMT window or all RTMT windows.
  - Application—Depending on your configuration, allows you to browse the applicable web pages for Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, Cisco Unity Connection Administration, and Cisco Unity Connection Serviceability.
  - Help—Allows you to access RTMT documentation online help or to view the RTMT version.
- Quick Launch Channel—You can click this pane with tabs on the left side of the RTMT window to display information about the server or information about the applications. The tab contains groups of icons that you can click to monitor various objects.
- Monitor pane—Pane where monitoring results display.

Monitoring Predefined Cisco Intercompany Media Engine Objects in RTMT

RTMT provides a set of predefined monitoring objects that assist you in monitoring the health of the Cisco Intercompany Media Engine feature. On the Cisco Unified Communications Manager server, you can monitor the call processing activity and routing activity of Cisco IME calls. On the Cisco Intercompany Media Engine server, you can monitor a variety of statistics related to Internet bandwidth and IME distributed cache status. You need objects from both servers to monitor the performance of the Cisco Intercompany Media Engine product.

This section contains the following information:

- Monitoring the Intercompany Media Services Predefined Object on the Cisco Unified Communications Manager Server, page 7-6
- Monitoring Objects on the Cisco IME Server, page 7-7

Monitoring the Intercompany Media Services Predefined Object on the Cisco Unified Communications Manager Server

Tip The polling rate in each precanned monitoring window remains fixed, and the default value specifies 30 seconds. If the collecting rate for the AMC (Alert Manager and Collector) service parameter changes, the polling rate in the precanned window also updates. In addition, the local time of the RTMT client application, not the backend server time, provides the basis for the time stamp in each chart.

Tip To zoom in on the monitor of a predefined object, click and drag the left mouse button over the area of the chart that interests you. 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.

The Intercompany Media Services monitoring category monitors the following items:

- Routing—Displays the total number of Cisco Intercompany Media Engine routes that Cisco Unified Communications Manager maintains. This total includes the following routes:
  - Learned routes that represent the phone numbers that the Cisco Intercompany Media Engine client learned and that exist in the Cisco Unified Communications Manager routing tables
  - Unique domains of peer enterprises for which Cisco Intercompany Media Engine routes exist
  - Published routes that represent the number of direct inward dialing numbers (DIDs) that were published successfully to the IME distributed hash table across all Cisco Intercompany Media Engine services
  - Rejected routes that represent the number of learned routes that got rejected because the administrator blocked them.

  These charts represent the following performance counters for the Cisco IME Client performance object: RoutesLearned, DomainsUnique, RoutesPublished, and RoutesRejected.

  To display information on routing, choose **CallManager > Cisco IME Client > Routing**.
- Call Activities—Allows you to monitor the total number of Cisco Intercompany Media Engine calls. This total includes the following types of calls:
  - Calls that were attempted (including calls that were accepted, busy, no answer, and failed)
  - Calls that were received
  - Calls that were set up (that is, made by Cisco Unified Communications Manager and accepted by the remote party)
  - Calls that were accepted (that is, received by Cisco Unified Communications Manager and answered by the called party)
  - Calls that completed fallback to the PSTN
  - Calls that did not successfully fallback to the PSTN.

  These charts represent the following performance counters for the Cisco IME Client performance object: CallsAttempted, CallAccepted, CallsReceived, CallsSetup, IMESetupsFailed, and FallbackCallsFailed.

  To display information on call activities, choose **CallManager > Cisco IME Client > Call Activities**.

For more information about available objects and counters, see "Cisco Intercompany Media Engine Performance Objects and Counters" section on page 11-1.

Monitoring Objects on the Cisco IME Server

The Cisco IME server contains the following objects:

- Monitoring IME Service, page 7-7
- Monitoring IME System Performance, page 7-8

Monitoring IME Service

The IME Service category monitors the following items:

- Network Activity—Displays the activity on the Cisco Unified Communications Manager that relates to Cisco Intercompany Media Engine. The Network Activity object displays these charts:
  - IME Distributed Cache Health—Displays the health of the IME distributed cache based on the IMEDistributedCacheHealth counter for the IME Server performance object.
  - IME Distributed Node Count—Displays an approximation of the number of nodes in the IME distributed cache, based on the value of the IMEDistributedCacheNodeCount counter for the IME Server performance object. Because each physical Cisco Intercompany Media Engine server contains multiple nodes, the number that displays in the chart does not indicate the number of physical Cisco Intercompany Media Engine servers that participate in the IME distributed cache.
  - Internet BW Received—Displays the amount of bandwidth in Kbits/s that the Cisco IME service uses for incoming Internet traffic and represents the InternetBandwidthRecv counter for the IME Server performance object.
  - Internet BW Send—Displays the amount in Kbits/s that the Cisco IME service uses for outgoing Internet traffic and represents the InternetBandwidthSend counter for the IME Server performance object.
  - IME Distributed Cache Stored Data Records—Displays the number of IME Distributed Cache records that the Cisco Intercompany Media Engine server stores and represents the IMEDistributedCacheStoredData counter for the IME Server performance object.

  To display information on network activity, choose **Cisco IME Service > Network Activity**.
- Server Activity—Allows you to monitor the activity on the Cisco Intercompany Media Engine server. The Server Activity object displays these charts:
  - Number of Registered Clients—Displays the current number of clients that connect to the Cisco IME service and represents the value of the ClientsRegistered counter for the IME Server performance object.
  - IME Distributed Cache Quota—Indicates the number of individual DIDs that can be written into the IME Distributed Cache, by Cisco Unified CMs attached to this IME server. This number is determined by the overall configuration of the IME Distributed Cache, and the IME license installed on the IME server.
  - IME Distributed Cache Quota Used—Indicates the total number of unique DID numbers that have been configured, to be published via enrolled patterns for Intercompany Media Services, by Cisco Unified CMs currently attached to this IME server.

- Terminating VCRs—Indicates the total number of IME voice call records that are stored on the Cisco IME server for the terminating side of a call. These records can be used for validation of learned routes.
- Validations Pending—Displays the number of pending validations on the Cisco IME service as well as the threshold for validations. This chart represents the ValidationsPending counter for the Cisco IME Server performance object.

To display information on server activity, choose **Cisco IME Service > Server Activity**.

For more information about available objects and counters, see "Cisco Intercompany Media Engine Performance Objects and Counters" section on page 11-1.

Monitoring IME System Performance

The IME System Performance monitoring category provides the SDL Queue object that 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 server or for an entire cluster (if applicable).

To display information on the SDL Queue, choose **Cisco IME Service > SDL Queue**. Select the type from the SDL Queue Type drop-down list box.

For more information about available objects and counters, see "Cisco Intercompany Media Engine Performance Objects and Counters" section on page 11-1.

Working with Trace and Log Central

The trace and log central feature in the Cisco Unified Real Time Monitoring Tool (RTMT) allows you to configure on-demand trace collection for a specific date range or an absolute time. You can collect trace files that contain search criteria that you specify and save the trace collection criteria for later use, schedule one recurring trace collection and download the trace files to a FTP or SFTP server on your network or to local (localhost) files on the Cisco IME, or collect a crash dump file.

If you download trace files to the localhost directories on the Cisco IME, you can access the files by opening an SFTP client. You connect to the Cisco IME server by using the adminsftp that you configured during installation.

For more information on using RTMT to collect traces, refer to the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

Related Topics

- Installing RTMT, page 7-1
- Uninstalling RTMT, page 7-3
- Launching RTMT, page 7-3
- Navigating RTMT, page 7-4
- Monitoring Predefined Cisco Intercompany Media Engine Objects in RTMT, page 7-5
- Working with Trace and Log Central, page 7-8
- Cisco IME Configuration in Cisco Unified Communications Manager Administration, page 3-1

- Cisco Intercompany Media Engine Performance Objects and Counters, page 11-1
- Cisco Intercompany Media Engine Alert Descriptions and Default Settings, page 12-1
- *Cisco Unified Real Time Monitoring Tool Administration Guide*

CHAPTER 8

Generating the Cisco IME Client Call Activity Report

The Cisco Serviceability Reporter service generates daily reports, including the Performance Protection Report, in Cisco Unified Serviceability. Each report provides a summary that comprises different charts that display the statistics for that particular report. Reporter generates reports once a day on the basis of logged information. You can access the reports that Reporter generates in Cisco Unified Serviceability from the Tools menu. Each summary report comprises different charts that display the statistics for that particular report. After you activate the service, report generation may take up to 24 hours. For a Cisco Unified Communications Manager cluster configuration, Reporter displays the data for each server in the cluster separately.

The Performance Protection Report provides trend analysis information on default monitoring objects for the last seven that allows you to track information about Cisco Intercompany Media Engine. The Performance Protection Report includes the Cisco IME Client Call Activity chart that shows the total calls and fallback call ratio for the Cisco IME client. The chart comprises two lines, one for the number of Cisco IME calls that were attempted and calls that were completed per hour for the last hour and one for the proportion of Cisco IME calls that have fallen back to the PSTN during the current hour and previous hour. If no data exists, Reporter generates a horizontal line on the bottom of the chart.

Table 8-1 provides a configuration checklist for configuring the Cisco Serviceability Reporter service on the Cisco Unified Communications Manager. server.

Note For more information on the Cisco Serviceability Reporter, refer to the *Cisco Unified Serviceability Administration Guide*.

