# Configuration and Administration of the IM and Presence Service on Cisco Unified Communications Manager, Release 10.5(1)

**First Published:** 2014-03-03

**Last Modified:** 2018-09-19

**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

# CONTENTS


PART I **Deployment Planning** 17

CHAPTER 1 **IM and Presence Service Features and Functions** 1

IM and Presence Service Components 1

Main Components 1

SIP Interface 2

AXL/SOAP Interface 3

LDAP Interface 3

XMPP Interface 3

CTI interface 4

Cisco IM and Presence Data Monitor 4

IM and Presence Service Feature Deployment Options 5

Deployment models 7

IM-Only Deployment 7

High Availability for Single-Node, Multiple-Node, and IM-Only Deployments 7

Presence Redundancy Groups and High Availability 8

Clustering Over WAN 9

User Assignment 9

End User Management 9

Availability and Instant Messaging 10

Chat 10

IM Forking 10

Offline IM 10

Broadcast IM 10

Chat Rooms on IM and Presence Service 10

Chat Room Limits 11

File Transfer 12
Important Notes About IM and Presence Service and Chat 12
IM Compliance 12
Presence Data Overview 12
Manual Presence 13
System Determined Presence 13
LDAP Integrations 14
Third-Party Integrations 14
Third-Party Client Integration 15
Supported Third-Party XMPP Clients 15
License Requirements for Third-Party Clients 16
XMPP Client Integration on Cisco Unified Communications Manager 16
LDAP Integration for XMPP Contact Search 16
DNS Configuration for XMPP Clients 16
IPv6 Support 16
IM Address Schemes and Default Domain 17
IM Address Using UserID@Default_Domain 17
IM Address Using Directory URI 18
IM Address Examples 18
IM Address Integration with Cisco Unified Communications Manager 19
UserID@Default_Domain Integration with Cisco Unified Communications Manager 19
Directory URI Integration with Cisco Unified Communications Manager 19
Multiple IM Domain Management 20
Security 20
Single Sign-On 20

CHAPTER 2 **Multinode Scalability and WAN Deployments** 23
Multinode Scalability Feature 23
Multinode Scalability Requirements 23
Scalability Options for Deployment 23
Cluster-Wide DNS SRV 25
Local Failover 25
Presence Redundancy Group Failure Detection 25
Method Event Routing 26

External Database Recommendations 26
Clustering Over WAN for Intracluster and Intercluster Deployments 26
Intracluster Deployments Over WAN 26
Multinode Configuration for Deployment Over WAN 27
Intercluster Deployments 27
Intercluster Deployments Over WAN 27
Intercluster Peer Relationships 27
Intercluster Router to Router Connections 28
Node Name Value for Intercluster Deployments 28
IM and Presence Default Domain Value for Intercluster Deployments 29
IM Address Scheme for Intercluster Deployments 29
Secure Intercluster Router to Router Connection 29

CHAPTER 3 **IM and Presence Service Planning Requirements 31**
Multinode Hardware Recommendations 31
Intercluster Hardware Recommendations 32
Supported End Points 32
LDAP Directory Servers Supported 33
WAN Bandwidth Requirements 33
WAN Bandwidth Considerations 33
Multinode Scalability and Performance 34
Multinode Scalability Requirements 34
Multinode Performance Recommendations 34
User License Requirements 34
DNS Domain and Default Domain Requirements 35

CHAPTER 4 **Workflows 37**
Basic Deployment with High Availability Workflow 37
Basic Deployment with High Availability and IP Phone Presence Workflow 39
Federation Deployment Workflow 42
IM-Only Deployment Workflow 45

PART II **System Configuration 47**

CHAPTER 5 **Cisco Unified Communications Manager configuration for integration with IM and Presence Service** 49

User and Device Configuration on Cisco Unified Communications Manager before Integration Task List 49

Configure Inter-Presence Group Subscription Parameter 51

SIP Trunk Configuration on Cisco Unified Communications Manager 51

Configure SIP Trunk Security Profile for IM and Presence Service 52

Configure SIP Trunk for IM and Presence Service 52

Configure Phone Presence for Unified Communications Manager Outside of Cluster 54

Configure TLS Peer Subject 54

Configure TLS Context 54

Verify Required Services Are Running on Cisco Unified Communications Manager 55

CHAPTER 6 **IM and Presence Service Network Setup** 57

Configuration changes and service restart notifications 57

Service Restart Notifications 57

Cisco XCP Router Restart 57

Restart Cisco XCP Router Service 58

DNS Domain Configuration 58

IM and Presence Service Clusters Deployed in Different DNS Domain or Subdomains 59

IM and Presence Service Nodes Within Cluster Deployed in Different DNS Domains or Subdomains 59

IM and Presence Service Nodes Within Cluster Deployed in DNS Domain That is Different Than the Associated Cisco Unified Communications Manager Cluster 60

Specify DNS Domain Associated with Cisco Unified Communications Manager Cluster 61

IM and Presence Service Default Domain Configuration 62

IM Address Configuration 63

IM Address Configuration Requirements 63

UserID@Default_Domain IM Address Interactions and Restrictions 64

Directory URI IM Address Interactions and Restrictions 64

Configure IM Address Task Flow 64

Stop Services 65

Assign IM Addressing Scheme 66

Restart Services 67
Domain Management for IM and Presence Service Clusters 68
IM Domain Management Interactions and Restrictions 68
View IM Address Domains 69
Add or Update IM Address Domains 69
Delete IM Address Domains 70
Routing Information Configuration on IM and Presence Service 71
Routing Communication Recommendations 71
Configure MDNS Routing and Cluster ID 71
Configure Routing Communication 72
Configure Cluster ID 73
Configure Throttling Rate for Availability State Change Messages 73
IPv6 Configuration 74
IPv6 Interactions and Restrictions 74
Enable IPv6 on Eth0 for IM and Presence Service 75
Disable IPv6 on Eth0 for IM and Presence Service 76
Enable IPv6 Enterprise Parameter 77
Configure Proxy Server Settings 77
Services on IM and Presence Service 78
Turn On Services for IM and Presence Service 78

CHAPTER 7 **IP Phone Presence Setup** 79
Static Route Configuration on IM and Presence Service 79
Route Embed Templates 79
Configure Route Embed Templates on IM and Presence Service 80
Configure Static Routes on IM and Presence Service 81
Presence Gateway Configuration on IM and Presence Service 84
Presence Gateway Configuration Option 84
Configure Presence Gateway 84
Configure SIP Publish Trunk on IM and Presence Service 85
Configure Cluster-Wide DNS SRV Name for SIP Publish Trunk 85

CHAPTER 8 **LDAP Directory Integration** 87
LDAP Server Name, Address, and Profile Configuration 87

LDAP Directory Integration with Cisco Unified Communications Manager Task List 87
Secure Connection Between Cisco Unified Communications Manager and LDAP Directory 88
Configure LDAP Synchronization for User Provisioning 88
Upload LDAP Authentication Server Certificates 90
Configure LDAP Authentication 90
Configure Secure Connection Between IM and Presence Service and LDAP Directory 91
LDAP Directory Integration for Contact Searches on XMPP Clients 92
LDAP Account Lock Issue 93
Configure LDAP Server Names and Addresses for XMPP Clients 93
Configure LDAP Search Settings for XMPP Clients 95
Turn On Cisco XCP Directory Service 97

CHAPTER 9 **Security Configuration on IM and Presence Service 99**
Security Setup Task List 99
Create Login Banner 100
Multi-Server Certificate Overview 101
IM and Presence Service Certificate Types 101
Certificate Exchange Configuration Between IM and Presence Service and Cisco Unified Communications Manager 104
Prerequisites for Configuring Security 104
Import Cisco Unified Communications Manager Certificate to IM and Presence Service 104
Restart SIP Proxy Service 105
Download Certificate from IM and Presence Service 105
Upload IM and Presence Service Certificate to Cisco Unified Communications Manager 106
Restart Cisco Unified Communications Manager Service 106
Multi-Server CA Signed Certificate Upload to IM and Presence Service 107
Single-Server CA Signed Certificate Upload to IM and Presence Service 107
CA-Signed Tomcat Certificate Task List 107
Upload Root Certificate and Intermediate Certificate of the Signing Certificate Authority 108
Restart Cisco Intercluster Sync Agent Service 108
Verify CA Certificates Have Synchronized to Other Clusters 109
Upload Signed Certificate to Each IM and Presence Service Node 110
Restart Cisco Tomcat Service 110
Verify Intercluster Syncing 111

CA-Signed cup-xmpp Certificate Upload 111
Upload Root Certificate and Intermediate Certificate of the Signing Certificate Authority 111
Restart Cisco Intercluster Sync Agent Service 112
Verify CA Certificates Have Synchronized to Other Clusters 113
Upload Signed Certificate to Each IM and Presence Service Node 113
Restart Cisco XCP Router Service On All Nodes 114
CA-Signed cup-xmpp-s2s Certificate Upload 114
Upload Root Certificate and Intermediate Certificate of Signing Certificate Authority 115
Verify CA Certificates Have Synchronized to Other Clusters 115
Upload Signed Certificate to Federation Nodes 116
Restart Cisco XCP XMPP Federation Connection Manager Service 117
Delete Self-Signed Trust Certificates 117
Delete Self-Signed Trust Certificates from IM and Presence Service 117
Delete Self-Signed Tomcat-Trust Certificates from Cisco Unified Communications Manager 118
SIP Security Settings Configuration on IM and Presence Service 119
Configure TLS Peer Subject 119
Configure TLS Context 120
XMPP Security Settings Configuration on IM and Presence Service 120
XMPP Security Modes 120
Configure Secure Connection Between IM and Presence Service and XMPP Clients 123
Turn On IM and Presence Service Services to Support XMPP Clients 124
Enable Wildcards in XMPP Federation Security Certificates 124
FIPS 140-2 Mode Configuration 125
FIPS 140-2 Mode 125
Node Reboot in FIPS 140-2 Mode 126
Force Manual Certificate Synchronization 126

CHAPTER 10 **Intercluster Peer Configuration** 127
Prerequisites for Intercluster Deployment 127
Intercluster Peer Configuration 128
Configure Intercluster Peer 128
Turn On Intercluster Sync Agent 129
Verify Intercluster Peer Status 130
Update Intercluster Sync Agent Tomcat Trust Certificates 130

Delete Intercluster Peer Connections 131

PART III Feature Configuration 133

CHAPTER 11 Availability and Instant Messaging on IM and Presence Service Configuration 135

Availability Setup on IM and Presence Service 135

Turn On or Off Availability Sharing for IM and Presence Service Cluster 135

Configure Ad-Hoc Presence Subscription Settings 136

Configure Maximum Contact List Size Per User 136

Configure Maximum Number of Watchers Per User 137

IM Setup On IM and Presence Service 138

Turn On or Off Instant Messaging for IM and Presence Service Cluster 138

Turn On or Off Offline Instant Messaging 138

Allow Clients to Log Instant Message History 139

Allow Cut and Paste in Instant Messages 140

Stream Management 140

Configure Stream Management 140

CHAPTER 12 OpenAM Single Sign-On 143

Single Sign-On Setup Task List 143

Single Sign-On Setup Preparation 145

Third-Party Software and System Requirements for Single Sign-On 145

Important Information Before Single Sign-On Setup 146

Single Sign-On Setup and Management Tasks 147

Provision Active Directory for Single Sign-On 147

Client Browser Setup for Single Sign-On 148

Configure Internet Explorer for Single Sign-On 148

Configure Firefox for Single Sign-On 149

Configure Windows Registry for the Real-Time Monitoring Tool 150

Install Java 150

Import IM and Presence Certificates Into OpenAM 154

Install Tomcat 156

Deploy OpenAM War On Apache Tomcat 159

Set Up OpenAM Using GUI Configurator 159

Set Up Policies On OpenAM Server 161
Set Up SSO Module Instance 163
Set Up J2EE Agent Profile On OpenAM Server 164
Set OpenAM Session Timeout 166
Import OpenAM Certificate Into IM and Presence Service 166
Activate Single Sign-On 168
Configure Access Permissions Before Enable SSO 168
Enable Single Sign-On Using GUI 170
Deactivate Single Sign-On 171
Configure Access Permissions Before Disable SSO 171
Disable Single Sign-On 173
Uninstall OpenAM on Windows 173
Set Debug Level 174

PART IV **Administration** 175

CHAPTER 13 **Chat Setup and Management** 177
Chat Deployments 177
Chat Deployment Scenario 1 177
Chat Deployment Scenario 2 177
Chat Deployment Scenario 3 178
Chat Deployment Scenario 4 178
Chat Administration Settings 179
Change IM Gateway Settings 179
Enable File Transfer 180
Limit Number Of Sign-In Sessions 180
Configure Persistent Chat Room Settings 181
Enable Persistent Chat 182
Configure Group Chat System Administration 185
Group Chat and Persistent Chat Default Settings Configuration and Reversion 185
Chat Node Alias Management 185
Chat Node Aliases 185
Key Considerations 186
Turn On or Off System-Generated Chat Node Aliases 187

Manage Chat Node Aliases Manually 188
Turn on Cisco XCP Text Conference Manager 189
Chat Room Management 190
Set Number of Chat Rooms 190
Configure Member Settings 190
Configure Availability Settings 191
Configure Invite Settings 191
Configure Occupancy Settings 192
Configure Chat Message Settings 192
Configure Moderated Room Settings 193
Configure History Settings 194
Group Chat and Persistent Chat Interactions and Restrictions 194

CHAPTER 14 End User Setup and Handling 197
End User Setup and Handling on IM and Presence Service 197
Authorization Policy Setup On IM and Presence Service 197
Automatic Authorization On IM and Presence Service 197
User Policy and Automatic Authorization 198
Configure Authorization Policy on IM and Presence Service 199
Bulk Rename User Contact IDs 200
Bulk Export User Contact Lists 201
Bulk Import Of User Contact Lists 202
Check Maximum Contact List Size 204
Upload Input File Using BAT 205
Create New Bulk Administration Job 205
Check Results of Bulk Administration Job 206
Duplicate User ID and Directory URI Management 207
User ID and Directory URI Monitoring 207
User ID and Directory URI Error Conditions 208
User ID and Directory URI Validation and Modification 209
User ID and Directory URI CLI Validation Examples 209
Set User Check Interval 210
Validate User IDs and Directory URIs Using System Troubleshooter 210

CHAPTER 15 User Migration 213
User Migration Between IM and Presence Service Clusters 213
Unassign Users From Current Cluster 214
Remove Stale Entries 214
Export User Contact Lists 215
Disable Users for IM and Presence Service 216
Move Users to New Cluster 217
LDAP Sync Enabled on Cisco Unified Communications Manager 217
LDAP Sync Not Enabled On Cisco Unified Communications Manager 218
Enable Users For IM and Presence Service On New Cluster 218
Import Contact Lists On Home Cluster 218

CHAPTER 16 Multilingual Support Configuration For IM and Presence Service 221
Locale Installation 221
Locale Installation Considerations 222
Locale Files 222
Install Locale Installer on IM and Presence Service 223
Error Messages 224
Localized Applications 226

PART V Troubleshooting IM and Presence Service 227

CHAPTER 17 Troubleshooting High Availability 229
Manual Failover, Fallback, and Recovery 229
Initiate Manual Failover 229
Initiate Manual Fallback 230
Initiate Manual Recovery 231
View Presence Redundancy Group Node Status 231
Node State Definitions 232
Node States, Causes, and Recommended Actions 233

CHAPTER 18 Troubleshooting UserID and Directory URI Errors 239
Received Duplicate UserID Error 239

Received Duplicate or Invalid Directory URI Error 240

CHAPTER 19 **Troubleshooting Single Sign-On 243**

Security Trust Error Message 243

"Invalid Profile Credentials" Message 244

"Module Name Is Invalid" Message 244

"Invalid OpenAM Access Manager (Openam) Server URL" Message 244

Web Browser Indicates a 401 Error 244

Web Browser Indicates a 403 Error or Displays a Blank Screen 245

"User is not Authorized to Perform this Function" Error 245

Web Browser Indicates an HTTP 404 Error 245

Web Browser Indicates an HTTP 500 Error or Displays a Blank Screen 245

"Authentication Failed" Message 246

Web Browser Displays OpenAM Login Screen 246

Web Browser Displays IM and Presence Service Login Screen 246

Internet Explorer Prompts for Username and Password 247

"User has no profile on this organization" Message 247

Problems Enabling SSO 247

Certificate Failure 248

CHAPTER 20 **Traces Used To Troubleshoot IM and Presence Service 249**

Troubleshooting IM and Presence Service Using Trace 249

Common Traces and Log File Locations for IM and Presence Service Nodes 250

IM and Presence Service Login and Authentication Traces 251

Availability, IM, Contact List, and Group Chat Traces 251

Availability and IM Traces for Partitioned Intradomain Federation MOC Contact Issues 252

Availability and IM Traces for XMPP-Based Interdomain Federation Contact Issues 253

Availability and IM Traces for SIP-Based Interdomain Federation Contact Issues 254