Table 8-1 Serviceability Reports Archive Configuration Checklist

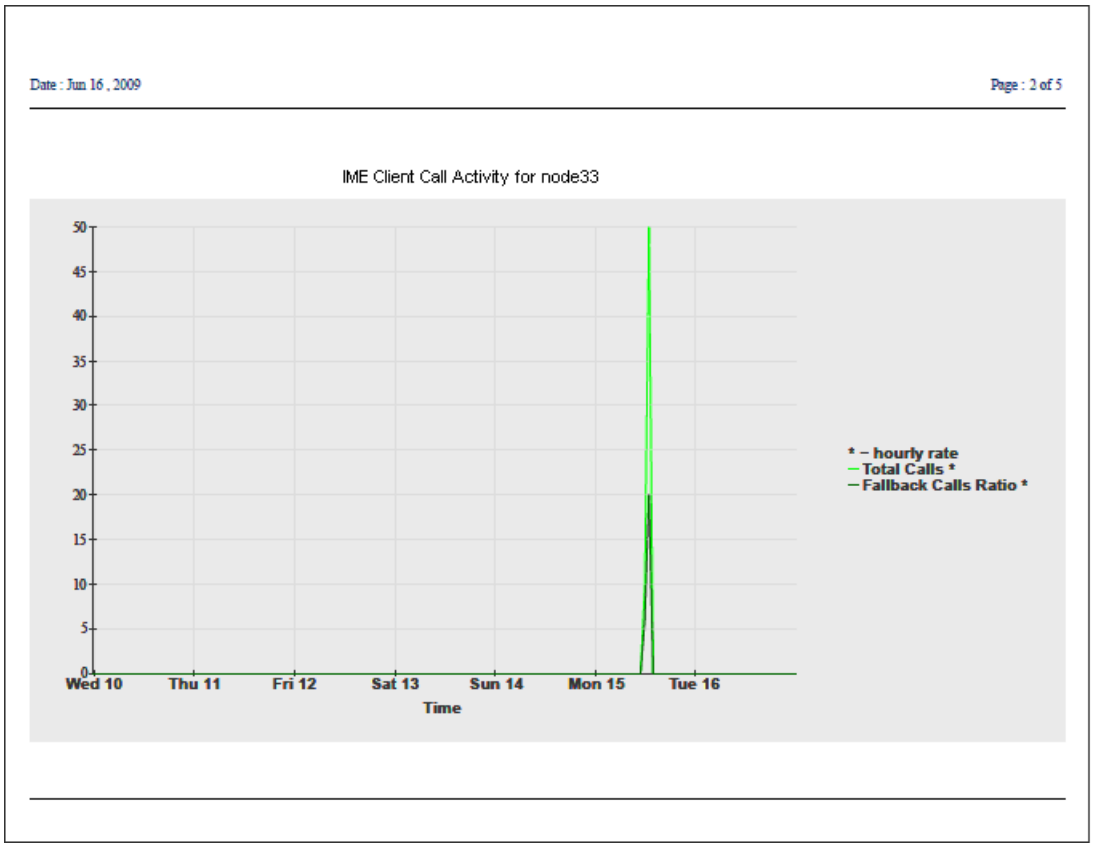
Configuration Steps		Related Procedures and Topics
Step 1	Activate the Cisco Serviceability Reporter service.	1. Choose **Tools > Service Activation**. The Service Activation window displays. 2. From the Server drop-down list box, choose the server where you want to activate the service; then, click **Go**. For a Cisco Unified Communications Manager cluster configuration, choose the first node. 3. Check the Cisco Serviceability Reporter check box, and click **Save**.

Table 8-1 Serviceability Reports Archive Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 2	Configure the Cisco Serviceability Reporter service parameters.	1. Choose **System > Service Parameters**. 2. From the Server drop-down list box, choose a server. For a Cisco Unified Communications Manager cluster configuration, choose the first node. 3. From the Service drop-down list box, choose the Cisco Serviceability Reporter service. 4. To view a list of parameters and their descriptions, click the question mark button. To view the list with a particular parameter at the top, click that parameter in the Service Parameter Configuration window. 5. 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. 6. Click **Save**.
Step 3	View the reports that the Cisco Serviceability Reporter service generates.	1. Choose **Tools > Serviceability Reports Archive**. The Serviceability Reports Archive window displays the month and year for which the reports are available. 2. From the Month-Year pane, choose the month and year for which you want to display reports. A list of days that correspond to the month displays. 3. To view reports, click the link that corresponds to the day for which reports were generated. The report files for the day that you chose display. 4. To view a particular PDF report, click the link of the report that you want to view. If you browsed into Cisco Unified Serviceability by using the server name, you must log in to Cisco Unified Serviceability before you can view the report. If your network uses Network Address Translation (NAT) and you are trying to access serviceability reports inside the NAT, enter the IP address for the private network that is associated with the NAT in the browser URL. If you are trying to access the reports outside the NAT, enter the public IP address, and NAT will accordingly translate/map to the private IP address. To view PDF reports, you must install Acrobat ® Reader on your machine. To download Acrobat Reader, click the link at the bottom of the Serviceability Reports Archive window. A window opens and displays the PDF file of the report that you chose.

Figure 8-1 shows an example of the Cisco IME Client Call Activity Report.

Figure 8-1 Cisco IME Client Call Activity Report



CHAPTER 9

Configuring SNMP on the Cisco IME Server

SNMP version 3 provides security features such as authentication (verifying that the request comes from a genuine source), privacy (encryption of data), authorization (verifying that the user allows the requested operation), and access control (verifying that the user has access to the objects requested.) To prevent SNMP packets from being exposed on the network, you can configure encryption with SNMPv3.

This chapter describes how to configure SNMP v3, so the network management system can monitor Cisco IME and contains the following topics:

- SNMP Configuration Checklist, page 9-1
- SNMP Users, page 9-3
- SNMP Trap Notification Destinations, page 9-4
- MIB2 System Group, page 9-7

SNMP Configuration Checklist

Table 9-1 provides an overview of the steps for configuring SNMP.

Table 9-1 SNMP Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Install and configure the SNMP NMS.	SNMP product documentation that supports the NMS
Step 2	In the CLI, verify that the system started the SNMP services, including: • SNMP Master Agent • Native Agent • System Application Agent • Cisco Syslog Agent • MIB2 Agent • Host Resources Agent	At the Cisco IME command line, type the following command: utils service list
Step 3	Configure the SNMP user.	SNMP Users, page 9-3
Step 4	Configure the notification destination for traps or informs.	• SNMP Trap Notification Destinations, page 9-4 • SNMP Inform Notification Destination, page 9-5

Table 9-1 SNMP Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 5	Configure the system contact and location for the MIB2 system group.	MIB2 System Group, page 9-7
Step 6	Configure trap settings for CISCO-SYSLOG-MIB.	Use these guidelines to configure CISCO-SYSLOG-MIB trap settings on your system: • Set clogsNotificationEnabled (1.3.6.1.4.1.9.9.41.1.1.2) to true by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID to true from the linux command line using: snmpset -c <*community string*> -v2c <*transmitter ipaddress*> 1.3.6.1.4.1.9.9.41.1.1.2.0 i 1 You can also use any other SNMP management application for the SNMP Set operation. • Set clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3) value by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID value from the linux command line using: snmpset -c public -v2c 1<*transmitter ipaddress*> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <*value*> Enter a severity number for the <value> setting. Severity values increase as severity decreases. A value of 1 (Emergency) indicates highest severity, and a value of 8 (Debug) indicates lowest severity. Syslog agent ignores any messages greater than the value that you specify; for example, to trap all syslog messages, use a value of 8.
Step 7	Restart the SNMP Master Agent service. (Optional) **Tip** The system automatically restarts the SNMP Master Agent after you execute the utils snmp config commands.	At the Cisco IME command line, type the following command: utils service start SNMP Master Agent
Step 8	On the NMS, configure the Cisco IME trap parameters.	• SNMP Management Information Base (MIB), page 9-8 • SNMP product documentation that supports the NMS

Additional Information

See the "Related Topics" section on page 9-11.

SNMP Users

Table 9-2 shows the commands that you need to work with SNMP users on the Cisco IME server:

Table 9-2 Trace CLI Commands

Task	Command
List the SNMP users.	utils snmp config user 3 list
Add an SNMP user	utils snmp config user 3 add The system prompts you for the parameters. See Table 9-3 for parameter names and descriptions.
Update an SNMP user	utils snmp config user 3 update The system prompts you for the parameters. See Table 9-3 for parameter names and descriptions.
Delete an SNMP user.	utils snmp config user 3 delete The system prompts you for the parameters. See Table 9-3 for parameter names and descriptions.

SNMP User CLI Parameters

Table 9-3 describes the SNMP user parameter settings for V3.

Table 9-3 SNMP User Parameter Settings for V3

Field	Description
username	The name of the user for which you want to provide access. The name can contain up to 32 characters and can contain any combination of alphanumeric characters, hyphens (-), and underscore characters (_). **Tip** Enter users that you have already configured for the network management system (NMS).
authprotocol	Authentication protocol. To specify HMAC-SHA, enter SHA.
authpassphrase	Specifies the authentication protocol password. The password must contain at least 8 characters.
privprotocol	Specifies the privacy protocol, either AES128, AES192, or AES256
privpassphrase	Specifies the privacy protocol password. The password must contain at least 8 characters.

Table 9-3 SNMP User Parameter Settings for V3 (continued)

Field	Description
accessprivilege	Enter one of the following options for the access level: • **ReadOnly**—The user can only read the values of MIB objects. • **ReadWrite**—The user can read and write the values of MIB objects. • **ReadWriteNotify**—The user can read and write the values of MIB objects and send MIB object values for a trap and inform messages. • **NotifyOnly**—The user can only send MIB object values for trap and inform messages. • **ReadNotifyOnly**—The user can read values of MIB objects and also send the values for trap and inform messages. • **None**—The user cannot read, write, or send trap information. **Tip** To change the trap configuration parameters, you need to configure a user with NotifyOnly, ReadNotifyOnly, or ReadWriteNotify privileges.
ipaddress1	Specify an IP address from which to accept packets. The default specifies to accept packets from all hosts.
ipaddress2	Specify an IP address from which to accept packets. The default specifies to accept packets from all hosts.

Additional Information

See the "Related Topics" section on page 9-11.

SNMP Trap Notification Destinations

An SNMP agent sends notifications to NMS in the form of traps or informs to identify important system events. Traps do not receive acknowledgments from the destination whereas informs do receive acknowledgments.

The following section applies to SNMP V3 notification destination configuration.

Table 9-4 shows the commands that you need to work with SNMP trap notification destinations on the Cisco IME server:

Table 9-4 SNMP Trap Notification Destinations CLI Commands

Task	Command
List trap notification destinations.	utils snmp config trap 3 list
Add a v3 trap notification destination that is associated with a configured v3 username.	utils snmp config trap 3 add The system prompts you for the parameters. See Table 9-5 for parameter names and descriptions.

Table 9-4 SNMP Trap Notification Destinations CLI Commands (continued)

Task	Command
Update a trap notification destination.	utils snmp config trap 3 update The system prompts you for the parameters. See Table 9-5 for parameter names and descriptions.
Delete a trap notification destination.	utils snmp config trap 3 delete The system prompts you for the parameters. See Table 9-5 for parameter names and descriptions.

Trap Notification Destination Parameter Settings

Table 9-5 describes the trap notification destination parameter settings for V3.

Table 9-5 Trap Notification Destination Parameter Settings for V3

Field	Description
ipaddress	The host IP address of the notification destination.
portno	The notification-receiving port number on the destination server.
oldportno	The notification-receiving port number on the destination server that is currently configured.
newportno	The notification-receiving port number on the destination server that you want to use when updating the trap notification destination.
username	Specifies the SNMP user associated to the notification destination.

Additional Information

See the "Related Topics" section on page 9-11.

SNMP Inform Notification Destination

An SNMP agent sends notifications to NMS in the form of traps or informs to identify important system events. Traps do not receive acknowledgments from the destination whereas informs do receive acknowledgments.

Table 9-6 describes the inform notification destination configuration settings for V3.

Table 9-6 SNMP Inform Notification Destination CLI Commands

Task	Command
List inform notification destinations.	utils snmp config inform 3 list
Add a v3 inform notification destination.	utils snmp config inform 3 add The system prompts you for the parameters. See Table 9-7 for parameter names and descriptions.

Table 9-6 SNMP Inform Notification Destination CLI Commands (continued)

Task	Command
Update an inform notification destination.	utils snmp config inform 3 update The system prompts you for the parameters. See Table 9-7 for parameter names and descriptions.
Delete an inform notification destination.	utils snmp config inform 3 delete The system prompts you for the parameters. See Table 9-7 for parameter names and descriptions.

Inform Notification Destination Parameter Settings

Table 9-7 Inform Notification Destination Parameter Settings for V3

Field	Description
ipaddress	The host IP address of the notification destination.
portno	The notification-receiving port number on the destination server.
oldportno	The notification-receiving port number on the destination server that is currently configured.
newportno	The notification-receiving port number on the destination server that you want to use when updating the inform notification destination.
username	Specifies the SNMP user associated to the notification destination.
oldusername	Specifies the v3 username that is currently associated with the inform.
newusername	Specifies the v3 username that you want to associate with the inform.
deleteuserconf	Specifies confirmation for deleting the old user, either Y or N.
authprotocol	Authentication protocol. To specify HMAC-SHA, enter SHA.
authpassphrase	Specifies the authentication protocol password. The password must contain at least 8 characters.
privprotocol	Specifies the privacy protocol, either AES128, AES192, or AES256
privpassphrase	Specifies the privacy protocol password. The password must contain at least 8 characters.
accessprivilege	Enter one of the following options for the access level: • **ReadWriteNotify**—The user can read and write the values of MIB objects and send MIB object values for a trap and inform messages. • **NotifyOnly**—The user can only send MIB object values for trap and inform messages. • **ReadNotifyOnly**—The user can read values of MIB objects and also send the values for trap and inform messages.
engineId	Specifies the remote engine ID of the server to which to send inform messages.

Additional Information

See the "Related Topics" section on page 9-11.

MIB2 System Group

You can use the CLI to configure the system contact and system location objects for the MIB-II system group. For example, you could enter Administrator, 555-121-6633, for the system contact and San Jose, Bldg 23, 2nd floor, for the system location.

Table 9-8 shows the commands that you need to work with MIB2 system groups on the Cisco IME server:

Table 9-8 MIB2 CLI Commands

Task	Command
List the MIB2 system group configuration	utils snmp config mib2 list
Add a MIB2 system group	utils snmp config mib2 add The system prompts you for the parameters. See Table 9-9 for parameter names and descriptions.
Update a MIB2 system group	utils snmp config mib2 update The system prompts you for the parameters. See Table 9-9 for parameter names and descriptions.
Delete a MIB2 system group	utils snmp config mib2 delete The system prompts you for the parameters. See Table 9-9 for parameter names and descriptions.

MIB2 System Group CLI Parameters

Table 9-9 describes the MIB2 System Group parameter settings.

Table 9-9 MIB2 System Group Parameter Settings

Field	Description
Server	The server for which you want to configure contacts.
SysContact	Specifies a person to notify when problems occur.
SysLocation	Specifies the location of the person that is identified as the system contact.

Additional Information

See the "Related Topics" section on page 9-11.

SNMP Management Information Base (MIB)

SNMP allows access to Management Information Base (MIB), which is a collection of information that is organized hierarchically. MIBs comprise managed objects, which are identified by object identifiers. A MIB object, which contains specific characteristics of a managed device, comprises one or more object instances (variables).

The SNMP interface provides these Cisco Standard MIBs:

- CISCO-CDP-MIB
- CISCO-SYSLOG-MIB

The Simple Network Management Protocol (SNMP) extension agent resides in the server and exposes the CISCO-CCM-MIB, which provides detailed information about devices that are known to the server. In the case of a cluster configuration, the SNMP extension agent resides in each server in the cluster. The CISCO-CCM-MIB provides device information such as device registration status, IP address, description, and model type for the server (not the cluster, in a configuration that supports clusters).

The SNMP interface also provides these Industry Standard MIBs:

- SYSAPPL-MIB
- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB

For vendor-specific supported hardware MIBS, refer to the "Vendor-Specific MIBs" section.

Cisco IME SNMP Interface supports the following MIBs.

CISCO-CDP-MIB

Use the Cisco Unified Communications Manager CDP subagent to read the Cisco Discovery Protocol MIB, CISCO-CDP-MIB. This MIB enables Cisco IME to advertise itself to other Cisco devices on the network.

The CDP subagent implements the CDP-MIB. The CDP-MIB contains the following objects:

- cdpInterfaceIfIndex
- cdpInterfaceMessageInterval
- cdpInterfaceEnable
- cdpInterfaceGroup
- cdpInterfacePort
- cdpGlobalRun
- cdpGlobalMessageInterval
- cdpGlobalHoldTime
- cdpGlobalLastChange
- cdpGobalDeviceId
- cdpGlobalDeviceIdFormat
- cdpGlobalDeviceIdFormatCpd

SYSAPPL-MIB

Use the System Application Agent to get information from the SYSAPPL-MIB, such as installed applications, application components, and processes that are running on the system.

System Application Agent supports the following object groups of SYSAPPL-MIB:

- sysApplInstallPkg
- sysApplRun
- sysApplMap
- sysApplInstallElmt
- sysApplElmtRun

MIB-II

Use MIB2 agent to get information from MIB-II. The MIB2 agent provides access to variables that are defined in RFC 1213, such as interfaces, IP, and so on, and supports the following groups of objects:

- system
- interfaces
- at
- ip
- icmp
- tcp
- udp
- snmp

HOST-RESOURCES MIB

Use Host Resources Agent to get values from HOST-RESOURCES-MIB. The Host Resources Agent provides SNMP access to host information, such as storage resources, process tables, device information, and installed software base. The Host Resources Agent supports the following groups of objects:

- hrSystem
- hrStorage
- hrDevice
- hrSWRun
- hrSWRunPerf
- hrSWInstalled

CISCO-SYSLOG-MIB

Syslog tracks and logs all system messages, from informational through critical. With this MIB, network management applications can receive syslog messages as SNMP traps:

The Cisco Syslog Agent supports trap functionality with the following MIB objects:

- clogNotificationsSent
- clogNotificationsEnabled
- clogMaxSeverity

- clogMsgIgnores
- clogMsgDrops

Vendor-Specific MIBs

The following MIBs exist on various Cisco MCS, depending on vendor and model number. To query these MIBS, you can use the standard MIB browsers that the hardware vendors develop; for example, HP Systems Insight Manager (SIM) and IBM Director Server+Console. For information on using the MIB browsers, refer to the documentation that the hardware vendor provides.

To review the vendor-specific MIB information, see the following tables:

- Table 9-10—Describes supported IBM MIBs
- Table 9-11—Describes supported HP MIBs

Table 9-10 IBM MIBs

MIB	OID	Description
Supported for browsing only		
IBM-SYSTEM-HEALTH-MIB	1.3.6.1.4.1.2.6.159.1.1.30	Provides temperature, voltage, and fan status
IBM-SYSTEM-ASSETID-MIB	1.3.6.1.4.1.2.6.159.1.1.60	Provides hardware component asset data
IBM-SYSTEM-LMSENSOR-MIB	1.3.6.1.4.1.2.6.159.1.1.80	Provides temperature, voltage, and fan details
IBM-SYSTEM-NETWORK-MIB	1.3.6.1.4.1.2.6.159.1.1.110	Provides Network Interface Card (NIC) status
IBM-SYSTEM-MEMORY-MIB	1.3.6.1.4.1.2.6.159.1.1.120	Provides physical memory details
IBM-SYSTEM-POWER-MIB	1.3.6.1.4.1.2.6.159.1.1.130	Provides power supply details
IBM-SYSTEM-PROCESSOR-MIB	1.3.6.1.4.1.2.6.159.1.1.140	Provides CPU asset/status data
Supported for system traps		
IBM-SYSTEM-TRAP	1.3.6.1.4.1.2.6.159.1.1.0	Provides temperature, voltage, fan, disk, NIC, memory, power supply, and CPU details
IBM-SYSTEM-RAID-MIB	1.3.6.1.4.1.2.6.167.2	Provides RAID status