Calendaring Traces 254

Intercluster Synchronization Traces and Inter-Clustering Troubleshooter 255

SIP Federation Traces 255

XMPP Federation Traces 256

High CPU and Low VM Alert Troubleshooting 256

APPENDIX A **High Availability Client Login Profiles** 259

High Availability Login Profiles 259

Important Notes About High Availability Login Profiles 259

Use High Availability Login Profile Tables 260

Example High Availability Login Configurations 260

Single Cluster Configuration 261

500 Users Full UC (1vCPU 700MHz 2GB) Active/Active Profile 261

500 Users Full UC (1vCPU 700MHz 2GB) Active/Standby Profile 261

1000 Users Full UC (1vCPU 1500MHz 2GB) Active/Active Profile 262

1000 Users Full UC (1vCPU 1500MHz 2GB) Active/Standby Profile 262

2000 Users Full UC (1vCPU 1500Mhz 4GB) Active/Active Profile 263

2000 Users Full UC (1vCPU 1500Mhz 4GB) Active/Standby Profile 263

5000 Users Full UC (4 GB 2vCPU) Active/Active Profile 263

5000 Users Full UC (4 GB 2vCPU) Active/Standby Profile 264

15000 Users Full UC (4 vCPU 8GB) Active/Active Profile 265

15000 Users Full UC (4 vCPU 8GB) Active/Standby Profile 266

APPENDIX B **Additional Requirements** 269

High Availability Login Profiles 269

Important Notes About High Availability Login Profiles 269

Use High Availability Login Profile Tables 270

Example High Availability Login Configurations 270

Single Cluster Configuration 271

500 Users Full UC (1vCPU 700MHz 2GB) Active/Active Profile 271

500 Users Full UC (1vCPU 700MHz 2GB) Active/Standby Profile 271

1000 Users Full UC (1vCPU 1500MHz 2GB) Active/Active Profile 272

1000 Users Full UC (1vCPU 1500MHz 2GB) Active/Standby Profile 272

2000 Users Full UC (1vCPU 1500Mhz 4GB) Active/Active Profile 273

2000 Users Full UC (1vCPU 1500Mhz 4GB) Active/Standby Profile 273

5000 Users Full UC (4 GB 2vCPU) Active/Active Profile 273

5000 Users Full UC (4 GB 2vCPU) Active/Standby Profile 274

15000 Users Full UC (4 vCPU 8GB) Active/Active Profile 275

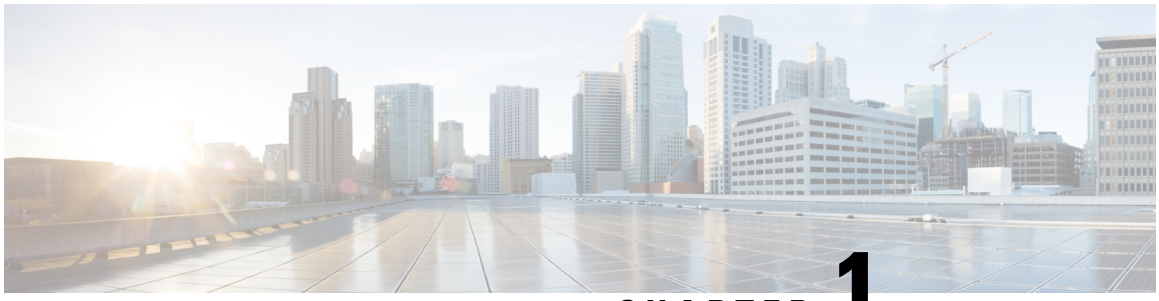
15000 Users Full UC (4 vCPU 8GB) Active/Standby Profile 276

XMPP Standards Compliance 277

PART I

# Deployment Planning


- IM and Presence Service Features and Functions, on page 1
- Multinode Scalability and WAN Deployments, on page 23
- IM and Presence Service Planning Requirements, on page 31
- Workflows, on page 37



CHAPTER 1

# IM and Presence Service Features and Functions

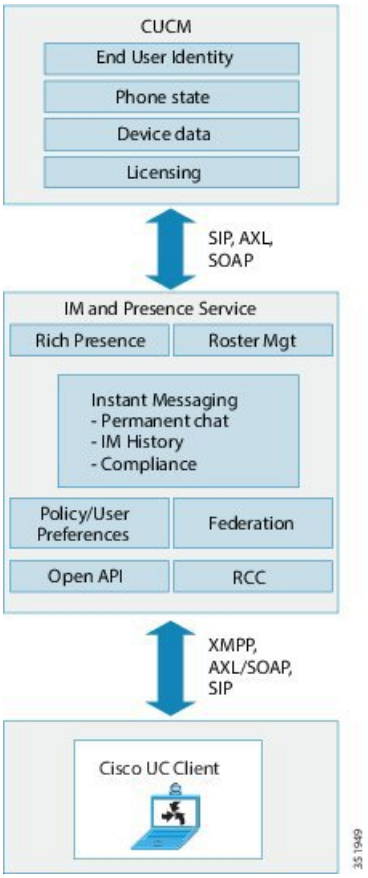

- IM and Presence Service Components, on page 1
- IM and Presence Service Feature Deployment Options, on page 5
- Deployment models, on page 7
- User Assignment, on page 9
- End User Management, on page 9
- Availability and Instant Messaging, on page 10
- LDAP Integrations, on page 14
- Third-Party Integrations, on page 14
- Third-Party Client Integration, on page 15
- IM Address Schemes and Default Domain, on page 17
- Security, on page 20
- Single Sign-On, on page 20


# IM and Presence Service Components

## Main Components

The following figure provides an overview of an IM and Presence Service deployment, including the main components and interfaces between Cisco Unified Communications Manager and IM and Presence Service.

*Figure 1: IM and Presence Service Basic Deployment*




# SIP Interface

A SIP connection handles the presence information exchange between Cisco Unified Communications Manager and Cisco Unified Presence. To enable the SIP connection on Cisco Unified Communications Manager, you must configure a SIP trunk pointing to the Cisco Unified Presence server.

On Cisco Unified Presence, configuring Cisco Unified Communications Manager as a Presence Gateway will allow Cisco Unified Presence to send SIP subscribe messages to Cisco Unified Communications Manager over the SIP trunk.

**Note** Cisco Unified Presence does not support clients (Cisco clients or third party) connecting to Cisco Unified Presence using SIP/SIMPLE interface over TLS. Only a SIP connection over TCP is supported.

### Related Topics

SIP Trunk Configuration on Cisco Unified Communications Manager, on page 51
Presence Gateway Configuration Option, on page 84

# AXL/SOAP Interface

The AXL/SOAP interface handles the database synchronization from Cisco Unified Communications Manager and populates the IM and Presence Service database. To activate the database synchronization, you must start the Sync Agent service on IM and Presence Service.

By default the Sync Agent load balances all users equally across all nodes within the IM and Presence Service cluster. You also have the option to manually assign users to a particular node in the cluster.

For guidelines on the recommended synchronization intervals when executing a database synchronization with Cisco Unified Communications Manager, for single and dual-node IM and Presence Service, see the IM and Presence Service SRND document.

**Note** The AXL interface is not supported for application developer interactions.

### Related Topics

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

# LDAP Interface

Cisco Unified Communications Manager obtains all user information via manual configuration or synchronization directly over LDAP. The IM and Presence Service then synchronizes all this user information from Cisco Unified Communications Manager (using the AXL/SOAP interface).

IM and Presence Service provides LDAP authentication for users of the Cisco Jabber client and IM and Presence Service user interface. If a Cisco Jabber user logs into IM and Presence Service, and LDAP authentication is enabled on Cisco Unified Communications Manager, IM and Presence Service goes directly to the LDAP directory for user authentication. When the user is authenticated, IM and Presence Service forwards this information to Cisco Jabber to continue the user login.

### Related Topics

LDAP Directory Integration, on page 87
LDAP Server Name, Address, and Profile Configuration, on page 87
Secure Connection Between Cisco Unified Communications Manager and LDAP Directory, on page 88
Configure LDAP Server Names and Addresses for XMPP Clients, on page 93

# XMPP Interface

An XMPP connection handles the presence information exchange and instant messaging operations for XMPP-based clients. The IM and Presence Service supports ad hoc and persistent chat rooms for XMPP-based clients. An IM Gateway supports the IM interoperability between SIP-based and XMPP-based clients in an IM and Presence Service deployment.

### Related Topics

Configure Secure Connection Between IM and Presence Service and XMPP Clients, on page 123

# CTI interface

The CTI (Computer Telephony Integration) interface handles all the CTI communication for users on the IM and Presence node to control phones on Cisco Unified Communications Manager. The CTI functionality allows users of the Cisco Jabber client to run the application in desk phone control mode.

The CTI functionality is also used for the IM and Presence Service remote call control feature on the Microsoft Office Communicator client. For information about configuring the remote call control feature, see the *Microsoft Office Communicator Call Control with Microsoft OCS for IM and Presence Service on Cisco Unified Communications Manager*.

To configure CTI functionality for IM and Presence Service users on Cisco Unified Communications Manager, users must be associated with a CTI-enabled group, and the primary extension assigned to that user must be enabled for CTI.

To configure Cisco Jabber desk phone control, you must configure a CTI server and profile, and assign any users that wish to use the application in desk phone mode to that profile. However, note that all CTI communication occurs directly between Cisco Unified Communications Manager and Cisco Jabber, and not through the IM and Presence Service node.

# Cisco IM and Presence Data Monitor

The Cisco IM and Presence Data Monitor monitors IDS replication state on the IM and Presence Service. Other IM and Presence services are dependent on the Cisco IM and Presence Data Monitor. These dependent services use the Cisco service to delay startup until such time as IDS replication is in a stable state.

The Cisco IM and Presence Data Monitor also checks the status of the Cisco Sync Agent sync from Cisco Unified Communications Manager. Dependent services are only allowed to start after IDS replication has set up and the Sync Agent on the IM and Presence database publisher node has completed its sync from Cisco Unified Communications Manager. After the timeout has been reached, the Cisco IM and Presence Data Monitor on the Publisher node will allow dependent services to start even if IDS replication and the Sync Agent have not completed.

On the subscriber nodes, the Cisco IM and Presence Data Monitor delays the startup of feature services until IDS replication is successfully established. The Cisco IM and Presence Data Monitor only delays the startup of feature services on the problem subscriber node in a cluster, it will not delay the startup of feature services on all subscriber nodes due to one problem node. For example, if IDS replication is successfully established on node1 and node2, but not on node3, the Cisco IM and Presence Data Monitor allows feature services to start on node1 and node2, but delays feature service startup on node3.

The Cisco IM and Presence Data Monitor behaves differently on the IM and Presence database publisher node. It only delays the startup of feature services until a timeout expires. When the timeout expires, it allows all feature services to start on the publisher node even if IDS replication is not successfully established.

The Cisco IM and Presence Data Monitor generates an alarm when it delays feature service startup on a node. It then generates a notification when IDS replication is successfully established on that node.

The Cisco IM and Presence Data Monitor impacts both a fresh multinode installation, and a software upgrade procedure. Both will only complete when the publisher node and subscriber nodes are running the same IM and Presence release, and IDS replication is successfully established on the subscriber nodes.

To check the status of the IDS replication on a node either:

- Use this CLI command:

  utils dbreplication runtimestate

- Use the Cisco Unified IM and Presence Reporting Tool. The “IM and Presence Database Status” report displays a detailed status of the cluster.

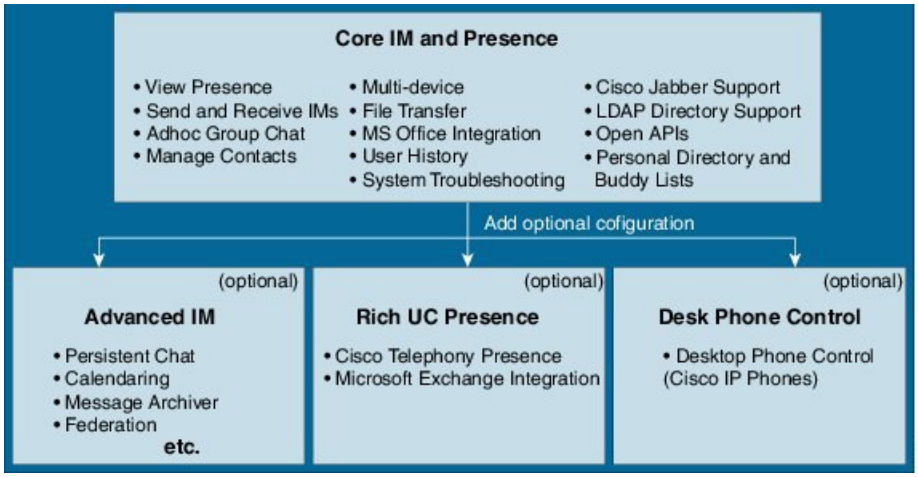
To check the status of the Cisco Sync Agent, navigate to the Cisco Unified CM IM and Presence Administration interface and select **Diagnostics** > **System Dashboard**. You will find the CUCM Publisher IP address as well as the Sync Status.

# IM and Presence Service Feature Deployment Options

Basic IM, availability, and ad hoc group chat are among the core features that are available after you install IM and Presence Service and configure your users in a basic deployment.

You can add optional features to enhance a basic deployment. The following figure shows the IM and Presence Service feature deployment options.

***Figure 2: IM and Presence Service Feature Deployment Options***



The following table lists the feature deployment options for IM and Presence Service.

***Table 1: IM and Presence Service Feature Deployment Options***

| Core IM and Availability Features | Advanced IM Features (optional) | Rich Unified Communications Availability features (optional) | Remote Desk Phone Control (optional) |
|---|---|---|---|
| View user availability<br>Securely send and receive rich text IMs<br>File transfers<br>Ad hoc group chat<br>Manage contacts<br>User history<br>Cisco Jabber support<br>Multiple client device support: Microsoft windows, MAC, Mobile, tablet, IOS, Android, BB<br>Microsoft Office integration<br>LDAP directory integration<br>Personal directory and buddy lists<br>Open APIs<br>System troubleshooting | Persistent chat<br>Message Archiver<br>Calendaring<br>Third-party XMPP client support<br>High availability<br>Scalability: multinode support and clustering over WAN<br>Interclustering peering<br>Enterprise federation (B2B):<br>• Cisco Unified Presence integration<br>• Cisco WebEx integration<br>• Microsoft Lync/OCS server integration (interdomain and partitioned intradomain federation)<br>• IBM SameTime integration<br>• Cisco Jabber XCP<br>Public federations (B2C):<br>• Google Talk, AOL integration<br>• XMMP services or BOTs<br>• Third-party Exchange Service integration<br>IM Compliance<br>Single Sign On<br>Custom login banner | Cisco telephony availability<br>Microsoft Exchange server integration | Remote Cisco IP Phone control<br>Microsoft Remote Call Control integration |

# Deployment models

## IM-Only Deployment

The IM and Presence Service supports an IM-only deployment. This type of deployment supports up to 25,000 users per node and up to 75,000 users in an IM and Presence Service cluster.

**Related Topics**

IM-Only Deployment Workflow, on page 45

## High Availability for Single-Node, Multiple-Node, and IM-Only Deployments

IM and Presence Service supports single-node, multiple-node, and IM-only High Availability deployments.

In a single-node deployment within a cluster, there is no High Availability failover protection for users assigned to the node. In a multiple-node deployment using presence redundancy groups, you can enable High Availability for the group so that users have failover protection.

Cisco recommends that you configure your IM and Presence Service deployments as High Availability deployments. Although you are permitted to have both High Availability and non-High Availability presence redundancy groups configured in a single deployment, this configuration is not recommended. You must manually turn on High Availability for a presence redundancy group using the Cisco Unified CM Administration interface. For more information about how to configure High Availability, see the *Cisco Unified Communications Manager Administration Guide*.

All IM and Presence Service nodes must belong to a presence redundancy group, which can consist of a single IM and Presence Service node or a pair of IM and Presence Service nodes. A pair of nodes is required for High Availability. Each node has an independent database and set of users operating with a shared availability database that is able to support common users.

You can achieve High Availability using two different setups: balanced and active/standby. You can set up the nodes in a presence redundancy group to work together in Balanced Mode, which provides redundant High Availability with automatic user load balancing and user failover in case one of the nodes fails because of component failure or power outage. In an active/standby setup, the standby node automatically takes over for the active node if the active node fails.

See the following guides for more information and instructions to set up presence redundancy groups, High Availability modes, and user assignments:

- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager  Bulk Administration Guide*
- *Cisco Unified Communications Manager Features and Services Guide*
- *Cisco Unified Communications Manager Installation Guide*
- *Cisco Unified Communications Manager System Guide*

# Presence Redundancy Groups and High Availability

A presence redundancy group is comprised of two IM and Presence Service nodes from the same cluster and provides both redundancy and recovery for IM and Presence Service clients and applications. Use **Cisco Unified CM Administration** to assign nodes to a presence redundancy group and to enable high availability.

- Failover - Occurs in a presence redundancy group when one or more critical services fails on an IM and Presence Service node in the group or a node in the group fails. Clients automatically connect to the other IM and Presence Service node in that group.
- Fallback - Occurs when a fallback command is issued from the Command Line Interface (CLI) or Cisco Unified Communications Manager during either of these conditions:
  - The failed IM and Presence Service node comes back into service and all critical services are running. The failed over clients in that group reconnect with the recovered node when it becomes available.
  - The backup activated IM and Presence Service node fails due to a critical service failure, and the peer node is in the Failed Over state and supports the automatic recovery fallback.

Automatic FallbackIM and Presence Service supports automatic fallback to the primary node after a failover. Automatic fallback is the process of moving users back to the primary node after a failover without manual intervention. You can enable automatic fallback with the Enable Automatic Fallback service parameter on the Cisco Unified CM IM and Presence Administration interface. Automatic fallback occurs in the following scenarios:

- A critical service on Node A fails—A critical service (for example, the Presence Engine) fails on Node A. Automatic failover occurs and all users are moved to Node B. Node A is in a state called “Failed Over with Critical Services Not Running”. When the critical service recovers, the node state changes to "Failed Over." When this occurs Node B tracks the health of Node A for 30 minutes. If no heartbeat is missed in this timeframe and the state of each node remains unchanged, automatic fallback occurs.
- Node A is rebooted—Automatic failover occurs and all users are moved to Node B. When Node A returns to a healthy state and remains in that state for 30 minutes automatic fallback will occur.
- Node A loses communications with Node B—Automatic failover occurs and all users are moved to Node B. When communications are re-established and remain unchanged for 30 minutes automatic fallback will occur.

If failover occurs for a reason other than one of the three scenarios listed here, you must recover the node manually. If you do not want to wait 30 minutes before the automatic fallback, you can perform a manual fallback to the primary node. For example: Using presence redundancy groups, Cisco Jabber clients will fail over to a backup IM and Presence Service node if the services or hardware fail on the local IM and Presence Service node. When the failed node comes online again, the clients automatically reconnect to the local IM and Presence Service node. When the failed node comes online, a manual fallback operation is required unless the automatic fallback option is set.

You can manually initiate a node failover, fallback, and recovery of IM and Presence Service nodes in the presence redundancy group. A manual fallback operation is required unless the automatic fallback option is set.

For instructions to set up presence redundancy groups and high availability, see *Cisco Unified Communications Manager Administration Guide*.

# Clustering Over WAN

The IM and Presence Service supports Clustering over WAN deployments.