Table 9-11 HP MIBs

MIB	OID	Description
Supported for browsing and system traps		
CPQSTDEQ-MIB	1.3.6.1.4.1.232.1	Provides hardware component configuration data
CPQSINFO-MIB	1.3.6.1.4.1.232.2	Provides hardware component asset data
CPQIDA-MIB	1.3.6.1.4.1.232.3	Provides RAID status/events
CPQHLTH-MIB	1.3.6.1.4.1.232.6	Provides hardware components status/events

Table 9-11 HP MIBs (continued)

MIB	OID	Description
CPQSTSYS-MIB	1.3.6.1.4.1.232.8	Provides storage (disk) systems status/events
CPQSM2-MIB	1.3.6.1.4.1.232.9	Provides iLO status/events
CPQTHRSH-MIB	1.3.6.1.4.1.232.10	Provides alarm threshold management
CPQHOST-MIB	1.3.6.1.4.1.232.11	Provides operating system information
CPQIDE-MIB	1.3.6.1.4.1.232.14	Provides IDE (CD-ROM) drive status/events
CPQNIC-MIB	1.3.6.1.4.1.232.18	Provides Network Interface Card (NIC) status/events

Related Topics

- SNMP Configuration Checklist, page 9-1
- SNMP Users, page 9-3
- SNMP Trap Notification Destinations, page 9-4
- SNMP Inform Notification Destination, page 9-5
- MIB2 System Group, page 9-7
- SNMP Management Information Base (MIB), page 9-8

CHAPTER 10

Troubleshooting

This section provides you will tools to help you to troubleshoot the Cisco Intercompany Media Engine server. For more information on troubleshooting the Cisco Intercompany Media Engine feature, refer to the following URL:

http://docwiki.cisco.com/wiki/Cisco_Intercompany_Media_Engine

This section contain the following topics:

- System History Log, page 10-1
- Audit Logging, page 10-4
- Netdump Utility, page 10-8

System History Log

This system history log provides a central location for getting a quick overview of the initial system install, system upgrades, Cisco option installations, and DRS backups and DRS restores, as well as switch version and reboot history.

This section contains the following topics:

- System History Log Overview, page 10-1
- System History Log Fields, page 10-2
- Accessing the System History Log, page 10-3

System History Log Overview

The system history log exists as a simple ASCII file, **system-history.log**, and the data does not get maintained in the database. Because it does not get excessively large, the system history file does not get rotated.

The system history log provides the following functions:

- Logs the initial software installation on a server.
- Logs the success, failure, or cancellation of every software upgrade (Cisco option files and patches).
- Logs every DRS backup and restore that is performed.
- Logs every invocation of Switch Version that is issued through either the CLI or the GUI.
- Logs every invocation of Restart and Shutdown that is issued through either the CLI or the GUI.

- Logs every boot of the system. If not correlated with a restart or shutdown entry, the boot is the result of a manual reboot, power cycle, or kernel panic.
- Maintains a single file that contains the system history, since initial installation or since feature availability.
- Exists in the install folder. You can access the log from the CLI by using the **file** commands or from the Real Time Monitoring Tool (RTMT).

System History Log Fields

The log displays a common header that contains information about the product name, product version, and kernel image; for example:

```
====================================
Product Name - Cisco Intercompany Media Engine
Product Version - 8.0.0.30671-1
Kernel Image - 2.6.9-78.EL
====================================
```

Each system history log entry contains the following fields:

timestamp userid action description start/result

The system history log fields can contain the following values:

- *timestamp*—Displays the local time and date on the server with the format *mm/dd/yyyy hh:mm:ss*.
- *userid*—Displays the user name of the user who invokes the action.
- *action*—Displays one of the following actions:
  - Install
  - Upgrade
  - Cisco Option Install
  - Switch Version
  - System Restart
  - Shutdown
  - Boot
  - DRS Backup
  - DRS Restore
- *description*—Displays one of the following messages:
  - *Version*: Displays for the Basic Install, and Upgrade actions.
  - *Cisco Option file name*: Displays for the Cisco Option Install action.
  - *Timestamp*: Displays for the DRS Backup and DRS Restore actions.
  - *Active version to inactive version*: Displays for the Switch Version action.
  - *Active version*: Displays for the System Restart, Shutdown, and Boot actions.

- *result*—Displays the following results:
  - Start
  - Success or Failure
  - Cancel

Example

Example 1 shows a sample of the system history log.

Example 1 System History Log

```
======================================
Product Name -    Cisco Intercompany Media Engine
Product Version - 8.0.0.30671-1
Kernel Image -    2.6.9-78.EL
======================================
08/28/2009 10:40:34 | root: Install 8.0.0.30671-1 Start
08/28/2009 10:58:03 | root: Boot 8.0.0.30671-1 Start
08/28/2009 11:02:47 | root: Install 8.0.0.30671-1 Success
08/28/2009 11:02:47 | root: Boot 8.0.0.30671-1 Start
08/28/2009 13:33:48 | root: Cisco Option Install ciscoime.proxy_commands.cop Start
08/28/2009 13:34:18 | root: Cisco Option Install ciscoime.proxy_commands.cop Success
09/07/2009 23:44:43 | root: Upgrade 8.0.0.30600-103 Start
09/07/2009 23:56:48 | root: Upgrade 8.0.0.30600-103 Success
09/07/2009 23:57:06 | root: Switch Version 8.0.0.30671-1 to 8.0.0.30600-103 Start
09/07/2009 23:57:52 | root: Switch Version 8.0.0.30671-1 to 8.0.0.30600-103 Success
09/07/2009 23:57:52 | root: Restart 8.0.0.30600-103 Start
09/08/2009 00:00:36 | root: Boot 8.0.0.30600-103 Start
09/17/2009 12:40:38 | root: Upgrade 8.0.0.96000-2 Start
09/17/2009 12:52:54 | root: Upgrade 8.0.0.96000-2 Success
09/17/2009 12:53:11 | root: Switch Version 8.0.0.30600-103 to 8.0.0.96000-2 Start
09/17/2009 12:53:55 | root: Switch Version 8.0.0.30600-103 to 8.0.0.96000-2 Success
09/17/2009 12:53:55 | root: Restart 8.0.0.96000-2 Start
09/17/2009 12:56:27 | root: Boot 8.0.0.96000-2 Start
09/17/2009 13:29:47 | root: Switch Version 8.0.0.96000-2 to 8.0.0.30600-103 Start
09/17/2009 13:30:34 | root: Switch Version 8.0.0.96000-2 to 8.0.0.30600-103 Success
09/17/2009 13:30:34 | root: Restart 8.0.0.30600-103 Start
09/17/2009 13:33:06 | root: Boot 8.0.0.30600-103 Start
09/17/2009 14:22:20 | root: Upgrade 8.0.0.30600-9003 Start
09/17/2009 14:33:30 | root: Upgrade 8.0.0.30600-9003 Success
09/17/2009 14:33:48 | root: Switch Version 8.0.0.30600-103 to 8.0.0.30600-9003 Start
09/17/2009 14:34:33 | root: Switch Version 8.0.0.30600-103 to 8.0.0.30600-9003 Success
09/17/2009 14:34:33 | root: Restart 8.0.0.30600-9003 Start
09/17/2009 14:37:03 | root: Boot 8.0.0.30600-9003 Start
```

Accessing the System History Log

You can use either the CLI or RTMT to access the system history log.

Using the CLI

You can access the system history log by using the CLI **file** command; for example:

- **file view install system-history.log**
- **file get install system-history.log**

For more information on the CLI **file** commands, see the *Cisco Intercompany Media Engine Command Line Interface Reference Guide*.

Using RTMT

You can also access the system history log by using RTMT. From the Trace and Log Central tab, choose **Collect Install Logs**.

For more information about using RTMT, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Audit Logging

Centralized audit logging ensures that configuration changes to the Cisco Intercompany Media Engine system gets logged in separate log files for auditing. An audit event represents any event that is required to be logged. The following Cisco Intercompany Media Engine system components generate audit events:

- Real Time Monitoring Tool
- Cisco Unified Communications Operating System
- Command Line Interface
- Remote Support Account Enabled (CLI commands issued by technical supports teams)

The following example displays a sample audit event:

```
10:39:28.787| UserID:Administrator  ClientAddress:10.194.109.32  Severity:6  EventType:
CLICommand  ResourceAccessed: GenericCLI  EventStatus: Success  CompulsoryEvent: No
AuditCategory: AdministrativeEvent  ComponentID: CLI  AuditDetails: CLI Command-> utils
ime license file install IME20091020095547801_node32.lic App ID:Command Line Cluster ID:
Node ID: node32
```

Audit logs, which contain information about audit events, get written in the common partition. The Log Partition Monitor (LPM) manages the purging of these audit logs as needed, similar to trace files. By default, the LPM purges the audit logs, but the audit user can change this setting from the Cisco Intercompany Media Engine command line interface (CLI). The LPM sends an alert whenever the common partition disk usage exceeds the threshold; however, the alert does not have the information about whether the disk is full because of audit logs or trace files.

Tip The Cisco Audit Event Service supports audit logging. If audit logs do not get written, then stop and start this service by using the CLI: utils service stop **Cisco Audit Event Service** and utils service start **Cisco Audit Event Service**.

All audit logs get collected, viewed and deleted from Trace and Log Central in the Real Time Monitoring Tool. Access the audit logs in RTMT in Trace and Log Central. Go to **System > Real-Time Trace > Audit Logs > Nodes**. After you select the node, another window displays System > Cisco Audit Logs.

The following types of audit logs display in RTMT:

- Application Log, page 10-4
- Operating System Log, page 10-5
- Remote Support Acct Enabled Log, page 10-5

Application Log

The application audit log, which displays in the AuditApp folder in RTMT, provides configuration changes for Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, the CLI, and Real Time Monitoring Tool (RTMT).

Although the Application Log stays enabled by default, you can disable audit logging by using the CLI **set auditlog status** command. If the audit logs get disabled, no new audit log files get created.

Cisco Unified Communications Manager creates one application audit log file until the configured maximum file size is reached; then, it closes and creates a new application audit log file. If the system specifies rotating the log files, Cisco Unified Communications Manager saves the configured number of files. Some of the logging events can be viewed by using RTMT SyslogViewer.