**Related Topics**

Clustering Over WAN for Intracluster and Intercluster Deployments, on page 26

# User Assignment

To allow users to receive availability and Instant Messaging (IM) services on IM and Presence Service, you must assign users to nodes, and presence redundancy groups, in your IM and Presence Service deployment. You can manually or automatically assign users in a IM and Presence deployment. You manage user assignment using the **User Assignment Mode for Presence Server** Enterprise Parameter setting. This parameter specifies the mode in which the sync agent distributes users to the nodes in the cluster.

**Balanced mode** (default) assigns users equally to each node in the presence redundancy group and attempts to balance the total number of users equally across each node. The default mode is Balanced.

**Active-Standby mode** assigns all users to the first node of the presence redundancy group, leaving the secondary node as a backup.

**None mode** results in no assignment of the users to the nodes in the cluster by the sync agent.

If you choose manual user assignment, you must manually assign your users to nodes and presence redundancy groups, using Cisco Unified Communications Manager Administration. See the *Cisco Unified Communications Manager Administration Guide* for more information.

# End User Management

You can use the IM and Presence Service GUI to perform the following end user management tasks:

- Check for duplicate and invalid end user instances across your deployment.
- Export contact lists.
- Import contact lists on the home cluster.

For instructions to migrate IM and Presence Service users, see topics related to user migration between clusters, user management, and administration.

For information about assigning users to IM and Presence Service nodes and to set up end users for IM and Presence Service, see the following guides:

- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager Bulk Administration Guide*
- *Installing Cisco Unified Communications Manager*

# Availability and Instant Messaging

## Chat

Point-to-point Instant Messaging (IM) supports real-time conversations between two users at a time. IM and Presence Service exchanges messages directly between users, from the sender to the recipient. Users must be online in their IM clients to exchange point-to-point IMs.

You can disable both the chat and availability functionality on IM and Presence Service.

### Related Topics

Turn On or Off Instant Messaging for IM and Presence Service Cluster, on page 138
Turn On or Off Availability Sharing for IM and Presence Service Cluster, on page 135

## IM Forking

When a user sends an IM to a contact who is signed in to multiple IM clients. IM and Presence Service delivers the IM to each client. This functionality is called IM forking. IM and Presence Service continues to fork IMs to each client, until the contact replies. Once the contact replies, IM and Presence Service only delivers IMs to the client on which the contact replied.

You can disable offline instant messaging on IM and Presence Service.

### Related Topics

Turn On or Off Offline Instant Messaging, on page 138

## Offline IM

Offline IM is the ability to send IMs to a contact when they are offline. When a user sends an IM to an offline contact, IM and Presence Service stores the IM and delivers the IM when the offline contact signs in to an IM client.

## Broadcast IM

Broadcast IM is the ability to send an IM to multiple contacts at the same time, for example, a user wants to send a notification to a large group of contacts. Note that not all IM clients support this feature.

## Chat Rooms on IM and Presence Service

IM and Presence Service supports IM exchange in both ad hoc chat rooms and persistent chat rooms. By default, the Text Conference (TC) component on IM and Presence Service is set up and configured to handle IM exchange in ad hoc chat rooms. There are additional requirements you must configure to support persistent chat rooms, described further in this module.

### Ad hoc Chat Rooms

Ad hoc chat rooms are IM sessions that remain in existence only as long as one person is still connected to the chat room, and are deleted from the system when the last user leaves the room. Records of the IM conversation are not maintained permanently. Ad hoc chat rooms are by default public rooms. A user can join by being invited, or uninvited by finding the room through service discovery or room search on a third-party XMPP client.

Ad hoc chat rooms are public rooms by default, but can be reconfigured to be private. However, how users can join public or private ad hoc rooms depends on the type of XMPP client in use.

- Cisco Jabber users must be invited by a room owner or administrator in order to join any ad hoc chat room (public or private)
- Users on third-party XMPP clients can be invited in order to join any ad hoc chat room (public or private), or they can search for public-only ad hoc rooms to join via room discovery service.

### Persistent Chat Rooms

Persistent chat rooms are group chat sessions that remain in existence even when all users have left the room and do not terminate like ad hoc group chat sessions. The intent is that users will return to persistent chat rooms over time to collaborate and share knowledge of a specific topic, search through archives of what was said on that topic (if this feature is enabled on IM and Presence Service), and then participate in the discussion of that topic in real-time. Administrators can also restrict access to persistent chat rooms so that only members of that room have access. See Configure Member Settings, on page 190 and IM and Presence Service Ad Hoc Group Chat Rooms Privacy Policy in the Important Notes section of the Release Notes for Cisco Unified Communications Manager and IM and Presence Service, Release 11.0(1).

The TC component on IM and Presence Service enables users to:

- create new rooms, and manage members and configurations of the rooms they create.
- invite other users to rooms.
- determine the presence status of the members displayed within the room. The presence status displayed in a room confirms the attendance of the member in a room but may not reflect their overall presence status.

In addition, the Persistent Chat feature on IM and Presence Service allows users to:

- search for and join existing chat rooms.
- store a transcript of the chat and make the message history available for searching.

## Chat Room Limits

The following table lists the chat room limits for IM and Presence Service.

***Table 2: Chat Room Limits for IM and Presence Service***

| Number Of... | Maximum |
|---|---|
| Persistent chat rooms per node | 1500 rooms |
| Total rooms per node (ad hoc and persistent) | 16500 rooms |
| Occupants per room | 1000 occupants |
| Messages retrieved from the archive<br><br>This is the max number of messages that are returned when a user queries the room history. | 100 messages |

| Number Of... | Maximum |
|---|---|
| Messages in chat history displayed by default<br>This is the number of messages that are displayed when a user joins a chat room. | 15 messages |

## File Transfer

IM and Presence Service supports point to point file transfer between XMPP clients compliant with XEP-0096 (http://xmpp.org/extensions/xep-0096.html).

**Related Topics**

Enable File Transfer, on page 180

## Important Notes About IM and Presence Service and Chat

For SIP to SIP IM, the following services must be running on IM and Presence Service:

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Router

For SIP to XMPP IM, the following services must be running on IM and Presence Service:

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Router
- Cisco XCP Text Conference Manager

# IM Compliance

For information about configuring Instant Message (IM) compliance on the IM and Presence Service, refer to the following documents:

- *Instant Messaging Compliance Guide for IM and Presence Service on Cisco Unified Communications Manager*:

  http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

- *Database Setup Guide for IM and Presence Service on Cisco Unified Communications Manager*:

  http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

# Presence Data Overview

IM and Presence Service recomposes a user's rich presence each time a presence update occurs. Theare are two main categories of presence update:

- System Determined Presence

- Manual Presence

## Manual Presence

Manual Presence is explicitly set by a user. This usually overrides system-determined presence. Manual Presence settings include:

- A user setting Do Not Disturb on their IM Client
- A user setting Away on their IM Client
- A user setting Available on their IM client to override a system-determined status such as phone/calendar presence.
- A user setting any of the above from a third party application

A user can only have a single Manual Presence status. This is cleared when either:

- The user explicitly clears it (or replaces it with a new manual status).
- The user's client clears in on sign-out.
- The IM and Presence server clears in when the user is signed out of all IM devices.

## System Determined Presence

System Determined Presence is automatically published by a presence source based on some interaction between the user and the system:

- Making a phone call
- Joining a meeting
- Signing into or out of an IM device
- An IM device going idle after a period of inactivity
- Setting a phone to Do Not Disturb

There are four categories of System Determined Presence:

- IM Device Status

  A specific status of an individual IM device belonging to a user. If a user has multiple IM devices, IM and Presence Service will compose an overall user status that best represents a user's status across all such devices.

- Calendar Status

  A specific status representing a user's free/busy status on their calendar. IM and Presence Service will incorporate such calendar status an overall user status.

- Phone Status

  This represents the user's phone activity (On-hook/off-hook). There are individual inputs for each user's Line Appearance. IM and Presence Service will incorporate.

- Third Party Application Status

This can push presence updates into IM and Presence Service through open Interfaces such as SIP, XMPP, BOSH or the Presence Web Service. These presence statuses are incorporated into an overall composed user status.

# LDAP Integrations

You can configure a corporate LDAP directory in this integration to satisfy a number of different requirements:

- **User provisioning**: You can provision users automatically from the LDAP directory into the Cisco Unified Communications Manager database. Cisco Unified Communications Manager synchronizes with the LDAP directory content so you avoid having to add, remove, or modify user information manually each time a change occurs in the LDAP directory.
- **User authentication**: You can authenticate users using the LDAP directory credentials. IM and Presence Service synchronizes all the user information from Cisco Unified Communications Manager to provide authentication for users of the Cisco Jabber client and IM and Presence Service user interface.

Cisco recommends integration of Cisco Unified Communications Manager and Directory server for user synchronization and authentication purposes.

**Note** When Cisco Unified Communications Manager is not integrated with LDAP, you must verify that the username is exactly the same in Active Directory and Cisco Unified Communications Manager before deploying IM and Presence Service.

**Related Topics**

LDAP Directory Integration with Cisco Unified Communications Manager Task List, on page 87

# Third-Party Integrations

For third-party integrations, see the document references in the following table.

| Guide Title | This Guide Contains ... |
|---|---|
| Microsoft Exchange for IM and Presence Service on Cisco Unified Communications Manager | • Integrating with Microsoft Exchange 2007, 2010, and 2013<br>• Configuring Microsoft Active Directory for this integration |
| Microsoft Office Communicator Call Control with Microsoft OCS for IM and Presence Service on Cisco Unified Communications Manager | • Configuring IM and Presence Service as a CSTA gateway for remote call control from the Microsoft Office Communicator client<br>• Configuring Microsoft Active Directory for this integration<br>• Load-balancing MOC requests in a dual node IM and Presence Service deployment over TCP<br>• Load-balancing MOC requests in a dual node IM and Presence Service deployment over TLS |

| Guide Title | This Guide Contains ... |
|---|---|
| Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager | • Configuring IM and Presence Service for interdomain federation over the SIP protocol with Microsoft OCS and AOL, and over the XMPP protocol with IBM Sametime, Googletalk, Webex Connect, and another IM and Presence Service Release 9.x enterprise. |
| Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager | • Configuring IM and Presence Service for Partitioned Intradomain Federation<br>• Configuring Microsoft OCS for Partitioned Intradomain Federation<br>• Configuring Microsoft LCS for Partitioned Intradomain Federation<br>• User Migration |
| Remote Call Control with Microsoft Lync Server for IM and Presence Service on Cisco Unified Communications Manager | • Configuring Cisco Unified Communications Manager and IM and Presence Service for integration with Microsoft Lync<br>• Configuring Microsoft Active Directory<br>• Configuring normalization rules<br>• Configuring security between IM and Presence Service and Microsoft Lync |

# Third-Party Client Integration

## Supported Third-Party XMPP Clients

IM and Presence Service supports standards-based XMPP to enable third-party XMPP client applications to integrate with IM and Presence Service for availability and instant messaging (IM) services. Third-party XMPP clients must comply with the XMPP standard as outlined in the Cisco Software Development Kit (SDK).

This module describes the configuration requirements for integrating XMPP clients with IM and Presence Service. If you are integrating XMPP-based API (web) client applications with IM and Presence Service, also see developer documentation for IM and Presence Service APIs on the Cisco Developer Portal:

http://developer.cisco.com/

**Note** The clients that are supported may differ depending on which IM address scheme is configured for the IM and Presence Service node.

# License Requirements for Third-Party Clients

You must assign IM and Presence Service capabilities for each user of an XMPP client application.

IM and Presence capabilities are included within both User Connect Licensing (UCL) and Cisco Unified Workspace Licensing (CUWL). Refer to the *Cisco Unified Communications Manager Enterprise License Manager User Guide* for more information.

# XMPP Client Integration on Cisco Unified Communications Manager

Before you integrate an XMPP client, perform the following tasks on Cisco Unified Communications Manager:

- Configure the licensing requirements.
- Configure the users and devices. Associate a device with each user, and associate each user with a line appearance.

### Related Topics

User License Requirements, on page 34
User and Device Configuration on Cisco Unified Communications Manager before Integration Task List, on page 49

# LDAP Integration for XMPP Contact Search

To allow users of the XMPP client applications to search and add contacts from an LDAP directory, configure the LDAP settings for XMPP clients on IM and Presence Service.

### Related Topics

LDAP Directory Integration for Contact Searches on XMPP Clients, on page 92

# DNS Configuration for XMPP Clients

You must enable DNS SRV in your deployment when you integrate XMPP clients with IM and Presence Service. The XMPP client performs a DNS SRV query to find an XMPP node (IM and Presence Service) to communicate with, and then performs a record lookup of the XMPP node to get the IP address.

**Note** If you have multiple IM domains configured in your IM and Presence Service deployment, a DNS SRV record is required for each domain. All SRV records can resolve to the same result set.

# IPv6 Support

IM and Presence Service supports Internet Protocol version 6 (IPv6), which uses packets to exchange data, voice, and video traffic over digital networks. IPv6 also increases the number of network address bits from 32 bits in IPv4 to 128 bits. IPv6 deployment in the IM and Presence Service network functions transparently in a dual-stack IPv4 and IPv6 environment. The default network setting is IPv4.

Outbound IPv6 traffic is allowed when IPv6 is enabled. For example, SIP S2S can be configured to use either static routes or DNS queries. When a static route is configured and IPv6 is enabled, the SIP proxy attempts

to establish an IPv6 connection if IPv6 IP traffic is provided. You can use IPv6 for connections to external databases, LDAP and Exchange servers, and for federation connections on IM and Presence Service even though the connection between IM and Presence Service and Cisco Unified Communications Manager uses IPv4.

If the service uses DNS requests (for example, with XMPP S2S), then after receiving the list of IP addresses as the result of the DNS query, the service attempts to connect to each IP address on the list one by one. If a listed IP address is IPv6, the server establishes an IPv6 connection. If the request to establish the IPv6 connection fails, the service moves on to the next IP address on the list.

If for any reason IPv6 gets disabled for either the enterprise parameter or for ETH0 on the IM and Presence Service node, the node can still perform internal DNS queries and connect to the external LDAP or database server if the server hostname that is configured on IM and Presence Service is a resolvable IPv6 address.

For additional information about IPv6 and for network guidelines, see the following documents:

- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager Features and Services Guide*
- *Command Line Interface Guide for Cisco Unified Communications Solutions*
- *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager*

# IM Address Schemes and Default Domain

The IM and Presence Service supports two IM addressing schemes:

- *UserID@Default_Domain* is the default IM address scheme when you install the IM and Presence Service.
- Directory URI IM address scheme supports multiple domains, alignment with the user's email address, and alignment with Microsoft SIP URI.

**Note** The chosen IM address scheme must be consistent across all IM and Presence Service clusters.

The default domain is a cluster-wide setting that is used as part of the IM address when using the *UserID@Default_Domain* IM address scheme.

### Related Topics

Configure IM Address Scheme
IM Address Using UserID@Default_Domain, on page 17
IM Address Using Directory URI, on page 18

# IM Address Using UserID@Default_Domain

The *UserID@Default_Domain* IM address scheme is the default option when you perform a fresh install or upgrade IM and Presence Service from an earlier version. To configure the default domain, choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Settings** > **Advanced Configuration**.

# IM Address Using Directory URI

The Directory URI address scheme aligns a user's IM address with their Cisco Unified Communications Manager Directory URI.

The Directory URI IM address scheme provides the following IM addressing features:

- Multiple domain support. IM addresses do not need to use a single IM and Presence Service domain.
- Alignment with the user's email address. The Cisco Unified Communications Manager Directory URI can be configured to align with a user's email address to provide a consistent identity for email, IM, voice and video communications.
- Alignment with Microsoft SIP URI. The Cisco Unified Communications Manager Directory URI can be configured to align with the Microsoft SIP URI to ensure that the user's identity is maintained when migrating from Microsoft OCS/Lync to IM and Presence Service.

You set the Directory URI using Cisco Unified CM IM and Presence Administration GUI in one of two ways:

- Synchronize the Directory URI from the LDAP directory source.

  If you add an LDAP directory source in Cisco Unified Communications Manager, you can set a value for the Directory URI. Cisco Unified Communications Manager then populates the Directory URI when you synchronize user data from the directory source.

  **Note** If LDAP Directory Sync is enabled in Cisco Unified Communications Manager, you can map the Directory URI to the email address (mailid) or the Microsoft OCS/Lync SIP URI (msRTCSIP-PrimaryUserAddress).

- Manually specify the Directory URI value in Cisco Unified Communications Manager.

  If you do not add an LDAP directory source in Cisco Unified Communications Manager, you can manually enter the Directory URI as a free-form URI.

**Caution** If you configure the node to use Directory URI as the IM address scheme, Cisco recommends that you deploy only clients that support Directory URI. Any client that does not support Directory URI will not work if the Directory URI IM address scheme is enabled. Cisco recommends that you use the *UserID@Default_Domain* IM address scheme and not the Directory URI IM address scheme if you have any deployed clients that do not support Directory URI.

See the *Cisco Unified Communications Manager Administration Guide* for more information about setting up the LDAP directory for Directory URI.

# IM Address Examples

The following table provides samples of the IM address options that are available for the IM and Presence Service.

| **IM and Presence Service Default Domain**: cisco.com<br>**User**: John Smith<br>**Userid**: js12345<br>**Mailid**: jsmith@cisco-sales.com<br>**SIPURI**: john.smith@webex.com | | |
|---|---|---|
| **IM Address Format** | **Directory URI Mapping** | **IM Address** |
| <userid>@<domain> | n/a | js12345@cisco.com |
| Directory URI | mailid | jsmith@cisco-sales.com |
| Directory URI | msRTCSIP-PrimaryUserAddress | john.smith@webex.com |

# IM Address Integration with Cisco Unified Communications Manager

## UserID@Default_Domain Integration with Cisco Unified Communications Manager

The default IM address scheme is *UserID@Default_Domain*. Use this IM address scheme for all clusters that meet the following criteria:

- Any IM and Presence Service cluster is deployed with a software release that is earlier than Release 10.0.
- Any deployed clients do not support the Directory URI IM address scheme.

As the name suggests, all IM addresses are part of a single, default IM domain. Use the Cisco Unified CM IM and Presence Administration GUI to configure a consistent domain across all IM and Presence Service clusters.

The IM and Presence Service IM address (JID) is always *UserID@Default_Domain*. The *UserID* can be free-form or synced from LDAP. The following fields are supported:

- sAMAccountName
- User Principle Name (UPN)
- Email address
- Employee number
- Telephone number

While UserID can be mapped to the email address, that does not mean the IM URI equals the email address. Instead it becomes <*email-address*>*@Default_Domain*. For example, `amckenzie@example.com@sales-example.com`. The Active Directory (AD) mapping setting that you choose is global to all users within that IM and Presence Service cluster. It is not possible to set different mappings for individual users.

## Directory URI Integration with Cisco Unified Communications Manager

Unlike the *UserID@Default_Domain* IM address scheme, which is limited to a single IM domain, the Directory URI IM address scheme supports multiple IM domains. Any domain specified in the Directory URI is treated

as hosted by IM and Presence Service. The user's IM address is used to align with their Directory URI, as configured on Cisco Unified Communications Manager.

Directory URI can be free-form or synchronized from LDAP. If LDAP synchronization is disabled, you can set Directory URI as a free-form URI. If LDAP Directory synchronization is enabled, you can map the Directory URI to the following fields:

- email address (mailid)
- Microsoft OCS/Lync SIP URI (msRTCSIP-PrimaryUserAddress)

For information about enabling LDAP, see the *Cisco Unified Communications Manager Administration Guide*.

## Multiple IM Domain Management

IM and Presence Service supports IM addressing across multiple IM address domains and automatically lists all domains in the system. Use the Cisco Unified CM IM and Presence Administration GUI to manually add, update, and delete local administrator-managed domains, as well as view all local and system managed domains.

If you are interoperating with Cisco Expressway, see the Cisco Expressway Administrator Guide (X8.2) for further information on domain limitations.

# Security

You can configure a secure connection between IM and Presence Service and Cisco Unified Communications Manager, XMPP clients, and SIP clients by exchanging certificates. Certificates can be self-signed or generated by a Certificate Authority (CA).

For more information, see topics related to security configuration.

# Single Sign-On

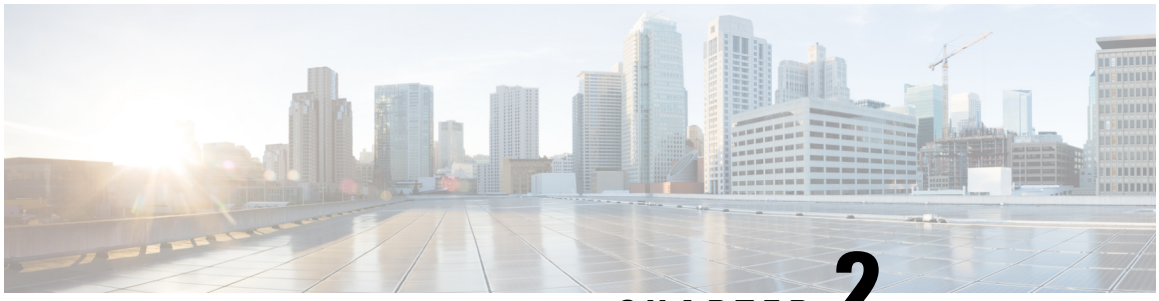
The OpenAM SSO feature allows system administrators to log in to a Windows client machine on a Windows domain and use the following IM and Presence Service applications without being required to sign in again:

- Cisco Unified CM IM and Presence Administration
- Cisco Unified IM and Presence Serviceability
- Cisco Unified IM and Presence Reporting
- IM and Presence Disaster Recovery System
- Cisco Unified Real-Time Monitoring Tool (RTMT) for IM and Presence Service
- Cisco Unified IM and Presence Service Operating System Administration
- Cisco Client Profile Agent – This option is only applicable to customers using Common Access Card (CAC) sign-on.

In Release 10.0 and later, there are two types of Single Sign-On (SSO) available:

- Security Assertion Markup Language (SAML) SSO
- OpenAM SSO

References to SSO refer to OpenAM SSO unless specifically identified as SAML SSO. For information about SAML SSO, see the *Cisco Unified Communications Manager Features and Services Guide*.



CHAPTER 2

# Multinode Scalability and WAN Deployments


- Multinode Scalability Feature, on page 23
- Cluster-Wide DNS SRV, on page 25
- Local Failover, on page 25
- Presence Redundancy Group Failure Detection, on page 25
- Method Event Routing, on page 26
- External Database Recommendations, on page 26
- Clustering Over WAN for Intracluster and Intercluster Deployments, on page 26


# Multinode Scalability Feature

## Multinode Scalability Requirements

IM and Presence Service supports multinode scalability:

- Six nodes per cluster
- 45,000 users per cluster with a maximum of 15,000 users per node in a full Unified Communication (UC) mode deployment
- 15,000 users per cluster in a presence redundancy group, and 45,000 users per cluster in a deployment with High Availability.
- Administrable customer-defined limit on the maximum contacts per user (default unlimited)
- The IM and Presence Service continues to support intercluster deployments with the multinode feature.

Scalability depends on the number of clusters in your deployment. For detailed VM configuration requirements and OVA templates, see *Virtualization for Unified CM IM and Presence* at the following url: http://docwiki.cisco.com/wiki/Virtualization_for_Unified_CM_IM_and_Presence

## Scalability Options for Deployment

IM and Presence Service clusters can support up to six nodes. If you originally installed less than six nodes, then you can install additional nodes at any time. If you want to scale your IM and Presence Service deployment to support more users, you must consider the multinode deployment model you have configured. The following table describes the scalability options for each multinode deployment model.

*Table 3: Multinode Scalability Options*

| Deployment Mode | Scalability Option | |
|---|---|---|
| | **Add a New Node to an Existing Presence Redundancy Group** | **Add a New Node to a New Presence Redundancy Group** |
| Balanced Non-Redundant High Availability Deployment | If you add a new node to an existing presence redundancy group, the new node can support the same number of users as the existing node; the presence redundancy group can now support twice the number of users. It also provides balanced High Availability for the users on the existing node and the new node in that presence redundancy group. | If you add a new node to a new presence redundancy group, you can support more users in your deployment.<br>This does not provide balanced High Availability for the users in the presence redundancy group. To provide balanced High Availability, you must add a second node to the presence redundancy group. |
| Balanced Redundant High Availability Deployment | If you add a new node to an existing presence redundancy group, the new node can support the same users as the existing node. For example, if the existing node supports 5000 users, the new node supports the same 5000 users. It also provides balanced redundant High Availability for the users on the existing node and the new node in that presence redundancy group.<br>**Note** You may have to reassign your users within the presence redundancy group, depending how many users were on the existing node. | If you add a new node to a new presence redundancy group, you can support more users in your deployment.<br>This does not provide balanced High Availability for the users in the presence redundancy group. To provide balanced High Availability, you must add a second node to the presence redundancy group. |
| Active/Standby Redundant High Availability Deployment | If you add a new node to an existing presence redundancy group, you provide High Availability for the users in the existing node in the presence redundancy group. This provides a High Availability enhancement only; it does not increase the number of users you can support in your deployment. | If you add a new node in a new presence redundancy group, you can support more users in your deployment.<br>This does not provide High Availability for the users in the presence redundancy group. To provide High Availability, you must add a second node to the presence redundancy group. |

# Cluster-Wide DNS SRV

For DNS configuration, you can define a cluster-wide IM and Presence Service address.

The SIP Publish Trunk on Cisco Unified Communications Manager uses the cluster-wide IM and Presence Service address to load-balance SIP PUBLISH messages from Cisco Unified Communications Manager to all nodes in the cluster. Notably this configuration ensures that the initial SIP PUBLISH messages are load-balanced across all nodes in the cluster. This configuration also provides a High Availability deployment as, in the event of a node failing, Cisco Unified Communications Manager will route the SIP PUBLISH messages to the remaining nodes.

The cluster-wide DNS configuration is not a required configuration. Cisco recommends this configuration as a method to load-balance the initial SIP PUBLISH messages across all nodes in the cluster. IM and Presence Service sends subsequent SIP PUBLISH messages for each device to the node where the user is homed on IM and Presence Service.

Even though IM and Presence Service supports multiple domains, you require only a single clusterwide DNS SRV record. You specify that DNS SRV record when you configure the Cisco Unified Communications Manager SIP trunk. Cisco recommends that you use the IM and Presence Service default domain as the destination address for that DNS SRV record.

**Note** You can specify any domain value as the destination address of the DNS SRV record; however, ensure that the SIP Proxy Service Parameter called SRV Cluster Name on IM and Presence Service matches the domain value you specify in the DNS SRV record. No users need to be assigned to the domain that is specified.

For more information, see topics related to configuring Cisco Unified Communications Manager for integration with IM and Presence Service and DNS SRV records.

**Related Topics**

Configure Cluster-Wide DNS SRV Name for SIP Publish Trunk, on page 85

# Local Failover

You can also deploy IM and Presence Service over WAN where one presence redundancy group is located in one geographic site, and a second presence redundancy group is located in another geographic site. The presence redundancy group can contain a single node, or a dual node for High Availability between the local nodes. This model provides no failover between geographic sites.

# Presence Redundancy Group Failure Detection

The IM and Presence Service supports a failure detection mechanism for a presence redundancy group. Each node in the presence redundancy group monitors the status, or heartbeat, of the peer node. To configure the heartbeat connection and heartbeat intervals on IM and Presence Service, choose **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters** > **Server Recovery Manager (service)**. In the section General Server Recovery Manager Parameters (Clusterwide), configure the following parameters:

- **Heart Beat Interval**: This parameter specifies how often in seconds the Server Recovery Manager sends a heartbeat message to the peer Server Recovery Manager in the same presence redundancy group. The heartbeat is used to determine network availability. The default value is 60 seconds.
- **Connect Timeout**: This parameter specifies how long in seconds the Server Recovery Manager waits to receive a response from a connection request to the peer Server Recovery Manager. The default value is 30 seconds.

**Note** Cisco recommend that you configure these parameters with the default values.

# Method Event Routing

When you deploy IM and Presence Service over WAN we recommend that you configure TCP method event routing on IM and Presence Service. Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Routing** > **Method/Event Routing** to configure method event routes.

# External Database Recommendations

If you configure external database servers in your Clustering over WAN deployment, Cisco recommends that you co-locate the external database servers with the IM and Presence Service nodes that will use the external database servers.

You can connect the IM and Presence Service node to the external database server using either IPv4 or IPv6 Internet transport protocol.

For more information about external database servers and IM and Presence Service, see *Database Setup Guide for IM and Presence Service on Cisco Unified Communications Manager*.

# Clustering Over WAN for Intracluster and Intercluster Deployments

IM and Presence Service supports Clustering over WAN for intracluster and intercluster deployments.

## Intracluster Deployments Over WAN

IM and Presence Service supports intracluster deployments over WAN, using the bandwidth recommendations provided in this module. IM and Presence Service supports a single presence redundancy group geographically split over WAN, where one node in the presence redundancy group is in one geographic site and the second node in the presence redundancy group is in another geographic location.

This model can provide geographical redundancy and remote failover, for example failover to a backup IM and Presence Service node on a remote site. With this model, the IM and Presence Service node does not need to be co-located with the Cisco Unified Communications Manager database publisher node. The Cisco Jabber client can be either local or remote to the IM and Presence Service node.

This model also supports High Availability for the clients, where the clients fail over to the remote peer IM and Presence Service node if the services or hardware fails on the home IM and Presence Service node. When the failed node comes online again, the clients automatically reconnect to the home IM and Presence Service node.

When you deploy IM and Presence Service over WAN with remote failover, note the following restriction:

- This model only supports High Availability at the system level. Certain IM and Presence Service components may still have a single point of failure. These components are the Cisco Sync Agent, Cisco Intercluster Sync Agent, and Cisco Unified CM IM and Presence Administration interface.

IM and Presence Service also supports multiple presence redundancy groups in a Clustering over WAN deployment. For information about scale for a Clustering over WAN deployment, see the IM and Presence Service SRND.

For additional information, see the IM and Presence Service Solution Reference Network Design (SRND):

## Multinode Configuration for Deployment Over WAN

When you configure the IM and Presence Service multinode feature for an intracluster deployment over WAN, configure the IM and Presence Service presence redundancy group, nodes and user assignment as described in the multinode section, but note the following recommendations:

- For optimum performance, Cisco recommends that you assign the majority of your users to the home IM and Presence Service node. This deployment model decreases the volume of messages sent to the remote IM and Presence Service node over WAN, however the failover time to the secondary node depends on the number of users failing over.
- If you wish to configure a High Availability deployment model over WAN, you can configure a presence redundancy group-wide DNS SRV address. In this case, IM and Presence Service sends the initial PUBLISH request message to the node specified by DNS SRV and the response message indicates the host node for the user. IM and Presence Service then sends all subsequent PUBLISH messages for that user to the host node. Before configuring this High Availability deployment model, you must consider if you have sufficient bandwidth for the potential volume of messages that may be sent over the WAN.

### Related Topics

Intracluster Deployments Over WAN, on page 26
http://www.cisco.com/go/designzone

# Intercluster Deployments

## Intercluster Deployments Over WAN

IM and Presence Service supports intercluster deployments over WAN, using the bandwidth recommendations provided in this module.

### Related Topics

WAN Bandwidth Requirements, on page 33

## Intercluster Peer Relationships

You can configure peer relationships that interconnect standalone IM and Presence Service clusters, known as intercluster peers. This intercluster peer functionality allows users in one IM and Presence Service cluster

to communicate and subscribe to the availability information of users in a remote IM and Presence Service cluster within the same domain. Keep in mind that if you delete an intercluster peer from one cluster, then you must also delete the corresponding peer in the remote cluster.

IM and Presence Service uses the AXL/SOAP interface to retrieve user information for the home cluster association. IM and Presence Service uses this user information to detect if a user is a local user (user on the home cluster), or a user on a remote IM and Presence Service cluster within the same domain.

IM and Presence Service uses the XMPP interface for the subscription and notification traffic. If IM and Presence Service detects a user to be on a remote cluster within the same domain, IM and Presence Service reroutes the messages to the remote cluster.

**Caution** Cisco highly recommends that you set up intercluster peers in a staggered manner, as the initial sync uses substantial bandwidth and CPU. Setting up multiple peers at the same time could result in excessive sync times.

## Intercluster Router to Router Connections

By default, IM and Presence Service assigns all nodes in a cluster as intercluster router-to-router connectors. When IM and Presence Service establishes an intercluster peer connection between the clusters over the AXL interface, it synchronizes the information from all intercluster router-to-router connector nodes in the home and remote clusters.

You must restart the Cisco XCP Router service on all nodes in both local and remote clusters for IM and Presence Service to establish a connection between the intercluster router-to-router connector nodes. Each intercluster router-to-router connector in one cluster then either initiates or accepts an intercluster connection with router-to-router connectors in the other cluster.

**Note** In an intercluster deployment, when you add a new node to a cluster, you must restart the Cisco XCP router on all nodes in both the local and remote clusters.

### Related Topics

Secure Intercluster Router to Router Connection, on page 29

## Node Name Value for Intercluster Deployments

The node name defined for any IM and Presence Service node must be resolvable by every other IM and Presence Service node on every cluster. Therefore, each IM and Presence Service node name must be the FQDN of the node. If DNS is not deployed in your network, each node name must be an IP address.

**Note** Specifying the hostname as the node name is only supported if all nodes across all clusters share the same DNS domain.

**Attention** When using the Cisco Jabber client, certificate warning messages can be encountered if the IP address is configured as the IM and Presence Service node name. To prevent Cisco Jabber from generating certificate warning messages, the FQDN should be used as the node name. For instructions to set the IM and Presence Service node name value, see *Cisco Unified Communications Manager Administration Guide*.

**Related Topics**

IM and Presence Default Domain Value for Intercluster Deployments, on page 29

## IM and Presence Default Domain Value for Intercluster Deployments

If you configure an intercluster deployment, note the following:

- The IM and Presence default domain value on the local cluster must match the IM and Presence default domain value on the remote cluster to ensure that intercluster functionality will work correctly.

See topics related to IM and Presence default domain configuration for detailed instructions.

**Related Topics**

IM and Presence Service Default Domain Configuration

Node Name Value for Intercluster Deployments, on page 28

## IM Address Scheme for Intercluster Deployments

For intercluster deployments, all nodes in each of the clusters must use the same IM address scheme. If any node in a cluster is running a version of IM and Presence Service that is earlier than Release 10, all nodes must be set to use the `UserID@Default_Domain` IM address scheme for backward compatibility.

For more information, see topics related to IM address scheme configuration.

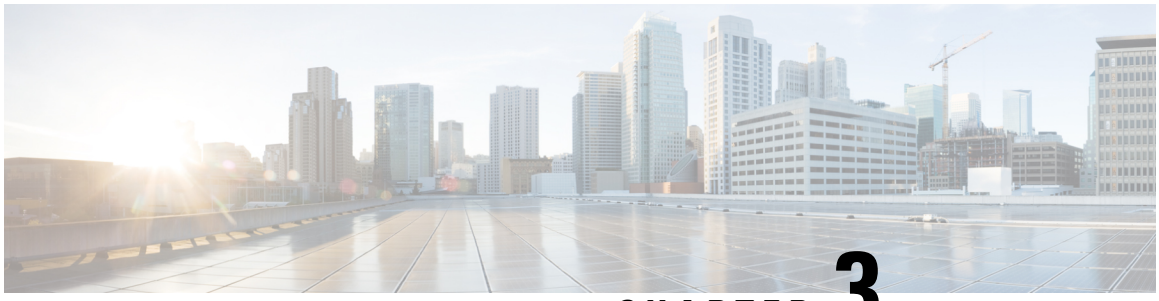
## Secure Intercluster Router to Router Connection

You can configure a secure XMPP connection between all router-to-router connectors in your IM and Presence Service deployment, incorporating both intracluster and intercluster router to router connections. Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Security** > **Settings**, and check **Enable XMPP Router-to-Router Secure Mode**.

When you turn on the secure mode for XMPP router-to-router connections, IM and Presence Service enforces a secure SSL connection using XMPP trust certificates. For intercluster deployments, IM and Presence Service enforces a secure SSL connection between each router-to-router connector node in the local cluster, and each router connector node in the remote cluster.