The following events get logged for Cisco Unified Serviceability:

- Activation, deactivation, start, or stop of a service from any Serviceability window.
- Changes in trace configurations and alarm configurations.
- Changes in SNMP configurations.

RTMT logs the following events with an audit event alarm:

- Alert configuration.
- Alert suspension.
- E-mail configuration.
- Set node alert status.
- Alert addition.
- Add alert action.
- Clear alert.
- Enable alert.
- Remove alert action.
- Remove alert.

Note Audit log logs a CLI command successfully, even when the command is not allowed to run. For example, the following operation is permitted only on a bootstrap server:

```
admin:set ime dht global storagequota 1
```

When the above command is run on other servers, Audit log logs the CLI command with status=Success, even though the user would have received the message, "This command is only allowed to be run on a bootstrap server."

Operating System Log

The operating system audit log, which displays in the vos folder in RTMT, reports events that are triggered by the operating system. It does not get enabled by default. The **utils auditd** CLI command enables, disables, or gives status about the events.

The vos folder does not display in RTMT unless the audit is enabled in the CLI.

Remote Support Acct Enabled Log

The Remote Support Acct Enabled audit log, which displays in the vos folder in RTMT, reports CLI commands that get issued by technical support teams. You cannot configure it, and the log gets created only if the Remote Support Acct gets enabled by the technical support team.

Configuring Audit Logging

Table 10-1 shows the commands that you need to work with SNMP users on the Cisco Intercompany Media Engine server:

Table 10-1 Audit Logging Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Enable the operating system audit log. You can retrieve audit log files for the system through RTMT. **Tip** To determine the status of the operating system audit log, enter the **utils auditd status** CLI command.	utils auditd *status* where, *status* equals enable or disable
Step 2	Enable audit logging. You can retrieve audit log files for the system through RTMT. **Tip** To determine the status of audit logging, enter the **show auditlog** CLI command.	set auditlog status The system prompts you to enter the *status* parameter where, *status* equals enable or disable
Step 3	Set purging status. The Log Partition Monitor (LPM) looks at the Enable Purging option to determine whether it needs to purge audit logs. When you enable purging, LPM purges all the audit log files in RTMT whenever the common partition disk usage goes above the high water mark; however, you can disable purging by unchecking the check box. If purging is disabled, the number of audit logs continues to increase until the disk is full. This action could cause a disruption of the system. Be aware that this purging option is available for audit logs in an active partition. If the audit logs reside in an inactive partition, the audit logs get purged when the disk usage goes above the high water mark. You can access the audit logs by choosing **Trace and Log Central > Audit Logs** in RTMT.	set auditlog purging The system prompts you to enter the *status* parameter where, *status* equals enable or disable
Step 4	Set log rotation status. The system reads this option to determine whether it needs to rotate the audit log files or it needs to continue to create new files. The maximum number of files cannot exceed 5000. When the Enable Rotation option is enabled, the system begins to overwrite the oldest audit log files after the maximum number of files gets reached. **Tip** When log rotation is disabled, audit log ignores the Maximum No. of Files setting.	set auditlogrotation The system prompts you to enter the *status* parameter where, *status* equals enable or disable

Table 10-1 Audit Logging Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 5	Set maximum number of files. Enter the maximum number of files that you want to include in the log. Ensure that the value that you enter for the Maximum No. of Files setting is greater than the value that you enter for the No. of Files Deleted on Log Rotation setting.	set auditlog maxfilesize The system prompts you to enter the *size* parameter where, *size* equals 1 to 10
Step 6	Set maximum file size.	set auditlog maxnumfiles The system prompts you to enter the *filecount* parameter where, *filecount* equals 1 to 10000
Step 7	Set the auditlog remote syslog severity level.	set auditlog remotesyslogseverity The system prompts you to enter the *severity* parameter where, *severity* equals one of the following: Emergency, Alert, Critical, Error, Warning, Notice, Informational, or Debug
Step 8	Enter the remote syslog server name.	set auditlog remotesyslogserver The system prompts you to enter the *servername* parameter where, *servername* equals a valid hostname of a remote syslog server

Netdump Utility

The netdump utility allows you to send data and memory crash dump logs from one server on the network to another. Servers that are configured as netdump clients send the crash logs to the server that is configured as the netdump server. The log file gets sent to the crash directory of the netdump server.

In a Cisco Unified Communications Manager cluster, you must configure at least two nodes as netdump servers, so the first node and subsequent nodes can send crash dump logs to each other.

For example, if your cluster contains three servers (one primary/first node and two subsequent nodes), you can configure the first node and subsequent node #1 as the netdump servers. Then, you can configure the first node as a netdump client of the subsequent node #1 and configure all of the subsequent nodes as netdump clients of the first node. If the first node crashes, it sends the netdump to subsequent node #1. If any subsequent node crashes, it sends the netdump to the first node.

You can use an external netdump server rather than configuring a Cisco Unified Communications Manager server as a netdump server. For information on configuring an external netdump server, contact TAC.

Note Cisco recommends that you configure the netdump utility after you install Cisco Unified Communications Manager to assist in troubleshooting. If you have not already done so, configure the netdump utility before you upgrade Cisco Unified Communications Manager from supported appliance releases.

To configure the netdump servers and clients, use the command line interface (CLI) that is available for the Cisco Unified Communications Operating System as described in the following sections:

- Configuring a Netdump Server, page 10-8
- Configuring a Netdump Client, page 10-9
- Working with Files That Are Collected by the Netdump Server, page 10-9
- Monitoring Netdump Status, page 10-9

Configuring a Netdump Server

To configure a node as a netdump server, use the following procedure:

Procedure

Step 1 On the node that you want to configure as the netdump server, start a CLI session as described in the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Step 2 Execute the **utils netdump server start** command.

Step 3 To view the status of the netdump server, execute the **utils netdump server status** command.

Step 4 Configure the netdump clients, as described in the "Configuring a Netdump Client" section on page 10-9.

Configuring a Netdump Client

To configure a node as a netdump client, use the following procedure:

Procedure

Step 1 On the node that you want to configure as the netdump client, start a CLI session as described in the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Step 2 Execute the **utils netdump client start** *ip-address-of-netdump-server* command.

Step 3 Execute the **utils netdump server add-client** *ip-address-of-netdump-client*. Repeat this command for each node that you want to configure as a netdump client.

Note Make sure that you enter the correct IP addresses. The CLI does not validate the IP addresses.

Step 4 To view the status of the netdump client, execute the **utils netdump client status** command.

Working with Files That Are Collected by the Netdump Server

To view the crash information from the netdump server, use the Real Time Monitoring Tool or the command line interface (CLI). To collect the netdump logs by using the Real Time Monitoring Tool, choose the Collect Files option from Trace & Log Central. From the Select System Services/Applications tab, choose the Netdump logs check box. For more information on collecting files using Real Time Monitoring Tool, see the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

To use the CLI to collect the netdump logs, use the "file" CLI commands on the files in the crash directory. The log filenames begin with the IP address of the netdump client and end with the date that the file gets created. For information on the file commands, refer to the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Monitoring Netdump Status

You can monitor the netdump status by configuring SyslogSearchStringFound alerts in Real Time Monitoring Tool. Use the following procedure to configure the appropriate alerts:

Procedure

Step 1 From the quick launch channel in Real Time Monitoring Tool, choose **Tools > Alert Central**.

Step 2 Right-click the SyslogStringMatchFound alert and choose **Set Alert/Properties**.

Step 3 Click **Next** three times.

Step 4 In the SysLog Alert window, click the **Add** button. When the Add Search String dialog box displays, enter **netdump: failed** and click **Add**. Then, click **Next**.

Note Make sure that the case and syntax matches exactly.

Step 5 In the Email Notification window, choose the appropriate trigger alert action, enter any user-defined email text, and click **Save**.

CHAPTER 11

Cisco Intercompany Media Engine Performance Objects and Counters

This section provides information on Cisco Intercompany Media Engine objects and counters. Both the Cisco Unified Communications Manager server and the Cisco Intercompany Media Engine server contain a unique set of objects and counters. You may need counters from both servers to monitor the performance of the Cisco Intercompany Media Engine product.

To access performance objects and counters, log in to RTMT on the appropriate server, and choose **System > Performance > Open Performance Monitoring**. For more information on working with performance counters and objects, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

This section contains the following information:

Cisco Intercompany Media Engine Server Objects

- IME Configuration Manager, page 11-2
- IME Server, page 11-2
- IME Server System Performance, page 11-4

Cisco Unified Communications Manager Server Objects

- IME Client, page 11-5
- IME Client Instance, page 11-7

Additional Information

Related Topics, page 11-7

IME Configuration Manager

The IME Configuration Manager object provides information about the IME distributed cache certificate. Table 11-1 contains information on the Cisco IME configuration counters.

Table 11-1 IME Configuration Manager

Counters	Counter Description
DaysUntilCertExpiry	This counter indicates the number of days that remain until the IME distributed cache certificate expires. You must replace the certificate before it expires. When the value of this counter falls below 14, an alert gets generated once every day until the value exceeds 14.

IME Server

The IME Server object provides information about the Cisco IME server. Table 11-2 contains information on the Cisco IME Server counters.

Table 11-2 IME Server

Counters	Counter Description
BlockedValidationOrigTLSLimit	This counter indicates the total number of blocked validations that occurred because the TLSValidationThreshold was reached.
BlockedValidationTermTLSLimit	This counter indicates the total number of blocked validations that occurred because the TLSValidationThreshold was reached.
ClientsRegistered	This counter indicates the number of Cisco IME clients that are currently connected to the Cisco IME server.
IMEDistributedCacheHealth	The counter indicates the health of the IME distributed cache. The following values may display: • 0 (red)—Warns that the IME distributed cache is not functioning properly; for example, the Cisco IME cannot resolve issues after the network has been partitioned In this case, validation attempts might fail. For example, the Cisco IME service is not connected to the network and is unable to reach the bootstrap servers. An alert gets generated once every hour until the value changes from red status. • 1 (yellow)—Indicates that the Cisco IME network is experiencing minor issues, such as connectivity between bootstrap servers or other Cisco IME network issues. (Check the Cisco IME alarms to determine network issues.) • 2 (green)—Indicates that the Cisco IME is functioning normally and is considered healthy.