**Related Topics**

Intercluster Router to Router Connections, on page 28



CHAPTER 3

# IM and Presence Service Planning Requirements


- Multinode Hardware Recommendations, on page 31
- Intercluster Hardware Recommendations, on page 32
- Supported End Points, on page 32
- LDAP Directory Servers Supported, on page 33
- WAN Bandwidth Requirements, on page 33
- Multinode Scalability and Performance, on page 34
- User License Requirements, on page 34
- DNS Domain and Default Domain Requirements, on page 35


## Multinode Hardware Recommendations

When configuring the multinode feature, consider the following:

- Cisco recommends turning on High Availability in your deployment.
- Cisco only supports virtualized deployments of IM and Presence Service on Cisco Unified Computing System servers or on a Cisco-approved third-party server configuration. Cisco does not support deployments of IM and Presence on Cisco Media Convergence Server (MCS) servers. For more information about the deployment of IM and Presence Service in a virtualized environment, see http://docwiki.cisco.com/wiki/Unified_Communications_in_a_Virtualized_Environment.
- Minimize your deployment, for example, instead of using five virtual machines that support a total of two thousand users, choose two virtual machines that can support a total of five thousand users.
- Use the same generation of server hardware.
- Use similar hardware for all nodes in your deployment. If you must mix generations of similar hardware, put the same generations of older hardware together in a presence redundancy group and put fewer users on this presence redundancy group than on the more powerful presence redundancy group. Note that we do not recommend this deployment practice.

**Note** For multinode deployments using mixed hardware (for example, UCS, MCS, or VMware), it is highly recommended that the IM and Presence Service subscriber and database publisher nodes in the same subcluster have similar database size. If a significant difference in database size exists between the two nodes, you will receive an error during installation of the subscriber node.

**Note** For multinode deployments, instead of using mixed virtual machine deployment sizes, it is highly recommended that the IM and Presence Service subscriber and database publisher nodes in the same presence redundancy group have similar database size. If a significant difference in database size exists between the two nodes, you will receive an error during installation of the subscriber node.

For a list of the supported hardware for the multinode feature, and hardware user assignment guidelines for the multinode feature, see the IM and Presence Service compatibility matrices at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html

# Intercluster Hardware Recommendations

When planning an intercluster deployment, it is recommended that similar deployments be used on all IM and Presence Service clusters in the Enterprise to allow for syncing of all user data between clusters. For example, if a virtual server supporting a 5000 user deployment is used in Cluster A, then a 5000 user virtual server deployment should be used in Cluster B even if only 500 users are needed in Cluster B .

# Supported End Points

The multinode scalability feature supports the following end points:

- Cisco Unified Communications Manager (desk phone)
- Cisco Jabber
- Third-Party XMPP clients
- Cisco Unified Mobile Communicator
- Microsoft Office Communicator (Microsoft soft client)
- Lotus Sametime (Lotus soft client)

**Note** Lotus clients are used on the Microsoft server that is integrated with IM and Presence Service for remote call control.

- Third-Party Interface clients
- Lync 2010 and 2013 Clients (Microsoft Office Communicator)

Only third party clients support the Directory URI IM address scheme. All other clients should use the *UserID@Default_Domain* IM address scheme. See topics related to the IM and Presence Service IM address schemes for more information.

# LDAP Directory Servers Supported

IM and Presence Service integrates with these LDAP directory servers:

- Microsoft Active Directory 2000, 2003, 2008
- Netscape Directory Server
- Sun ONE Directory Server 5.2
- OpenLDAP

### Related Topics

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html
http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

# WAN Bandwidth Requirements

At a minimum, you must dedicate 5 Mbps of bandwidth for each IM and Presence Service presence redundancy group, with no more than an 80 millisecond round-trip latency. These bandwidth recommendations apply to both intracluster and intercluster WAN deployments. Any bandwidth less than this recommendation can adversely impact performance.

**Note** Each IM and Presence Service presence redundancy group that you add to your Clustering over WAN deployment requires an additional (dedicated) 5 Mbps of bandwidth.

## WAN Bandwidth Considerations

When you calculate the bandwidth requirements for your Clustering over WAN deployment, consider the following:

- In your bandwidth considerations, you must include the normal bandwidth consumption of a Cisco Unified Communications Manager cluster. If you configure multiple nodes, Cisco Unified Communications Manager uses a round-robin mechanism to load balance SIP/SIMPLE messages, which consumes more bandwidth. To improve performance and decrease traffic, you could provision a single dedicated Cisco Unified Communications Manager node for all SIP/SIMPLE messages sent between the IM and Presence Service and Cisco Unified Communications Manager.
- In your bandwidth considerations, we also recommend that you consider the number of contacts in the contact list for a Cisco Jabber user, and the size of user profiles on IM and Presence Service. See the IM and Presence Service SRND for recommendations regarding the size of a contact list when you deploy IM and Presence over WAN. Note also that the maximum contact list size on IM and Presence Service is 200, so you need to factor this in to your bandwidth considerations for systems with large numbers of users.

For additional information, see the *IM and Presence Service Solution Reference Network Design (SRND)*:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/uc7_0.html

# Multinode Scalability and Performance

## Multinode Scalability Requirements

IM and Presence Service supports multinode scalability:

- Six nodes per cluster
- 45,000 users per cluster with a maximum of 15,000 users per node in a full Unified Communication (UC) mode deployment
- 15,000 users per cluster in a presence redundancy group, and 45,000 users per cluster in a deployment with High Availability.
- Administrable customer-defined limit on the maximum contacts per user (default unlimited)
- The IM and Presence Service continues to support intercluster deployments with the multinode feature.

Scalability depends on the number of clusters in your deployment. For detailed VM configuration requirements and OVA templates, see *Virtualization for Unified CM IM and Presence* at the following url: http://docwiki.cisco.com/wiki/Virtualization_for_Unified_CM_IM_and_Presence

## Multinode Performance Recommendations

You can achieve optimum performance with the multinode feature when:

- The resources on all IM and Presence Service nodes are equivalent in terms of memory, disk size, and age. Mixing virtual server hardware classes results in nodes that are under-powered, therefore resulting in poor performance.
- You deploy virtual server hardware that complies with the hardware recommendations.
- You configure a Balanced Mode deployment model. In this case, the total number of users is equally divided across all nodes in all presence redundancy groups. The IM and Presence Service defaults to Balanced Mode user assignment to achieve optimum performance.

### Related Topics

Multinode Hardware Recommendations, on page 31
Balanced User Assignment Redundant High Availability Deployment

# User License Requirements

IM and Availability functionality does not require a node license or software version license. However, you must assign IM and Availability functionality to each IM and Presence Service user.

You can assign IM and Availability on a per user basis, regardless of the number of clients you associate with each user. When you assign IM and Availability to a user, this enables the user to send and receive IMs and also to send and receive availability updates. If the user is not enabled for IM and Availability, no availability updates are allowed for that user.

You can enable a user for IM and Presence Service functionality in the **End User Configuration** window in Cisco Unified Communications Manager. See the *Cisco Unified Communications Manager Administration Guide* for more information.

IM and Availability functionality is included within both User Connect Licensing (UCL) and Cisco Unified Workspace Licensing (CUWL). Refer to the *Cisco Unified Communications Manager Enterprise License Manager User Guide* for more information.

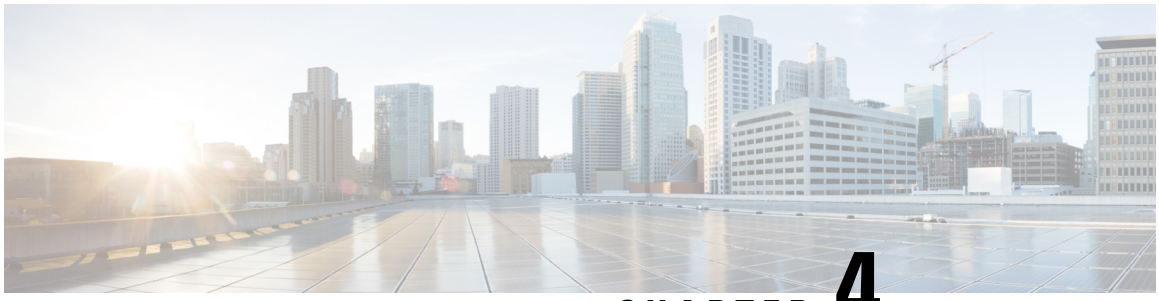
# DNS Domain and Default Domain Requirements

The following DNS domain and IM and Presence Service default domain conditions apply. To resolve any domain-related deployment issues, Cisco recommends that you set all IM and Presence Service node names in the cluster to the FQDN or IP address rather than the hostname.

- For inter-cluster IM and Presence Service deployments, it is required that each IM and Presence Service cluster shares the same underlying DNS domain.
- The DNS domain associated with any client devices should map to the IM and Presence Service DNS domain.
- Ensure that the DNS domain aligns with the IM and Presence Service default domain.

  The IM and Presence Service default domain value is set to the DNS domain by default during installation. You can not change the IM and Presence Service default domain during installation. To change the default domain to a value that is different from the DNS domain, you must use the Cisco Unified CM IM and Presence Administration GUI.

**Caution** Failure to set all IM and Presence Service node names in the cluster to the FQDN or IP address rather than the hostname can result in communications failure between nodes in a cluster. Affected functions include SIP and XMPP-based inter-cluster communications, High Availability, client sign-in, and SIP-based list subscriptions.



CHAPTER 4

# Workflows

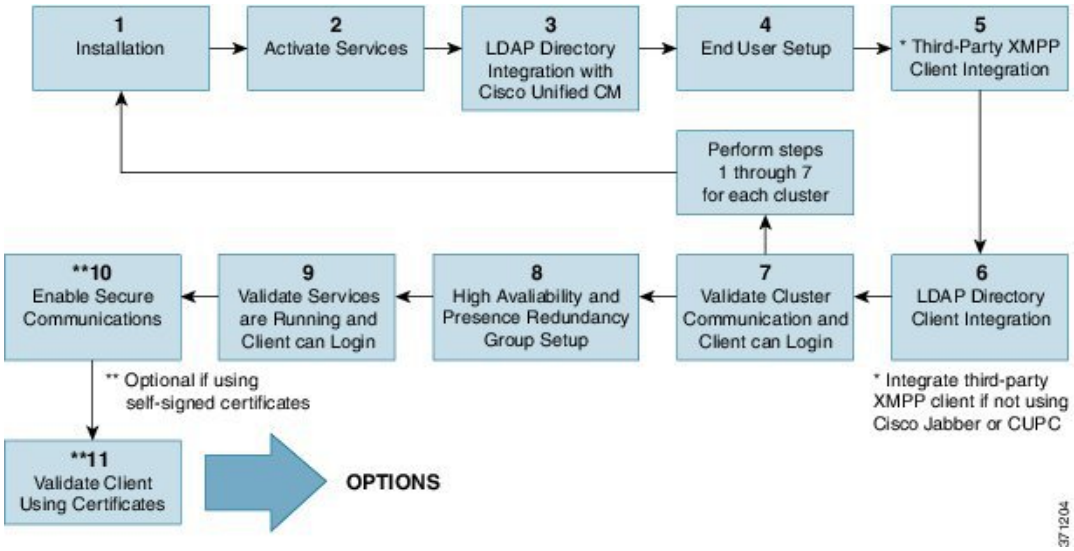

- Basic Deployment with High Availability Workflow, on page 37
- Basic Deployment with High Availability and IP Phone Presence Workflow, on page 39
- Federation Deployment Workflow, on page 42
- IM-Only Deployment Workflow, on page 45


## Basic Deployment with High Availability Workflow

The following workflow diagram shows the high-level steps to set up a basic IM and Presence Service deployment with High Availability. Users have access to the core IM and availability features, such as basic IM functionality, presence, and Ad Hoc group chats after a basic setup. Optional features can be configured to enhance user functionality.

For more advanced deployment scenarios and workflows, see topics related to workflows that include phone presence setup and federation.

***Figure 3: Basic IM and Presence Service Deployment Workflow with High Availability***




The following table describes each task in the workflow.

**Tip** Perform all preparation tasks before installing or configuring the IM and Presence Service node. Review topics related to deployment options and planning requirements.

***Table 4: Task List for Basic Workflow with High Availability***

| | Task | Description |
|---|---|---|
| 1 | Installation | For detailed Installation instructions, see *Installing Cisco Unified Communications Manager*. |
| 2 | Activate Services | You must manually activate feature services after you install the node. For detailed instructions, see *Installing Cisco Unified Communications Manager*.<br>**Tip** Network services start automatically after you install the node. |
| 3 | LDAP Directory Integration with Cisco Unified Communications Manager | Set up LDAP directory integration on the IM and Presence Service node:<br>• Secure the Cisco Unified Communications Manager and LDAP directory connection.<br>• Secure the connection between IM and Presence Service and the LDAP server.<br>**Tip** Integration of Cisco Unified Communications Manager and Cisco Jabber with the LDAP server is the recommended setup. For alternative setups, see topics related to LDAP integration. |
| 4 | End User Setup | Assign users to nodes and presence redundancy groups in yourIM and Presence Service deployment. You can manually or automatically assign users to the nodes in your IM and Presence Service deployment. See the *Cisco Unified Communications Manager Administration Guide* for instructions to assign users. The **User Assignment Mode for Presence Server Enterprise Parameter** is used to set the user assignment mode to balanced, active-stand-by, or none.<br>**Tip** Use Cisco Unified CM IM and Presence Administration to migrate users, export and import contact lists. |
| 5 | Third-Party XMPP Client Integration | (Optional) Integrate your third-party XMPP client if you are not using Cisco Jabber. |
| 6 | LDAP Directory Client Integration | Setup user integration with the LDAP directory:<br>• Configure LDAP synchronization for user provisioning.<br>• Upload LDAP server certificates.<br>• Configure LDAP user authentication.<br>**Tip** Integration of Cisco Unified Communications Manager and Cisco Jabber with the LDAP server is the recommended setup. For alternative setups, see topics related to LDAP integration. |

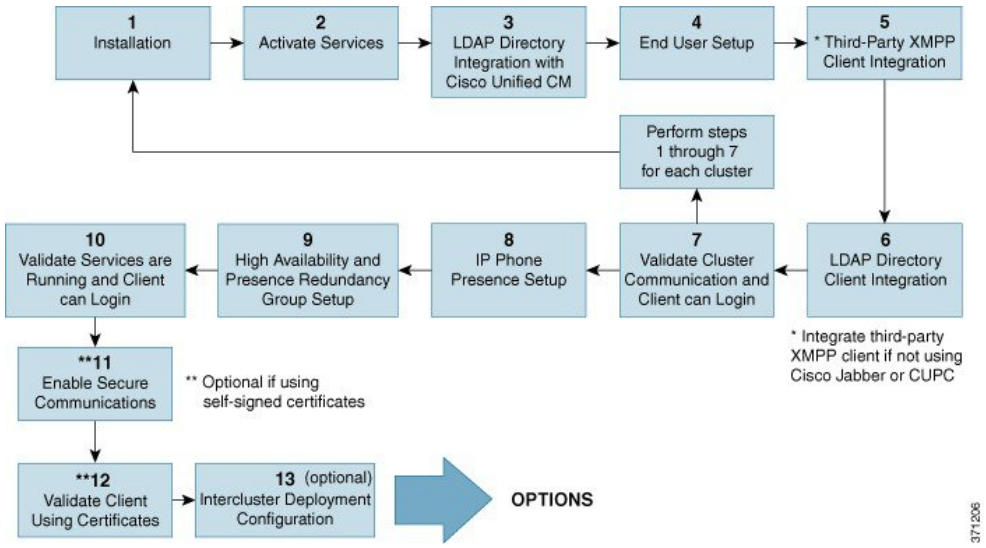
| | Task | Description |
|---|---|---|
| 7 | Validate Cluster Communications and Client can Login | Confirm that IM and availability can be exchanged within the cluster. Verify that IM's can be sent and received, and that changes in a user's availability can be seen. When more than one cluster is setup, validate basic IM and availability across clusters. |
| 8 | High Availability and Presence Redundancy Group Setup | For instructions to set up high availability and presence redundancy groups, see the *Cisco Unified Communications Manager Administration Guide*. |
| 9 | Validate Services are Running and Client can Login | Perform validate tasks to ensure services are running. Confirm that the client can login to IM and Presence Service and has availability. |
| 10 | Enable Secure Communications | Perform the following tasks to enable secure communications on the IM and Presence Service node:<br>• Configure certificate exchange between IM and Presence Service and Cisco Unified Communications Manager.<br>• Upload CA signed certificates to IM and Presence Service.<br>• Configure SIP security settings on IM and Presence Service for the TLS peer subject.<br>• (Optional) Configure XMPP security settings on IM and Presence Service. |
| 11 | Validate Client using certificates | Confirm that the client can login to IM and Presence Service and has availability. |

# Basic Deployment with High Availability and IP Phone Presence Workflow

The following workflow diagram shows the high-level steps to set up a basic IM and Presence Service deployment with High Availability and IP phone presence. Users have access to the core IM and availability features, such as basic IM functionality, presence, and Ad Hoc group chats after a basic setup. Optional features can be configured to enhance user functionality.

Optional features can also be configured to enhance user functionality. For more information about feature options or other deployment workflows, see topics related to features and options for IM and Presence Service and High Availability deployment setup.

*Figure 4: Basic IM and Presence Service Workflow with High Availability and IP Phone Presence*




The following table describes each task in the workflow.

*Table 5: Task List for Basic Workflow with High Availability and IP Phone Presence*

| | Task | Description |
|---|---|---|
| 1 | Installation | For detailed Installation instructions, see *Installing Cisco Unified Communications Manager*. |
| 2 | Activate Services | You must manually activate feature services after you install the node. For detailed instructions, see *Installing Cisco Unified Communications Manager*.<br>**Tip** Network services start automatically after you install the node. |
| 3 | LDAP Directory Integration with Cisco Unified Communications Manager | Set up LDAP directory integration on the IM and Presence Service node:<br>• Secure the Cisco Unified Communications Manager and LDAP directory connection.<br>• Secure the connection between IM and Presence Service and the LDAP server.<br>**Tip** Integration of Cisco Unified Communications Manager and Cisco Jabber with the LDAP server is the recommended setup. For alternative setups, see topics related to LDAP integration. |

| | Task | Description |
|---|---|---|
| 4 | End User Setup | Assign users to nodes and presence redundancy groups in yourIM and Presence Service deployment. You can manually or automatically assign users to the nodes in your IM and Presence Service deployment. See the *Cisco Unified Communications Manager Administration Guide* for instructions to assign users. The **User Assignment Mode for Presence Server Enterprise Parameter** is used to set the user assignment mode to balanced, active-stand-by, or none.<br>**Tip** Use the IM and Presence Service GUI to migrate users, export and import contact lists. |
| 5 | Third-Party XMPP Client Integration | (Optional) Integrate your third-party XMPP client if you are not using Cisco Jabber. |
| 6 | LDAP Directory Client Integration | Setup user integration with the LDAP directory:<br>• Configure LDAP synchronization for user provisioning.<br>• Upload LDAP server certificates.<br>• Configure LDAP user authentication.<br>**Tip** Integration of Cisco Unified Communications Manager and Cisco Jabber with the LDAP server is the recommended setup. For alternative setups, see topics related to LDAP integration. |
| 7 | Validate Cluster Communications and Client can Login | Confirm that IM and availability can be exchanged within the cluster. Verify that IM's can be sent and received, and that changes in a user's availability can be seen. When more than one cluster is setup, validate basic IM and availability across clusters. |
| 8 | IP Phone Presence Setup | Set up the following on IM and Presence Service node:<br>• Static routes<br>• Presence Gateway<br>• SIP publish trunk<br>• Cluster-wide DNS SRV name for SIP publish trunk |
| 9 | High Availability and Presence Redundancy Group Setup | For instructions to set up high availability and presence redundancy groups, see the *Cisco Unified Communications Manager Administration Guide*. |
| 10 | Validate Services are Running and Client can Login | Perform validate tasks to ensure services are running. Confirm that the client can login to IM and Presence Service and has availability. |

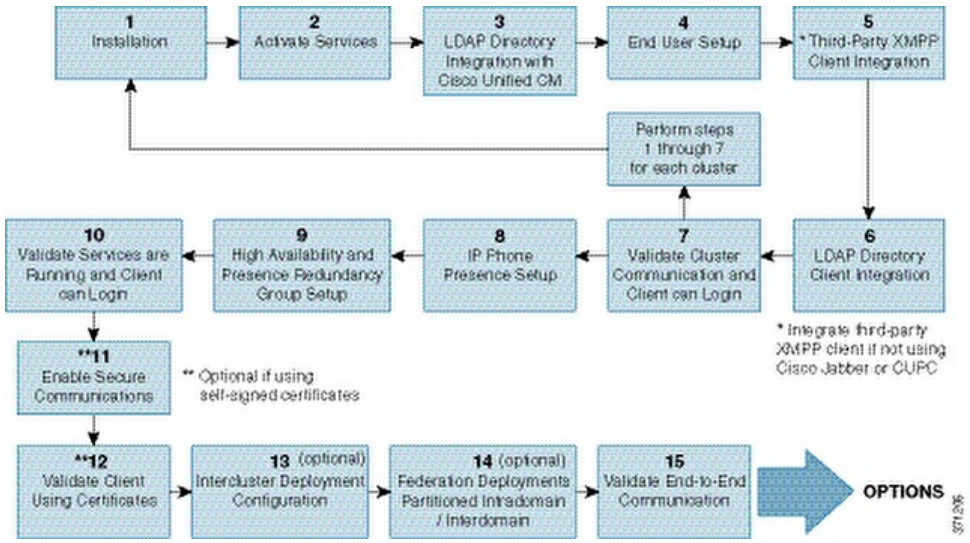
| | Task | Description |
|---|---|---|
| 11 | Enable Secure Communications | Perform the following tasks to enable secure communications on the IM and Presence Service node:<br>• Configure certificate exchange between IM and Presence Service and Cisco Unified Communications Manager.<br>• Upload CA signed certificates to IM and Presence Service.<br>• Configure SIP security settings on IM and Presence Service for the TLS peer subject.<br>• (Optional) Configure XMPP security settings on IM and Presence Service. |
| 12 | Validate Client using certificates | Confirm that the client can login to IM and Presence Service and has availability. |
| 13 | Intercluster Deployment Configuration | Configure your intercluster peer relationships, router to router connections, and set the node name and IM address scheme. |

# Federation Deployment Workflow

The following workflow diagram shows the high-level steps to set up IM and Presence Service deployment with High Availability and IP phone presence for a Federation deployment. For detailed instructions to configure federation, see the *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager* guide and the *Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager* guide.

Users have access to the core IM and availability features, such as basic IM functionality, presence, and Ad Hoc group chats after a basic setup. Optional features can be configured to enhance user functionality. For more information about feature options, see topics related to features and options for IM and Presence Service.

*Figure 5: IM and Presence Service Workflow for Federation Deployment*




The following table describes each task in the workflow.

*Table 6: Task List for IM and Presence Service Workflow for Federation*

| | Task | Description |
|---|---|---|
| 1 | Installation | For detailed Installation instructions, see *Installing Cisco Unified Communications Manager*. |
| 2 | Activate Services | You must manually activate feature services after you install the node. For detailed instructions, see *Installing Cisco Unified Communications Manager*.<br>**Tip** Network services start automatically after you install the node. |
| 3 | LDAP Directory Integration with Cisco Unified Communications Manager | Set up LDAP directory integration on the IM and Presence Service node:<br>• Secure the Cisco Unified Communications Manager and LDAP directory connection.<br>• Secure the connection between IM and Presence Service and the LDAP server.<br>**Tip** Integration of Cisco Unified Communications Manager and Cisco Jabber with the LDAP server is the recommended setup. For alternative setups, see topics related to LDAP integration. |

| | Task | Description |
|---|---|---|
| 4 | End User Setup | Assign users to nodes and presence redundancy groups in yourIM and Presence Service deployment. You can manually or automatically assign users to the nodes in your IM and Presence Service deployment. See the *Cisco Unified Communications Manager Administration Guide* for instructions to assign users. The **User Assignment Mode for Presence Server Enterprise Parameter** is used to set the user assignment mode to balanced, active-stand-by, or none.<br>**Tip** Use the IM and Presence Service GUI to migrate users, export and import contact lists. |
| 5 | Third-Party XMPP Client Integration | (Optional) Integrate your third-party XMPP client if you are not using Cisco Jabber or Cisco Unified Communications Manager. |
| 6 | LDAP Directory Client Integration | Setup user integration with the LDAP directory:<br>• Configure LDAP synchronization for user provisioning.<br>• Upload LDAP server certificates.<br>• Configure LDAP user authentication.<br>**Tip** Integration of Cisco Unified Communications Manager and Cisco Jabber with the LDAP server is the recommended setup. For alternative setups, see topics related to LDAP integration. |
| 7 | Validate Cluster Communications | Confirm that IM and availability can be exchanged within the cluster. Verify that IM's can be sent and received, and that changes in a user's availability can be seen. When more than one cluster is setup, validate basic IM and availability across clusters. |
| 8 | IP Phone Presence Setup | Set up the following on IM and Presence Service node:<br>• Static routes<br>• Presence Gateway<br>• SIP publish trunk<br>• Cluster-wide DNS SRV name for SIP publish trunk |
| 9 | High Availability and Presence Redundancy Group Setup | For instructions to set up high availability and presence redundancy groups, see the *Cisco Unified Communications Manager Administration Guide*. |
| 10 | Validate Services are Running and Client can Login | Perform validate tasks to ensure services are running. Confirm that the client can login to IM and Presence Service and has availability. |

| | Task | Description |
|---|---|---|
| 11 | Enable Secure Communications | Perform the following tasks to enable secure communications on the IM and Presence Service node:<br>• Configure certificate exchange between IM and Presence Service and Cisco Unified Communications Manager.<br>• Upload CA signed certificates to IM and Presence Service.<br>• Configure SIP security settings on IM and Presence Service for the TLS peer subject.<br>• (Optional) Configure XMPP security settings on IM and Presence Service. |
| 12 | Validate Client using certificates | Confirm that the client can login to IM and Presence Service and has availability. |
| 13 | Intercluster Deployment Configuration | Configure your intercluster peer relationships, router to router connections, and set the node name and IM address scheme. |
| 14 | Federation Deployments | Configure Interdomain Federation or Partitioned Intradomain Federation for your deployment. For instructions and requirements, see *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager* and *Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager*. |
| 15 | Validate End-to-End Communication | Perform validation tasks to confirm end-to-end communications. Confirm that IM and availability can be exchanged across clusters. Verify that IM's can be sent and received, and that changes in a user's availability can be seen. |

# IM-Only Deployment Workflow

This section describes the required configuration for an IM-only IM and Presence Service deployment.

**Note** Enhanced IM addressing options are available for IM-only IM and Presence Service deployments.

The following table describes the tasks to configure an IM-only deployment.

***Table 7: Task List for IM-Only IM and Presence Service Deployment***

| Task | Description |
|---|---|
| Create and license your users for IM and Presence Service on Cisco Unified Communications Manager | See the Cisco Unified Communications Manager documentation at this URL:<br>http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html |

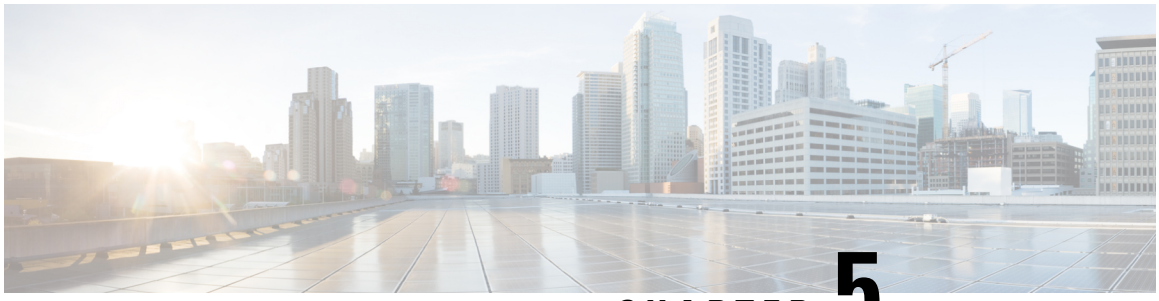
| Task | Description |
| --- | --- |
| Integrate the LDAP server for Cisco Jabber | Configure the LDAP settings on IM and Presence Service to allow Cisco Jabber users to search for contacts from the LDAP directory.<br>**Note** You should create an LDAP profile and verify LDAP attribute mappings, even if your Cisco Jabber client does not currently integrate with LDAP profiles on IM and Presence Service. |

See the appropriate Cisco Jabber client documentation for more information about directory requirements and setup.

PART II

# System Configuration


- Cisco Unified Communications Manager configuration for integration with IM and Presence Service, on page 49
- IM and Presence Service Network Setup, on page 57
- IP Phone Presence Setup , on page 79
- LDAP Directory Integration, on page 87
- Security Configuration on IM and Presence Service, on page 99
- Intercluster Peer Configuration, on page 127



CHAPTER 5

# Cisco Unified Communications Manager configuration for integration with IM and Presence Service


- User and Device Configuration on Cisco Unified Communications Manager before Integration Task List, on page 49
- Configure Inter-Presence Group Subscription Parameter, on page 51
- SIP Trunk Configuration on Cisco Unified Communications Manager, on page 51
- Verify Required Services Are Running on Cisco Unified Communications Manager, on page 55


## User and Device Configuration on Cisco Unified Communications Manager before Integration Task List

Before you configure Cisco Unified Communications Manager for integration with the IM and Presence Service, make sure that the following user and device configuration is completed on Cisco Unified Communications Manager.

*Table 8: Task List to Configure Users and Devices on Cisco Unified Communications Manager Before Integration with IM and Presence Service*

| Task | Description |
|---|---|
| Modify the User Credential Policy | This procedure is applicable only if you are integrating with Cisco Unified Communications Manager Release 6.0 or later.<br><br>Cisco recommends that you set an expiration date on the credential policy for users. The only type of user that does not require a credential policy expiration date is an Application user.<br><br>Cisco Unified Communications Manager does not use the credential policy if you are using an LDAP server to authenticate your users on Cisco Unified Communications Manager.<br><br>**Cisco Unified CM Administration** > **User Management** > **Credential Policy Default** |
| Configure the phone devices, and associate a Directory Number (DN) with each device | Check **Allow Control of Device from CTI** to allow the phone to interoperate with the client.<br><br>**Cisco Unified CM Administration** > **Device** > **Phone** |
| Configure the users, and associate a device with each user | Ensure that the user ID value is unique for each user.<br><br>**Cisco Unified CM Administration** > **User Management** > **End User**. |
| Associate a user with a line appearance | This procedure is applicable only to Cisco Unified Communications Manager Release 6.0 or later.<br><br>**Cisco Unified CM Administration** > **Device** > **Phone** |
| Add users to CTI-enabled user group | To enable desk phone control, you must add the users to a CTI-enabled user group.<br><br>**Cisco Unified CM Administration** > **User Management** > **User Group** |
| (Optional) Set directoryURI value for users | If the IM and Presence Service nodes are using the Directory URI IM address scheme, you must set the directoryURI value for the users. The user's Directory URI value can either be synchronized to the Cisco Unified Communications Manager LDAP Directory or manually updated.<br><br>See the *Cisco Unified Communications Manager Administration Guide* for instructions to enable LDAP or to edit the Directory URI value manually for the user if LDAP is not enabled. |

**Note** Because menu options and parameters may vary by Cisco Unified Communications Manager releases, see the Cisco Unified Communications Manager documentation that applies to your release.

**Related Topics**

LDAP Directory Integration, on page 87

# Configure Inter-Presence Group Subscription Parameter

You enable the Inter-Presence Group Subscription parameter to allow users in one Presence Group to subscribe to the availability information for users in a different presence group.

Restriction

You can only enable the Inter-Presence Group Subscription parameter when the subscription permission for the default Standard Presence Group, or any new Presence Groups, is set to **Use System Default**. To configure Presence Groups, choose **Cisco Unified CM Administration** > **System** > **Presence Groups**.

### Procedure

**Step 1** Choose **Cisco Unified CM Administration** > **System** > **Service Parameters**.

**Step 2** Choose a Cisco Unified Communications Manager node from the Server menu.

**Step 3** Choose **Cisco CallManager** from the Service menu.

**Step 4** Choose **Allow Subscription** for Default Inter-Presence Group Subscription in the Clusterwide Parameters (System - Presence) section.

**Step 5** Click **Save**.

**Tip** You no longer have to manually add the IM and Presence Service as an Application Server on Cisco Unified Communications Manager:

### What to do next

Proceed to configure a SIP trunk on Cisco Unified Communications Manager.

# SIP Trunk Configuration on Cisco Unified Communications Manager

The port number that you configure for the SIP Trunk differs depending on the version of the IM and Presence Service that you are deploying. For IM and Presence Service release 9.0(x) and later, configure the port number 5060 for the SIP Trunk.

# Configure SIP Trunk Security Profile for IM and Presence Service

### Procedure

**Step 1** Choose **Cisco Unified CM Administration** > **System** > **Security** > **SIP Trunk Security Profile**.

**Step 2** Click **Find.**

**Step 3** Click **Non Secure SIP Trunk Profile**.

**Step 4** Click **Copy** and enter CUP Trunk in the **Name** field.

**Step 5** Verify that the setting for Device Security Mode is **Non Secure**.

**Step 6** Verify that the setting for Incoming Transport Type is **TCP+UDP**.

**Step 7** Verify that the setting for Outgoing Transport Type is **TCP**.

**Step 8** Check to enable these items:

- **Accept Presence Subscription**
- Accept Out-of-Dialog REFER
- Accept Unsolicited Notification
- Accept Replaces Header

**Step 9** Click **Save**.

### What to do next

Proceed to configure the SIP trunk on Cisco Unified Communication Manager

# Configure SIP Trunk for IM and Presence Service

You only configure one SIP trunk between a Cisco Unified Communications Manager cluster and an IM and Presence Service cluster. After you configure the SIP trunk, you must assign that SIP trunk as the IM and Presence PUBLISH Trunk on Cisco Unified Communications Manager by choosing **Cisco Unified CM Administration** > **System** > **Service Parameters**.

In the Destination Address field, enter a value using one of the following formats:

- Dotted IP Address
- Fully Qualified Domain Name (FQDN)
- DNS SRV

If high availability is configured for the IM and Presence cluster, multiple entries should be entered in the Dotted IP Address or FQDN to identify the various nodes in the cluster. DNS SRV cannot be used for an IM and Presence cluster if high availability is configured.

### Before you begin

- Configure the SIP Trunk security profile on Cisco Unified Communications Manager.

- Read the Presence Gateway configuration options topic.

### Procedure

**Step 1** Choose **Cisco Unified CM Administration** > **Device** > **Trunk**.

**Step 2** Click **Add New**.

**Step 3** Choose **SIP Trunk** from the Trunk Type menu.

**Step 4** Choose **SIP** from the Device Protocol menu.

**Step 5** Choose **None** for the Trunk Service Type.

**Step 6** Click **Next**.

**Step 7** Enter **CUPS-SIP-Trunk** for the Device Name.

**Step 8** Choose a device pool from the Device Pool menu.

**Step 9** In the SIP Information section at the bottom of the window, configure the following values:

a) In the Destination Address field, enter the Dotted IP Address, or the FQDN, which can be resolved by DNS and must match the SRV Cluster Name configured on the IM and Presence node.

b) Check the **Destination Address is an SRV** if you are configuring a multinode deployment.

In this scenario, Cisco Unified Communications Manager performs a DNS SRV record query to resolve the name, for example *_sip._tcp.hostname.tld*. If you are configuring a single-node deployment, leave this checkbox unchecked and Cisco Unified Communications Manager will perform a DNS A record query to resolve the name, for example *hostname.tld*.

Cisco recommends that you use the IM and Presence Service default domain as the destination address of the DNS SRV record.

**Note** You can specify any domain value as the destination address of the DNS SRV record. No users need to be assigned to the domain that is specified. If the domain value that you enter differs from the IM and Presence Service default domain, you must ensure that the SIP Proxy Service Parameter called SRV Cluster Name on IM and Presence Service matches the domain value that you specify in the DNS SRV record. If you use the default domain, then no changes are required to the SRV Cluster Name parameter.