Table 11-2 IME Server (continued)

Counters	Counter Description
IMEDistributedCacheNodeCount	The counter is an integer that indicates an approximation of the total number of nodes in the IME distributed cache. Since each physical Cisco IME server hosts multiple nodes, this counter does not directly indicate the number of physical Cisco IME servers that participate in the IME distributed cache. This counter can provide an indication of the health of the IME distributed cache; for example, a problem may exist with the IME distributed cache if an expected value displays on one day (for example, 300), but then on the next day, the value drops dramatically (for example, to 10 or 2).
IMEDistributedCacheQuota	Indicates the number of individual DIDs that can be written into the IME Distributed Cache, by Cisco Unified CMs attached to this IME server. This number is determined by the overall configuration of the IME Distributed Cache, and the IME license installed on the IME server.
IMEDistributedCacheQuotaUsed	Indicates the total number of unique DID numbers that have been configured, to be published via enrolled patterns for Intercompany Media Services, by Cisco Unified CMs currently attached to this IME server.
IMEDistributedCacheReads	This counter indicates the total number of reads that the Cisco IME server has attempted into the IME distributed cache. This number serves as an indicator of whether the Cisco IME server is functional; that is, whether the server is interacting with other nodes.
IMEDistributedCacheStoredData	This counter indicates the amount of IME distributed cache storage, measured in bytes, that this Cisco IME server provides.
IMEDistributedCacheStores	This counter indicates the total number of stores (published numbers) that the Cisco IME server has attempted into the IME distributed cache. This number serves as an indicator of whether the Cisco IME server is functional.
InternetBandwidthRecv	This counter measures the amount of downlink Internet bandwidth, in Kbits/s, that the Cisco IME server is consuming.
InternetBandwidthSend	This counter measures the amount of uplink Internet bandwidth that the Cisco IME server in Kbits/s is consuming.
TerminatingVCRs	This counter indicates the total Cisco IME voice call records (VCRs) that are stored on the Cisco IME server after receiving calls. You can use these records for validating learned routes.
ValidationAttempts	This counter indicates the total number of attempts that the Cisco IME server has made at performing a validation because the dialed number was found in the Cisco IME network. This counter provides an overall indication of system usage.
ValidationsAwaitingConfirmation	This counter indicates the total number of destination phone numbers that have been validated, but that are awaiting further calls to improve the security of the system. If you use a higher level of security for learning new routes, the Cisco IME server requires multiple successful validations for a route before that route is available for calls over IP. This counter tracks the number of successful validations that have not resulted in available IP routes.

Table 11-2 IME Server (continued)

Counters	Counter Description
ValidationsPending	This counter, which is an integer, indicates the number of scheduled validation attempts to retrieve a learned route. This value indicates the backlog of work for the Cisco IME service on the Cisco IME server. An alert gets generated when the value rises either above the high watermark or falls below the low watermark. After the high watermark is reached, an alert gets sent immediately and then once an hour until the value falls below the high watermark. When the high watermark is reached, the Cisco IME service cannot clear the backlog of work prior to the expiration of data; this situation causes records to drop, and validation may not occur. To reduce the workload, add more Cisco IME servers that can share the workload.
ValidationsBlocked	This counter indicates the number of times that the Cisco IME service rejected a validation attempt because the calling party was not trusted; that is, the party was on a blacklist or not on a whitelist. This value provides an indication of the number of cases where a VoIP calls cannot happen in the future because of the blocked validation.

IME Server System Performance

The Cisco IME System Performance object provides information about performance on the Cisco IME server. Table 11-3 contains information on the Cisco IME server system performance counters.

Table 11-3 IME Server System Performance

Counters	Counter Description
QueueSignalsPresent 1-High	This counter indicates the number of high-priority signals in the queue on the Cisco IME server. High-priority signals include timeout events, internal KeepAlive messages, internal process creation, and so on. A large number of high-priority events causes degraded performance of the Cisco IME service and results in slower or failed validations. Use this counter in conjunction with the QueueSignalsProcessed 1-High counter to determine the processing delay on the Cisco IME server.
QueueSignalsPresent 2-Normal	This counter indicates the number of normal-priority signals in the queue on the Cisco IME server. Normal-priority signals include call validations, IME distributed cache operations such as stores and reads, and so on. A large number of normal-priority events causes degraded performance of the Cisco IME service and may result in slower or failed validations or disruption to IME distributed cache connectivity. Use this counter in conjunction with the QueueSignalsProcessed 2-Normal counter to determine the processing delay on the Cisco IME server. Since high-priority signal must complete before normal priority signals begin to process, check the high-priority counters to accurately understand why a delay occurs.

Table 11-3 IME Server System Performance (continued)

Counters	Counter Description
QueueSignalsPresent 3-Low	This counter indicates the number of low-priority signals in the queue on the Cisco IME server. Low-priority signals include IME distributed cache signaling and other events. A large number of signals in this queue may disrupt IME distributed cache connectivity or other events.
QueueSignalsPresent 4-Lowest	This counter indicates the number of lowest-priority signals in the queue on the Cisco IME server. A large number of signals in this queue may disrupt IME distributed cache connectivity and other events.
QueueSignalsProcessed 1-High	This counter indicates the number of high-priority signals that the Cisco IME service processes for each one-second interval. Use this counter in conjunction with the QueueSignalsPresent 1-High counter to determine the processing delay for this queue.
QueueSignalsProcessed 2-Normal	This counter indicates the number of normal-priority signals that the Cisco IME service processes for each one-second interval. Use this counter in conjunction with the QueueSignalsPresent 1-High counter to determine the processing delay for this queue. High-priority signals are processed before normal-priority signals.
QueueSignalsProcessed 3-Low	This counter indicates the number of low-priority signals that the Cisco IME service processes for each one-second interval. Use this counter in conjunction with the QueueSignalsPresent 3-Low counter to determine the processing delay for this queue.
QueueSignalsProcessed 4-Lowest	This counter indicates the number of lowest-priority signals that the Cisco IME service processes for each one-second interval. Use this counter in conjunction with the QueueSignalsPresent 4-Lowest counter to determine the processing delay for this queue.
QueueSignalsProcessed Total	This counter provides a total of all queue signals that the Cisco IME service processes for each one-second period for all queue levels: high, normal, low, and lowest.

IME Client

The IME Client object provides information about the Cisco IME client on the Cisco Unified Communications Manager server. Table 11-4 contains information on the Cisco IME client counters.

Table 11-4 Cisco IME Client

Counters	Counter Description
CallsAccepted	This counter indicates the number of Cisco IME calls that the Cisco Unified Communications Manager received successfully and that the called party answered, resulting in an IP call.
CallsAttempted	This counter indicates the number of calls that the Cisco Unified Communications Manager received through Cisco IME. This number includes accepted calls, failed calls, and busy, no-answer calls. The counter increments each time that Cisco Unified Communications Manager receives a call through Cisco IME.

Table 11-4 Cisco IME Client (continued)

Counters	Counter Description
CallsReceived	This counter indicates the number of calls that Cisco Unified Communications Manager receives through Cisco IME. This number includes accepted calls, failed calls, and busy, no-answer calls. The counter increments on call initiation.
CallsSetup	This counter indicates the number of Cisco IME calls that Cisco Unified Communications Manager placed successfully and that the remote party answered, resulting in an IP call.
DomainsUnique	This counter indicates the number of unique domain names of peer enterprises that the Cisco IME client discovered. The counter serves as an indicator of overall system usage.
FallbackCallsFailed	This counter indicates the total number of failed fallback attempts.
FallbackCallsSuccessful	This counter indicates the total number of Cisco IME calls that have fallen back to the PSTN mid-call due to a quality problem. The counter includes calls initiated and calls received by this Cisco Unified Communications Manager.
IMESetupsFailed	This counter indicates the total number of call attempts for which a Cisco IME route was available but that were set up through the PSTN due to a failure to connect to the target over the IP network.
RoutesLearned	This counter indicates the total number of distinct phone numbers that the Cisco IME has learned and that are present as routes in the Cisco Unified Communications Manager routing tables. If this number grows too large, the server may exceed the per-cluster limit, and you may need to add additional servers to your cluster.
RoutesPublished	This counter indicates the total number of DIDs that were published successfully into the IME distributed cache across all Cisco IME client instances. The counter provides a dynamic measurement that gives you an indication of your own provisioned usage and a sense of how successful the system has been in storing the DIDs in the network.
RoutesRejected	This counter indicates the number of learned routes that were rejected because the the administrator blacklisted the number or domain. This counter provides an indication of the number of cases where a VoIP call cannot happen in the future because of the blocked validation.
VCRUploadRequests	This counter indicates the number of voice call record (VCR) upload requests that the Cisco Unified Communications Manager has sent to the Cisco IME server to be stored in the IME distributed cache.

IME Client Instance

The IME Client Instance object provides information about the Cisco IME client instance on the Cisco Unified Communications Manager server. Table 11-1 contains information on the Cisco IME client instance counters.

Table 11-5 IME Client

Counters	Counter Description
IMEServiceStatus	This counter indicates the overall health of the connection to the Cisco IME services for a particular Cisco IME client instance (Cisco Unified Communications Manager). The following values may display for the counter: • 0—Indicates an unknown state (which may mean that the Cisco IME service is not active). If the value specifies 0, an alert gets generated once per hour while the connection remains in the unknown state. • 1—Indicates a healthy state; that is, the Cisco IME service is active, and the Cisco Unified Communications Manager has successfully established a connection to its primary and backup servers for the Cisco IME client instance, if configured. • 2—Indicates an unhealthy state; that is, the Cisco IME service is active, but the Cisco Unified Communications Manager has not successfully established a connection to its primary and backup servers for the Cisco IME client instance, if configured.