In both scenarios, the Cisco Unified Communications SIP trunk Destination Address must resolve by DNS and match the SRV Cluster Name configured on the IM and Presence node.

c) Enter `5060` for the Destination Port.

d) Choose **Non Secure SIP Trunk Profile** from the SIP Trunk Security Profile menu.

e) Choose **Standard SIP Profile** from the SIP Profile menu.

**Step 10** Click **Save**.

Troubleshooting Tip

If you modify the DNS entry of the Publish SIP Trunk SRV record by changing the port number or IP address, you must restart all devices that previously published to that address and ensure each device points to the correct IM and Presence Service contact.

### Related Topics

Configure Cluster-Wide DNS SRV Name for SIP Publish Trunk, on page 85

Configure SIP Trunk Security Profile for IM and Presence Service, on page 52
Configure SIP Publish Trunk on IM and Presence Service, on page 85
Presence Gateway Configuration Option, on page 84

# Configure Phone Presence for Unified Communications Manager Outside of Cluster

You can allow phone presence from a Cisco Unified Communications Manager that is outside of the IM and Presence Service cluster. Default requests from a Cisco Unified Communications Manager that is outside of the cluster will not be accepted by IM and Presence Service. You can also configure a SIP Trunk on Cisco Unified Communications Manager.

You must configure the TLS context before you configure the TLS peer subject.

## Configure TLS Peer Subject

In order for the IM and Presence Service to accept a SIP PUBLISH from a Cisco Unified Communications Manager outside of its cluster, the Cisco Unified Communications Manager needs to be listed as a TLS Trusted Peer of the IM and Presence Service.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Security** > **TLS Peer Subjects**.

**Step 2** Click **Add New**.

**Step 3** Enter the IP Address of the external Cisco Unified Communications Manager in the **Peer Subject Name** field.

**Step 4** Enter the name of the node in the **Description** field.

**Step 5** Click **Save**.

### What to do next

Configure the TLS context.

## Configure TLS Context

Use the following procedure to configure TLS context.

### Before you begin

Configure the TLS peer subject.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence AdministrationSystemSecurityTLS Context Configuration**.

**Step 2** Click **Find**.

**Step 3** Click **Default_Cisco_UP_SIP_Proxy_Peer_Auth_TLS_Context**.

**Step 4** From the list of available TLS peer subjects, choose the TLS peer subject that you configured.

**Step 5** Move this TLS peer subject to Selected TLS Peer Subjects.

**Step 6** Click **Save**.

**Step 7** Restart the OAMAgent.

**Step 8** Restart the Cisco Presence Engine.

**Tip** You must restart in this order for the changes to take effect.

# Verify Required Services Are Running on Cisco Unified Communications Manager

You can view, start, and stop Cisco Unified Communications Manager services from a Cisco Unified Communications Manager node or an IM and Presence Service node. The following procedure provides steps to follow on a Cisco Unified Communications Manager node. To view Cisco Unified Communications Manager services from an IM and Presence Service node, choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Service Activation**.

### Procedure

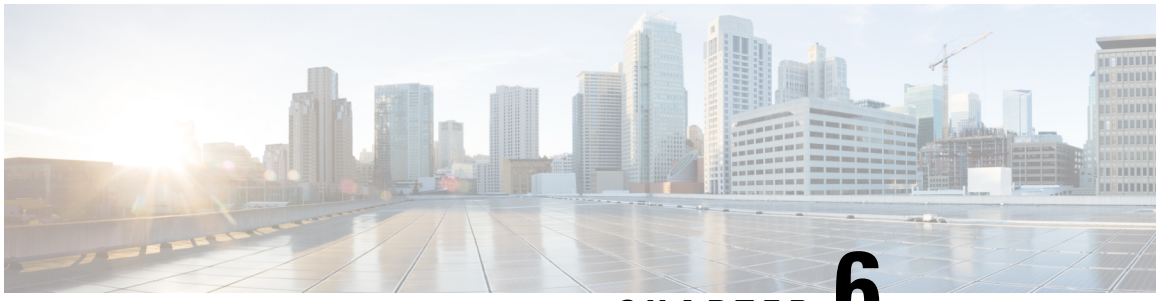
**Step 1** On Cisco Unified Communications Manager, choose **Cisco Unified Serviceability** > **Tools** > **Control Center - Feature Services**.

**Step 2** Choose a Cisco Unified Communications Manager node from the Server menu.

**Step 3** Make sure that the following services are running:

- Cisco CallManager
- Cisco TFTP
- Cisco CTIManager
- Cisco AXL Web Service (for data synchronization between IM and Presence and Cisco Unified Communications Manager)

**Tip** To turn on a service on Cisco Unified Communications Manager, choose **Cisco Unified Serviceability** > **Tools** > **Service Activation.**



CHAPTER 6

# IM and Presence Service Network Setup


- Configuration changes and service restart notifications, on page 57
- DNS Domain Configuration, on page 58
- IM and Presence Service Default Domain Configuration, on page 62
- IM Address Configuration, on page 63
- Domain Management for IM and Presence Service Clusters, on page 68
- Routing Information Configuration on IM and Presence Service, on page 71
- IPv6 Configuration, on page 74
- Configure Proxy Server Settings, on page 77
- Services on IM and Presence Service, on page 78


# Configuration changes and service restart notifications

## Service Restart Notifications

If you make a configuration change in Cisco Unified CM IM and Presence Administration that impacts an IM and Presence XCP service, you will need to restart XCP services for your changes to take effect. IM and Presence Service notifies you of exactly which node the configuration change impacts and of any service that you must restart. An Active Notifications popup window displays on each page of Cisco Unified CM IM and Presence Administration to serve as a visual reminder that you must restart services. Use your mouse to hover over the dialog bubble icon to see the list of active notifications (if any) and associated severity levels. From the list of active notifications you can go directly to Cisco Unified IM and Presence Serviceability, where you can restart the required service.

It is good practice to monitor the service restart popup window for service restart notifications, particularly if you make configuration changes after you deploy IM and Presence Service in the network. Most tasks in the accompanying documentation indicate if service restarts are required.

See the Online Help topic on Service Restart Notifications for information about the types of service notifications, and the service notification security levels.

## Cisco XCP Router Restart

The Cisco XCP Router must be running for all availability and messaging services to function properly on IM and Presence Service. This applies to both SIP-based and XMPP-based client messaging. If you restart the Cisco XCP Router, IM and Presence Service automatically restarts all active XCP services.

The topics in this module indicate if you need to restart the Cisco XCP Router following a configuration change. Note that you must restart the Cisco XCP Router, not turn off and turn on the Cisco XCP Router. If you turn off the Cisco XCP Router, rather than restart this service, IM and Presence Service stops all other XCP services. Subsequently when you then turn on the XCP router, IM and Presence Service will not automatically turn on the other XCP services; you need to manually turn on the other XCP services.

# Restart Cisco XCP Router Service

### Procedure

**Step 1** On IM and Presence Service, choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Network Services**.

**Step 2** Choose the node from the Server list box and select **Go**.

**Step 3** Click the radio button next to the Cisco XCP Router service in the IM and Presence Service section.

**Step 4** Click **Restart**.

**Step 5** Click **OK** when a message indicates that restarting may take a while.

# DNS Domain Configuration

The Cisco Unified Communications Manager IM and Presence Service supports flexible node deployment across any number of DNS domains. To support this flexibility, all IM and Presence Service nodes within the deployment must have a node name set to that node's Fully Qualified Domain Name (FQDN). Some sample node deployment options are described below.

**Note** If any IM and Presence Service node name is based on the hostname only, then all IM and Presence Service nodes must share the same DNS domain.

There is no requirement that the IM and Presence Service default domain or any other IM domain that is hosted by the system to align with the DNS domain. An IM and Presence Service deployment can have a common presence domain, while having nodes deployed across multiple DNS domains.

**Note** If you have Cisco Jabber connected over VPN, during the TLS handshake between the IM and Presence Service and the Cisco Jabber client, the IM and Presnece server performs a reverse lookup for the client's IP subnet. If the reverse lookup fails, the TLS handshake times out in the client machine.

For more information, see *Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service*.

### Related Topics

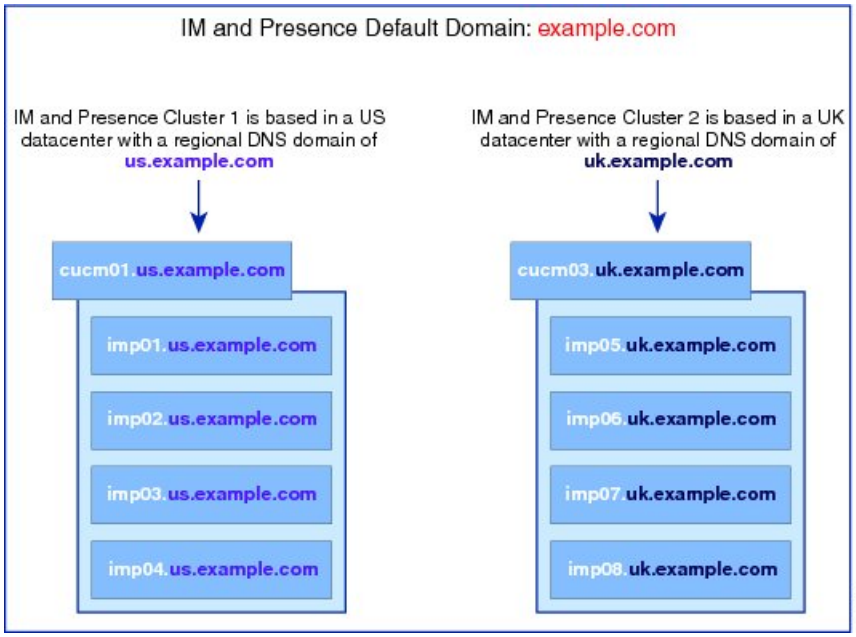
Specify DNS Domain Associated with Cisco Unified Communications Manager Cluster, on page 61
IM and Presence Service Default Domain Configuration

Node Name Recommendations

# IM and Presence Service Clusters Deployed in Different DNS Domain or Subdomains

IM and Presence Service supports having the nodes associated with one IM and Presence Service cluster in a different DNS domain or subdomain to the nodes that form a peer IM and Presence Service cluster. The diagram below highlights a sample deployment scenario that is supported.

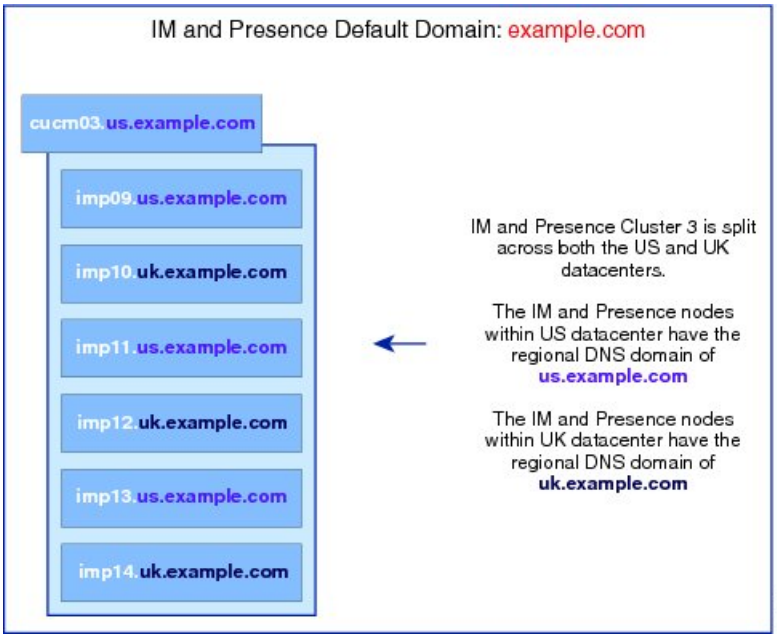
***Figure 6: IM and Presence Service Clusters Deployed in Different DNS Domain or Subdomains***




# IM and Presence Service Nodes Within Cluster Deployed in Different DNS Domains or Subdomains

IM and Presence Service supports having the nodes within any IM and Presence Service cluster deployed across multiple DNS domains or subdomains. The diagram below highlights a sample deployment scenario that is supported.

*Figure 7: IM and Presence Service Nodes Within a Cluster Deployed in Different DNS Domains or Subdomains*

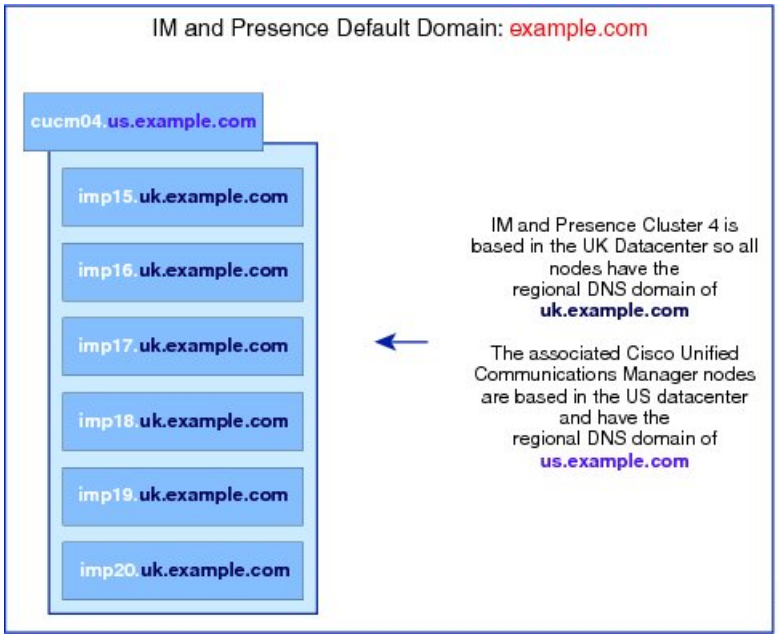



**Note** High availability is also fully supported in scenarios where the two nodes within a presence redundancy group are in different DNS domains or subdomains.

# IM and Presence Service Nodes Within Cluster Deployed in DNS Domain That is Different Than the Associated Cisco Unified Communications Manager Cluster

IM and Presence Service supports having the IM and Presence Service nodes in a different DNS domain to their associated Cisco Unified Communications Manager cluster. The diagram below highlights a sample deployment scenario that is supported.

*Figure 8: IM and Presence Service Nodes Within a Cluster Deployed in a DNS Domain That is Different Than the Associated Cisco Unified Communications Manager Cluster*




**Note** To support Availability Integration with Cisco Unified Communications Manager, the **CUCM Domain** SIP Proxy service parameter must match the DNS domain of the Cisco Unified Communications Manager cluster.

By default, the CUCM Domain SIP Proxy service parameter is set to the DNS domain of the IM and Presence database publisher node. Therefore, if the DNS domain of the IM and Presence database publisher node differs from the DNS domain of the Cisco Unified Communications Manager cluster, you must update this service parameter using the Cisco Unified CM IM and Presence Administration GUI on the IM and Presence database publisher node. Refer to the topic *Specify DNS domain associated with Cisco Unified Communications Manager* for more information.

# Specify DNS Domain Associated with Cisco Unified Communications Manager Cluster

**Note** This procedure is required only if the DNS domain of the IM and Presence database publisher node differs from that of the Cisco Unified Communications Manager nodes.

IM and Presence Service maintains Access Control List (ACL) entries for all Cisco Unified Communications Manager nodes within the cluster. This enables seamless sharing of Availability between the nodes. These ACL entries are FQDN based and are generated by appending the Cisco Unified Communications Manager hostname to the DNS domain of the IM and Presence database publisher node.

If the DNS domain of the IM and Presence database publisher node differs from that of the Cisco Unified Communications Manager nodes, then invalid ACL entries will be added. To avoid this, you must perform

the following procedure from the Cisco Unified CM IM and Presence Administration GUI of the IM and Presence database publisher node.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters.**

**Step 2** From the **Server** drop-down list, choose the IM and Presence Service node.

**Step 3** From the **Service** drop-down list, choose **Cisco SIP Proxy**.

**Step 4** Edit the **CUCM Domain** field in the General Proxy Parameters (Clusterwide) section to match the DNS domain of the Cisco Unified Communications Manager nodes.

By default this parameter is set to the DNS domain of the IM and Presence database publisher node.

**Step 5** Click **Save**.

### Related Topics

DNS Domain Configuration, on page 58

# IM and Presence Service Default Domain Configuration

Follow this procedure if you want to change the default domain value for IM and Presence Service within a cluster. This procedure is applicable if you have a DNS or non-DNS deployment.

**Caution** Disable high availability for the presence redundancy group before you stop any services as part of this procedure. If you stop the services while high availability is enabled, a system failover occurs.

This procedure changes only the default domain of the IM and Presence Service cluster. It does not change the DNS domain associated with any IM and Presence Service node within that cluster. For instructions on how to change the DNS domain of an IM and Presence Service node, see *Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service*.

**Note** The default domain is configured when you add an IM and Presence Service publisher node to Cisco Unified Communications Manager. If the system fails to retrieve the default domain value from the Cisco Unified Communications Manager during node installation, the default domain value is reset to DOMAIN.NOT.SET. Use this procedure to change the IM and Presence Service default domain value to a valid domain value.

### Procedure

**Step 1** Stop the following services on all IM and Presence Service nodes in your cluster in the order listed:

- Cisco Client Profile Agent
- Cisco XCP Router

**Note** When you stop the Cisco XCP Router, all XCP feature service is automatically stopped.

- Cisco Sync Agent
- Cisco SIP Proxy
- Cisco Presence Engine

**Step 2** On the IM and Presence Service database publisher node, perform the following steps to configure the new domain value:

a) Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Settings** > **Advanced Configuration**.
b) Choose **Default Domain**.
c) In the **Domain Name** field, enter the new presence domain and click **Save**.

A system update can take up to 1 hour to complete. If the update fails, the **Re-try** button appears. Click **Re-try** to reapply the changes or click **Cancel**.

**Step 3** On all nodes in the cluster, manually start all services that had been stopped at the beginning of this procedure.