Related Topics

- Cisco IME Configuration in Cisco Unified Communications Manager Administration, page 3-1
- Using RTMT with Cisco Intercompany Media Engine, page 7-1
- *Cisco Unified Real-Time Monitoring Tool Administration Guide*

CHAPTER 12

Cisco Intercompany Media Engine Alert Descriptions and Default Settings

This section provides information on Cisco Intercompany Media Engine alerts. Both the Cisco Unified Communications Manager server and the Cisco Intercompany Media Engine server generate a unique set of alerts when predefined conditions are met. You need to monitor alerts from both servers to determine the status of the Cisco Intercompany Media Engine product.

To access alerts, login to RTMT on the appropriate server, and choose **System > Tools > Alert > Alert Central**. For more information on working with alerts, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

The following list comprises the Cisco Intercompany Media Engine alerts, their definitions, and default settings:

Cisco Intercompany Media Engine Server Alerts

- BannedFromNetwork, page 12-2
- IMEDistributedCacheCertificateExpiring, page 12-2
- IMEDistributedCacheFailure, page 12-3
- IMESdlLinkOutOfService, page 12-4
- InvalidCertificate, page 12-5
- InvalidCredentials, page 12-5
- MessageOfTheDay, page 12-6
- SWUpdateRequired, page 12-6
- TicketPasswordChanged, page 12-7
- ValidationsPendingExceeded, page 12-8

Cisco Unified Communications Manager Server Alerts

- IMEDistributedCacheInactive, page 12-9
- IMEOverQuota, page 12-9
- IMEQualityAlert, page 12-10
- InsufficientFallbackIdentifiers, page 12-11
- IMEServiceStatus, page 12-12
- InvalidCredentials, page 12-13

- TCPSetupToIMEFailed, page 12-13
- TLSConnectionToIMEFailed, page 12-14

Additional Information

Related Topics, page 12-15

BannedFromNetwork

This alert indicates that network administrators have banned this Cisco IME server from the network (IME distributed cache ring), making this Cisco IME service fully or partly inoperative. Network administrators rarely ban servers but do so if they detect that the server is being used to launch malicious attacks into the network. If you receive this alert in error, contact TAC immediately.

Default Configuration

Table 12-1 Default Configuration for the BannedFromNetwork Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Cisco IME service banned from network
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEDistributedCacheCertificateExpiring

This alert indicates the number of days that remain until the certificate that is used for the IME distributed cache expires. You must replace the certificate prior to expiration.

Default Configuration

Table 12-2 Default Configuration for the IMEDistributedCacheCertificateExpiring Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning

Table 12-2 Default Configuration for the IMEDistributedCacheCertificateExpiring Alert

Value	Default Configuration
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Cisco IME distributed cache certificate about to expire. 14 days.
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alerts within 1440 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEDistributedCacheFailure

This alert indicates the health of the IME distributed cache. A value of zero (red) means that the IME distributed cache is suffering from a significant problem such as one of the following conditions:

- The Cisco IME cannot resolve issues after the network was partitioned. In this case, validation attempts may fail.
- The Cisco IME service is not connected to the network at all and is unable to reach the bootstrap servers.

A value of one (yellow) indicates that the Cisco IME network is experiencing minor issues, such as connectivity between bootstrap servers or other Cisco IME network issues. Check for any alarms that may indicate why this counter is 1. A value of two indicates that IME distributed cache is functioning normally and the system is considered healthy.

Default Configuration

Table 12-3 Default Configuration for the IMEDistributedCacheFailure Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: IME distributed cache failure in states 1: network experience minor issues 0: network in trouble
Duration	Trigger alert immediately
Frequency	Trigger 1 alert within 60 minutes

Table 12-3 Default Configuration for the IMEDistributedCacheFailure Alert (continued)

Value	Default Configuration
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMESdlLinkOutOfService

This alert indicates that the Cisco IME service has lost communication with Cisco IME Config Manager services, such as Cisco AMC service or Cisco CallManager service.

This alert usually indicates that one of these services has gone down (either intentionally, for maintenance; or unintentionally, due to a service failure or connectivity failure).

Default Configuration

Table 12-4 Default Configuration for the IMESdlLinkOutOfService Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SDLLinkOOS event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

InvalidCertificate

This alert indicates that the administrator enabled the IME distributed cache on the Cisco IME server but omitted the configuration of a valid certificate or configured an incorrect certificate.

Default Configuration

Table 12-5 Default Configuration for the InvalidCertificate Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Invalid certificate configured
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

InvalidCredentials

The alert indicates that the Cisco Unified Communications Manager cannot connect to the Cisco IME server, because the username and password that are configured on Cisco Unified Communications Manager do not match those configured on the Cisco IME server.

The alert includes the username and password that were used to connect to the Cisco IME server as well as the IP address and name of the target Cisco IME server. To resolve this alert, log into the Cisco IME server and check that the username and password that are configured match those configured in Cisco Unified Communications Manager.

Default Configuration

Table 12-6 Default Configuration for the InvalidCredentials Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Invalid or mismatched credentials.

Table 12-6 Default Configuration for the InvalidCredentials Alert (continued)

Value	Default Configuration
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

MessageOfTheDay

The Cisco IME service generates this alert when the administrators of the Cisco IME network have a message for you.

Default Configuration

Table 12-7 Default Configuration for the MessageOfTheDay Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Notice
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Message from network administrators
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 1440 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SWUpdateRequired

The Cisco IME server generates this alert when a new version of the Cisco IME server software is required. This alert repeats until you perform the upgrade. To obtain more information about the software update, go to the Cisco website. You should install critical updates within days of receiving this alert.

These upgrades address security vulnerabilities or key functional outages. In some cases, if you do not apply a critical upgrade immediately, the Cisco IME server may become unable to connect to the network.

Default Configuration

Table 12-8 Default Configuration for the SWUpdateRequired Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Software update required
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alerts within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

TicketPasswordChanged

The Cisco IME server generates this alert when the administrator changes the password that is used to generate the validation tickets.

Verify that an authorized administrator changed the password. Unauthorized changes may indicate compromise to the administrative interfaces on the Cisco IME service. If you determine that unauthorized changes have been made, change the administrative passwords on the Cisco IME server immediately to prevent further unauthorized access. To change the administrative password, type **set password admin** in the Cisco IME server CLI.

Default Configuration

Table 12-9 Default Configuration for the TicketPasswordChanged Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Notice
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Ticket password changed
Duration	Trigger alert immediately
Frequency	Trigger on every poll
Schedule	24 hours daily

Table 12-9 Default Configuration for the TicketPasswordChanged Alert (continued)

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

ValidationsPendingExceeded

This alert indicates the number of pending validations on the Cisco IME server. This number provides an indicator of the backlog of work on the Cisco IME server.

Default Configuration

Table 12-10 Default Configuration for the ValidationsPendingExceeded Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Cisco IME pending validations exceeded 100
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alerts within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEDistributedCacheInactive

This alarm gets generated when a Cisco Unified Communications Manager attempts to connect to the Cisco IME server, but the IME distributed cache is not currently active.

Ensure that the certificate for the Cisco IME server is provisioned and that the IME distributed cache has been activated via the CLI.

Default Configuration

Table 12-11 Default Configuration for the IMEDistributedCacheInactive Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Inactive IME Distributed Cache
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEOverQuota

This alert indicates that the Cisco Unified Communications Manager servers that use this Cisco IME service have exceed the quota for published direct inward dialing numbers (DIDs) to the IME distributed cache. The alert includes the name of the Cisco IME server as well as the current and target quota values.

Ensure that you have correctly provisioned the DID prefixes on all of the Cisco Unified Communications Manager servers that use this Cisco IME service.

If you have provisioned the prefixes correctly, you have exceeded the capacity of your Cisco IME service, and you need to configure another service and divide the DID prefixes across the Cisco IME client instances (Cisco Unified Communications Managers) on different Cisco IME services.

Default Configuration

Table 12-12 Default Configuration for the IMEOverQuota Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers

Table 12-12 Default Configuration for the IMEOverQuota Alert (continued)

Value	Default Configuration
Threshold	Trigger alert when following condition met: VAP over quota
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEQualityAlert

This alert gets generated when Cisco Unified Communications Manager determines that a substantial number of Cisco IME calls fail back to PSTN or fail to be set up due to IP network quality problems. Two types of events trigger this alert:

- A large number of the currently active Cisco IME calls have all requested fallback or have fallen back to the PSTN.
- A large number of the recent call attempts have gone to the PSTN and not been made over IP.

When you receive this alert, check your IP connectivity. If no problems exist with the IP connectivity, you may need to review the CDRs, CMRs, and logs from the firewalls to determine why calls have fallen back to the PSTN or have not been made over IP.

Default Configuration

Table 12-13 Default Configuration for the IMEQualityAlert Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Cisco IME link quality problem
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

InsufficientFallbackIdentifiers

This alert gets generated when too many Cisco IME calls that are currently in progress use the same fallback DID and no more DTMF digit sequences exist to allocate to a new Cisco IME call that Cisco Unified Communications Manager is processing. The new call continues, but the call cannot fallback to the PSTN if voice-quality deteriorates.

If this alert gets generated, note the fallback profile that associates with this call. Check that profile in Cisco Unified Communications Manager Administration, and examine the current setting for the "Fallback Number of Correlation DTMF Digits" field. Increase the value of that field by one, and check whether the new value eliminates these alerts. In general, this parameter should be large enough so that the number of simultaneous Cisco IME calls that are made to enrolled numbers that associate with that profile is always substantially less than 10 raised to the power of this number. For example, if you always have fewer than 10,000 simultaneous Cisco IME calls for the patterns that associate with this fallback profile, setting this value to 5 (10 to the power of 5 equals 100,000) should keep Cisco Unified Communications Manager from generating this alert.

However, increasing this value results in a small increase in the amount of time it takes to perform the fallback. As such, you should set the "Fallback Number of Correlation DTMF Digits" field to a value just large enough to prevent this alert from getting generated.

Instead of increasing the value of the DTMF digits field, you can add another fallback profile with a different fallback DID and associate that fallback profile with a smaller number of enrolled patterns. If you use this method, you can use a smaller number of digits.

Default Configuration

Table 12-14 Default Configuration for the InsufficientFallbackIdentifiers Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Cannot allocate fallback identifier
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alerts within one minute
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEServiceStatus

This alert indicates the overall health of the connection to the Cisco IME services for a particular Cisco IME client instance (Cisco Unified Communications Manager). The alert indicates the following states:

- 0—Unknown. Likely indicates that the Cisco IME service has not been activated.
- 1—Healthy. Indicates that the Cisco Unified Communications Manager has successfully established a connection to its primary and backup servers for the Cisco IME client instance, if configured.
- 2—Unhealthy. Indicates that the Cisco IME has been activated but has not successfully completed handshake procedures with the Cisco IME server. Note that this counter reflects the handshake status of both the primary and the secondary IME servers.

Default Configuration

Table 12-15 Default Configuration for the IMEServiceStatus Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: VAP Connection Problem
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert every 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

InvalidCredentials

The alert indicates that the Cisco Unified Communications Manager cannot connect to the Cisco IME server because the username and/or password configured on Cisco Unified Communications Manager do not match those configured on the Cisco IME server.

The alert includes the username and password that were used to connect to the Cisco IME server as well as the IP address and name of the target Cisco IME server. To resolve this alert, log into the Cisco IME server and check that the configured username and password match the username and password that are configured in Cisco Unified Communications Manager.

Default Configuration

Table 12-16 Default Configuration for the InvalidCredentials Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Credential Failure to Cisco IME server
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

TCPSetupToIMEFailed

This alert occurs when Cisco Unified Communications Manager cannot establish a TCP connection to a Cisco IME server. This alert typically occurs when the IP address and port of the Cisco IME server are misconfigured in Cisco Unified Communications Manager Administration or when an Intranet connectivity problem exists and prevents the connection from being set up.

Ensure that the IP address and port of the Cisco IME server in the alert are valid. If the problem persists, test the connectivity between the Cisco Unified Communications Manager servers and the Cisco IME server.

Default Configuration

Table 12-17 Default Configuration for the TCPSetupToIMEFailed Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical

Table 12-17 Default Configuration for the TCPSetupToIMEFailed Alert (continued)

Value	Default Configuration
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Connection Failure to Cisco IME server
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

TLSConnectionToIMEFailed

This alert occurs when a TLS connection to the Cisco IME service could not be established because the certificate presented by the Cisco IME service has expired or is not in the Cisco Unified Communications Manager CTL.

Ensure that the Cisco IME service certificate has been configured into the Cisco Unified Communications Manager.

Default Configuration

Table 12-18 Default Configuration for the TLSConnectionToIMEFailed Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: TLS Failure to Cisco IME service
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

Related Topics

- Cisco IME Configuration in Cisco Unified Communications Manager Administration, page 3-1
- Using RTMT with Cisco Intercompany Media Engine, page 7-1
- *Cisco Unified Real Time Monitoring Tool Administration Guide*

INDEX

A

alerts, Cisco IME 12-1
audit logging 10-4

C

certificates, Cisco IME
  manually renewing 2-24
  purchasing and enrolling 2-22
Cisco AMC Service 6-2
Cisco CDP Agent service 6-4
Cisco-CDP-MIB 9-8
Cisco CDP service 6-3
Cisco Certificate Expiry Monitor service 6-4
Cisco DRF Local 6-3
Cisco DRF Master 6-2
Cisco IME Client Call Activity Report 8-1
Cisco Intercompany Media Engine
  components 1-6
  configuration 3-1
  configuration checklist 3-6
  features and benefits 1-1
  how it works 1-2
  overview 1-1
Cisco Intercompany Media Engine feature parameters 3-37
Cisco Intercompany Media Engine server
  associating with Cisco IME services 3-26
  registration status 3-41
  verifying connectivity 3-40
Cisco Intercompany Media Engine service
  configuring 3-26
Cisco Log Partition Monitoring Tool service 6-2
Cisco RIS Data Collector service 6-2
Cisco Syslog Agent service 6-4
CISCO-SYSLOG-MIB 9-9
Cisco Tomcat service 6-3
Cisco Trace Collection Service 6-3
Cisco Trace Collection Servlet 6-3
connectivity between Cisco IME and Unified CM 3-40

D

deployment models 1-8
DID publication 3-42

E

enrolled groups
  associating with Cisco IME services 3-26
  associating with enrolled patterns 3-21
  configuring 3-19
enrolled patterns
  configuring 3-21
exclusion groups
  associating with Cisco IME services 3-26
  associating with exclusion numbers 3-23
  configuring 3-22
exclusion numbers
  configuring 3-23

F

fallback
  configuring feature parameters 3-47
  configuring profiles 3-43

feature parameters
configuring Cisco Intercompany Media Engine 3-37
configuring fallback 3-47
firewall information, configuring 3-49

H

history log
See system history log
Host Resources Agent service 6-4
HOST-RESOURCES MIB 9-9

I

IME Client
perfmon object and counters 11-5
IME Client Instance
perfmon object and counters 11-7
IME Configuration Manager
perfmon object and counters 11-2
IME Server
perfmon object and counters 11-2
IME Server System Performance
perfmon object and counters 11-4
IME Service predefined objects 7-7
IME System Performance 7-8
inform notification destination 9-5
informs
configuration settings 9-5, 9-6
installing Cisco IME
FAQ 2-2
important considerations 2-1
overview 2-1
post-installation tasks 2-17
pre-installation tasks 2-5
starting 2-13
Intercompany Media Services predefined object 7-6
IP address, configuring external address and port 3-28

L

learned routes
working with 3-49
license files
obtaining Cisco IME 2-8
uploading to Cisco IME server 2-22

M

Management Information Base (MIB)
Cisco-CDP-MIB 9-8
CISCO-SYSLOG-MIB 9-9
HOST-RESOURCES MIB 9-9
MIB-II 9-9
overview 9-8
SYSAPPL-MIB 9-9
MIB2 Agent service 6-4
MIB2 system group 9-7
MIB-II 9-9

N

netdump utility
configuring 10-8
configuring netdump clients 10-9
configuring netdump servers 10-8
monitoring status 10-9
working with collected files 10-9
Network Agent Adaptor service 6-4
network services
Control Center 6-1
overview 6-1
starting 6-1
stopping 6-1
viewing status 6-1
notification destination (V3)
configuration settings 9-5, 9-6

O

off-path deployment 1-9
overview
  network services 6-1

P

parameters
  configuring Cisco Intercompany Media Engine 3-37
  configuring fallback 3-47
passwords, resetting 2-25
perfmon
  object and counters
    IME Client 11-5
    IME Client Instance 11-7
    IME Configuration Manager 11-2
    IME Server 11-2
    IME Server System Performance 11-4
performance monitoring
  object and counters
    IME Client 11-5
    IME Client Instance 11-7
    IME Configuration Manager 11-2
    IME Server 11-2
    IME Server System Performance 11-4
performance objects and counters, Cisco IME 11-1
ports, configuring external IP address and port 3-28
post-installation tasks, Cisco IME 2-17
predefined objects
  IME Service 7-7
  IME System Performance 7-8
  Intercompany Media Services 7-6
  overview, Cisco IME 7-5
PSTN access trunks, configuring 3-36

R

Real-Time Monitoring Tool
  installing 7-1
  launching 7-3
  navigating 7-4
  predefined Cisco IME Objects
    IME Service 7-7
    IME System Performance 7-8
    Intercompany Media Services 7-6
    overview 7-5
  service 6-2
    Cisco AMC Service 6-2
    Cisco CallManager Serviceability RTMT 6-2
    Cisco Log Partition Monitoring Tool 6-2
    Cisco RIS Data Collector 6-2
  uninstalling 7-3
registration status 3-41

S

server connections, configuring 3-14
service
  Cisco AMC Service 6-2
  Cisco CallManager Serviceability RTMT 6-2
  Cisco CDP 6-3
  Cisco CDP Agent 6-4
  Cisco Certificate Expiry Monitor 6-4
  Cisco DRF Local 6-3
  Cisco DRF Master 6-2
  Cisco Log Partition Monitoring Tool 6-2
  Cisco RIS Data Collector 6-2
  Cisco Syslog Agent 6-4
  Cisco Tomcat 6-3
  Cisco Trace Collection Service 6-3
  Cisco Trace Collection Servlet 6-3
  Host Resources Agent 6-4
  MIB2 Agent 6-4
  Native Agent Adaptor 6-4
  network services 6-1
  SNMP Master Agent 6-3
  System Application Agent 6-4

SNMP
configuration checklist 9-1
configuring on Cisco IME server 9-1
inform notification destination 9-5
informs
configuration settings 9-5, 9-6
MIB 9-8
notification destination (V3)
configuration settings 9-5, 9-6
service
Cisco CDP Agent 6-4
Cisco Syslog Agent 6-4
Host Resources Agent 6-4
MIB2 Agent 6-4
Network Agent Adaptor 6-4
SNMP Master Agent 6-3
System Application Agent 6-4
trap notification destinations 9-4
traps
configuration settings 9-5, 9-6
users 9-3
SNMP Master Agent service 6-3
SYSAPPL-MIB 9-9
System Application Agent service 6-4
system history log 10-1
accessing
using RTMT 10-4
using the CLI 10-3
fields 10-2
overview 10-1

T

transformations
configuring Cisco IME E.164 3-35
configuring profiles 3-30
transformations, configuring called and calling party patterns 3-29
trap notification destinations 9-4
traps
configuration settings 9-5, 9-6
troubleshooting
Cisco IME installation 2-27
Cisco Intercompany Media Engine 10-1
trunks
configuring PSTN access 3-36
trust elements
configuring 3-25
trust groups
associating with Cisco IME services 3-26
associating with trust elements 3-25
configuring 3-24

V

Vservice publication 3-42