On every node in the cluster, manually restart any XCP feature services that were previously running.

# IM Address Configuration

## IM Address Configuration Requirements

The IM and Presence Service default domain and the IM address scheme that you use must be consistent across all IM and Presence Service clusters. The IM address scheme you set affects all user JIDs and cannot be performed in a phased manner without disrupting communication between clusters which may have different settings.

If any of the deployed clients do not support directory URI as the IM address, administrators should disable the directory URI IM address scheme.

The following services must be stopped on all nodes in the cluster before you can configure the IM address scheme:

- Cisco Client Profile Agent
- Cisco XCP Router
- Cisco Sync Agent
- Cisco SIP Proxy
- Cisco Presence Engine

See the interactions and restrictions topics for detailed requirements that are specific to each of the IM address schemes, and see the IM address configuration planning topics for additional information before you configure the IM address on IM and Presence Service.

## UserID@Default_Domain IM Address Interactions and Restrictions

The following restrictions apply to the *UserID@Default_Domain* IM address scheme:

- All IM addresses are part of the IM and Presence default domain, therefore, multiple domains are not supported.
- The IM address scheme must be consistent across all IM and Presence Service clusters.
- The default domain value must be consistent across all clusters.
- If *userid* is mapped to an LDAP field on Cisco Unified Communications Manager, that LDAP mapping must be consistent across all clusters.

## Directory URI IM Address Interactions and Restrictions

To support multiple domain configurations, you must set Directory URI as the IM address scheme for IM and Presence Service.

**Caution** If you configure the node to use Directory URI as the IM address scheme, Cisco recommends that you deploy only clients that support Directory URI. Any client that does not support Directory URI will not work if the Directory URI IM address scheme is enabled. Cisco recommends that you use the *UserID@Default_Domain* IM address scheme and not the Directory URI IM address scheme if you have any deployed clients that do not support Directory URI.

Observe the following restrictions and interactions when using the Directory URI IM address scheme:

- All users have a valid Directory URI value configured on Cisco Unified Communications Manager.
- All deployed clients must support Directory URI as the IM address and use either EDI-based or UDS-based directory integration.

  **Note** For UDS-based integration with Jabber, you must be running at least release 10.6 of Jabber.

- The IM address scheme must be consistent across all IM and Presence Service clusters.
- All clusters must be running a version of Cisco Unified Communications Manager that supports the Directory URI addressing scheme.
- If LDAP Sync is disabled, you can set the Directory URI as a free-form URI. If LDAP Directory Sync is enabled, you can map the Directory URI to the email address (mailid) or the Microsoft OCS/Lync SIP URI (msRTCSIP-PrimaryUserAddress).
- The Directory URI IM address settings are global and apply to all users in the cluster. You cannot set a different Directory URI IM address for individual users in the cluster.

# Configure IM Address Task Flow

Complete the following tasks to configure IM addressing for your system.

**Note** If you only want to edit existing IM user addresses and you do not want to change the default domain or the IM addressing scheme, you can proceed to step 4.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Stop Services, on page 65 | You must stop essential IM and Presence services before updating your IM addressing configuration. |
| **Step 2** | Assign IM Addressing Scheme, on page 66 | Update your IM addressing configuration with new settings such as the default domain and IM addressing scheme. |
| **Step 3** | Restart Services, on page 67 | Restart essential IM and Presence services. You must restart services before updating user addresses or provisioning users. |
| **Step 4** | Update IM user addresses | Update IM user addresses by configuring the corresponding user settings in Cisco Unified Communications Manager. The IM addressing scheme that you configured determines which end user information derives the IM address.<br>For details, see the "End User Setup" chapter of the *Cisco Unified Communications Manager Administration Guide* at: http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html |

## Stop Services

Prior to updating your IM addressing scheme configuration stop essential IM and Presence Services. Make sure to stop services in the prescribed order.

### Before you begin

If you have High Availability (HA) configured, disable it before you stop services. Otherwise, a system failover will occur. To do this:

- In the **Presence Topology** window of the IM and Presence Service, take a record of the number of assigned users for each cluster node.
- In the **Presence Redundancy Group Configuration** window of Cisco Unified Communications Manager, disable high availability in the subcluster.
- After your changes, wait at least two minutes for the HA settings to sync across the cluster before you stop services.

For details on High Availability, see the 'Presence Redundancy Groups' chapter of the *System Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

### Procedure

**Step 1** From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center – Network Services**

**Step 2** Stop the following IM and Presence Services, in this order, by selecting the service and clicking the **Stop** button:

a) **Cisco Sync Agent**
b) **Cisco Client Profile Agent**

**Step 3** After both services have stopped, choose **Tools** > **Control Center – Feature Services** and stop the following services in this order:

a) **Cisco Presence Engine**
b) **Cisco SIP Proxy**

**Step 4** After both services have stopped, choose **Tools** > **Control Center – Feature Services** and stop the following service:

- Cisco XCP Router

**Note** When you stop the XCP Router service, all related XCP feature services stop automatically.

### What to do next

After services are stopped, you can update your IM addressing scheme.

Assign IM Addressing Scheme, on page 66

## Assign IM Addressing Scheme

Use this procedure to configure a new domain and IM address scheme, or to update an existing domain and address scheme.

**Note** Make sure that the IM addressing scheme that you configure is consistent across all clusters.

### Before you begin

Make sure to stop services before you configure an addressing scheme. For details, see:

Stop Services, on page 65

### Procedure

**Step 1** In Cisco Unified CM IM and Presence Administration, choose **Presence** > **Settings** > **Advanced Configuration**.

**Step 2** To assign a new default domain, check the **Default Domain** check box and, in the text box, enter the new domain.

**Step 3** To change the address scheme, check the **IM Address Scheme** check box, and select one of the following options from the drop-down list box:

- **UserID@[Default_Domain]**—Each IM user address is derived from the UserID along with the default domain. This is the default setting.
- **Directory URI**—Each IM user address matches the directory URI that is configured for that user in Cisco Unified Communications Manager.

**Step 4** Click **Save**.

If you chose Directory URI as the IM address scheme, you may be prompted to ensure that the deployed clients can support multiple domains. Click **OK** to proceed or click **Cancel**.

If any user has an invalid Directory URI setting, a dialog box appears. Click **OK** to proceed or click **Cancel**, and then fix the user settings before reconfiguring the IM address scheme.

A system update can take up to 1 hour to complete. Click **Re-try** to reapply the changes or click **Cancel**.

### What to do next

After your addressing scheme is assigned, you can restart services.

Restart Services, on page 67

## Restart Services

Once your IM addressing scheme is configured, restart services. You must do this prior to updating user address information or provisioning new users. Make sure to follow the prescribed order in starting services.

### Before you begin

Assign IM Addressing Scheme, on page 66

### Procedure

**Step 1** From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center – Network Services**.

**Step 2** Start the following service by selecting the service and clicking the **Start** button:

- **Cisco XCP Router**

**Step 3** After the service starts, choose **Tools** > **Control Center – Feature Services** and start the following services in this order:

a) **Cisco SIP Proxy**
b) **Cisco Presence Engine**

**Step 4** Confirm that the Cisco Presence Engine service is running on all nodes before proceeding to the next step.

**Step 5** Choose **Tools** > **Control Center – Network Services** and start the following services in this order:

a) **Cisco Client Profile Agent**

b) **Cisco Sync Agent**

### What to do next

Once services are up and running, you can update end user IM addresses. IM addresses are derived from user IDs or directory URIs that are provisioned in Cisco Unified Communications Manager depending on which IM address scheme you configured.

For details, see the "End User Setup" chapter of the *Cisco Unified Communications Manager Administration Guide* at: http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

# Domain Management for IM and Presence Service Clusters

You can manually add, update, and delete local IM address domains using the Cisco Unified CM IM and Presence Administration GUI.

The **IM and Presence Domain** window displays the following domains:

- Administrator-managed IM address domains. These are internal domains that are added manually but not yet assigned to any users, or they were added automatically by the Sync Agent but the user's domain has since changed and so it is no longer in use.
- System-managed IM address domains. These are internal domains that are in use by a user in the deployment and which can be added either manually or automatically.

If the domain appears in the **IM and Presence Domain** window, the domain is enabled. There is no enabling or disabling of domains.

The Cisco Sync Agent service performs a nightly audit and checks the Directory URI of each user on the local cluster, and on the peer cluster if interclustering is configured, and automatically builds a list of unique domains. A domain changes from being administrator managed to system managed when a user in the cluster is assigned that domain. The domain changes back to administrator managed when the domain is not in use by any user in the cluster.

**Note** All IM and Presence Service and Cisco Unified Communications Manager nodes and clusters must support multiple domains to use this feature. Ensure that all nodes in the IM and Presence Service clusters are operating using Release 10.0 or greater and that Directory URI IM addressing is configured.

# IM Domain Management Interactions and Restrictions

- You can add or delete only administrator-managed domains that are associated with the local cluster.
- You cannot edit system managed domains.

- You cannot edit system-managed or administrator managed domains that are associated with other clusters.
- It is possible to have a domain configured on two clusters, but in use on only the peer cluster. This appears as a system-managed domain on the local cluster, but is identified as being in use on only the peer cluster.
- Some security certificates may need to be regenerated after you manually add, update, or delete a domain. When generating a self-signed certificate or a certificate signing request (CSR), the Subject Common Name (CN) is set to the FQDN of the node, while the local IM and Presence default domain and all additional domains hosted by the system are added to the certificate as Subject Alt Names (SAN).
- For XMPP Federation over TLS, you must regenerate the TLS certificate if adding or removing an IM address domain.

# View IM Address Domains

All system-managed and administrator-managed presence domains across the IM and Presence Service deployment are displayed in the **Presence > Domains> Find and List Domains** window. A check mark in one of the information fields indicates if a domain is associated with the local cluster and/or with any peer clusters. The following information fields are displayed for administrator-managed presence domains:

- Domain
- Configured on Local Cluster
- Configured on Peer Cluster(s)

The following information fields are displayed for system-managed presence domains:

- Domain
- In use on Local Cluster
- In use on Peer Cluster(s)

### Procedure

Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Domains**. The **Find and List Domains** window appears.

# Add or Update IM Address Domains

You can manually add IM address domains to your local cluster and update existing IM address domains that are on your local cluster using Cisco Unified CM IM and Presence Administration GUI.

You can enter a domain name of up to a maximum of 255 characters and each domain must be unique across the cluster. Allowable values are any upper- or lowercase letter (a-zA-Z), any number (0-9), the hyphen (-), or the dot (.). The dot serves as a domain label separator. Domain labels must not start with a hyphen. The last label (for example, .com) must not start with a number. Abc.1om is an example of an invalid domain.

System-managed domains cannot be edited because they are in use. A system-managed domain automatically becomes an administrator-managed domain if there are no longer users on the system with that IM address domain (for example, if the users are deleted). You can edit or delete administrator-managed domains.

**Procedure**

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Domains**.

The **Find and List Domains** window appears displaying all administrator-managed and system-managed IM address domains.

**Step 2** Perform one of the following actions:

- Click **Add New** to add a new domain. The **Domains** window appears.
- Choose the domain to edit from the list of domains. The **Domains** window appears.

**Step 3** Enter a unique domain name up to a maximum of 255 characters in the **Domain Name** field, and then click **Save**.

**Tip** A warning message appears. If you are using TLS XMPP Federation, proceed to generate a new TLS certificate.

# Delete IM Address Domains

You can delete administrator-managed IM address domains that are in the local cluster using Cisco Unified CM IM and Presence Administration GUI.

System-managed domains cannot be deleted because they are in use. A system-managed domain automatically becomes an administrator-managed domain if there are no longer users on the system with that IM address domain (for example, if the users are deleted). You can edit or delete administrator-managed domains.

**Note** If you delete an administrator-managed domain that is configured on both local and peer clusters, the domain remains in the administrator-managed domains list; however, that domain is marked as configured on the peer cluster only. To completely remove the entry, you must delete the domain from all clusters on which it is configured.

**Procedure**

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Domains**.

The **Find and List Domains** window appears displaying all administrator-managed and system-managed IM address domains.

**Step 2** Choose the administrator-managed domains to delete using one of the following methods, and then click **Delete Selected**.

- Check the check box beside the domains to delete.
- Click **Select All** to select all domains in the list of administrator-managed domains.

**Tip** Click **Clear All** to clear all selections.

**Step 3** Click **OK** to confirm the deletion or click **Cancel**.

# Routing Information Configuration on IM and Presence Service

## Routing Communication Recommendations

Router-to-router communication is the default mechanism for establishing the XCP route fabric on IM and Presence Service. In this case, IM and Presence Service dynamically configure all router-to-router connections between nodes in a cluster. Choose this routing configuration type if not all the nodes in your cluster are in the same multicast domain. Note that when you choose router-to-router communication:

- Your deployment incurs the additional performance overhead while IM and Presence Service establishes the XCP route fabric.
- You do not need to restart the Cisco XCP Router on all nodes in your deployment when you add a new node.
- If you delete or remove a node, you must restart the Cisco XCP Router on all nodes in your deployment.

Alternatively, you can choose MDNS for your deployment. A requirement for MDNS routing is that all nodes in the cluster are in the same multicast domain. MDNS routing can seamlessly support new XCP routers joining the XCP route fabric.

If you choose MDNS as the routing communication, you must have multicast DNS enabled in your network. In some networks multicast is enabled by default or enabled in a certain area of the network, for example, in an area that contains the nodes that form the cluster. In these networks, you do not need to perform any additional configuration in your network to use MDNS routing. When multicast DNS is disabled in the network, MDNS packets cannot reach the other nodes in a cluster. If multicast DNS is disabled in your network, you must perform a configuration change to your network equipment to use MDNS routing.

## Configure MDNS Routing and Cluster ID

At installation, the system assigns a unique cluster ID to the IM and Presence database publisher node. The systems distributes the cluster ID so that all nodes in your cluster share the same cluster ID value. The nodes in the cluster use the cluster ID to identify other nodes in the multicast domain using MDNS. A requirement for MDNS routing is that the cluster ID value is unique to prevent nodes in one standalone IM and Presence Service cluster from establishing router-to-router connections with nodes in another standalone cluster. Standalone clusters should only communicate over intercluster peer connections.

Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Settings** > **Standard Configuration** to view or configure the cluster ID value for a cluster. If you change the cluster ID value, make sure that the value remains unique to your IM and Presence Service deployment.

**Note** If you deploy the Chat feature, IM and Presence Service uses the cluster ID value to define chat node aliases. There are certain configuration scenarios that may require you to change the cluster ID value. See the Group Chat module for details.

**Related Topics**

Chat Setup and Management, on page 177

# Configure Routing Communication

To allow the nodes in a cluster to route messages to each other, you must configure the routing communication type. This setting determines the mechanism for establishing router connections between nodes in a cluster. Configure the routing communication type on the IM and Presence database publisher node, and IM and Presence Service applies this routing configuration to all nodes in the cluster.

For single node IM and Presence Service deployments, we recommend that you leave the routing communication type at the default setting.

**Caution** You must configure the routing communication type before you complete your cluster configuration and start to accept user traffic into your IM and Presence Service deployment.

### Before you begin

- If you want to use MDNS routing, confirm that MDNS is enabled in your network.
- If you want to use router-to-router communication, and DNS is not available in your network, for each node you must configure the IP address as the node name in the cluster topology. To edit the node name, choose **Cisco Unified CM IM and Presence Administration** > **System** > **Presence Topology**, and click the edit link on a node. Perform this configuration after you install IM and Presence Service, and before you restart the Cisco XCP Router on all nodes.

**Attention** When using the Cisco Jabber client, certificate warning messages can be encountered if the IP address is configured as the IM and Presence Service node name. To prevent Cisco Jabber from generating certificate warning messages, the FQDN should be used as the node name.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters**.

**Step 2** Choose an IM and Presence Service node from the **Server** drop-down list.

**Step 3** Choose Cisco XCP Router from the **Service** drop-down list.

**Step 4** Choose one of these Routing Communication Types from the menu:

- **Multicast DNS (MDNS)** - Choose Multicast DNS communication if the nodes in your cluster are in the same multicast domain. Multicast DNS communication is enabled by default on IM and Presence Service.

- **Router to Router** - Choose Router-to-Router communication if the nodes in your cluster are not in the same multicast domain.

**Step 5** Click **Save**.

**Step 6** Restart the Cisco XCP Router service on all nodes in your deployment.

**Related Topics**

Restart Cisco XCP Router Service, on page 58

# Configure Cluster ID

At installation, the system assigns a default unique cluster ID to the IM and Presence database publisher node. If you configure multiple nodes in the cluster, the systems distributes the cluster ID so that each node in your cluster shares the same cluster ID value.

We recommend that you leave the cluster ID value at the default setting. If you do change the cluster ID value, note the following:

- If you choose MDNS routing, all nodes must have the same cluster ID to allow them to identify other nodes in the multicast domain.
- If you are deploying the Group Chat feature, IM and Presence Service uses the cluster ID value for chat node alias mappings, and there are certain configuration scenarios that may require you to change the cluster ID value. See the Group Chat module for details.

If you change the default Cluster ID value, you only need to make this change on the IM and Presence database publisher node, and the system replicates the new Cluster ID value to the other nodes in the cluster.

**Procedure**

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Settings** > **Standard Configuration**.

**Step 2** View or edit the Cluster ID value.

**Note** By default, IM and Presence Service assigns the cluster ID value “StandaloneCluster” to a cluster.

**Step 3** Click **Save**.

**Tip** IM and Presence Service does not permit the underscore character (_) in the Cluster ID value. Ensure the Cluster ID value does not contain this character.

**Related Topics**

Chat Setup and Management, on page 177

# Configure Throttling Rate for Availability State Change Messages

To prevent an overload of the on IM and Presence Service, you can configure the rate of availability (presence) changes sent to the Cisco XCP Router in messages per second. When you configure this value, IM and Presence Service throttles the rate of availability (presence) changes back to meet the configured value.

**Procedure**

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters.**

**Step 2** Choose the IM and Presence Service node from the Server menu.

**Step 3** Choose **Cisco Presence Engine** from the Service menu.

**Step 4** In the Clusterwide Parameters section, edit the **Presence Change Throttle Rate** parameter. This parameter defines the number of presence updates per second.

**Step 5** Click **Save**.

# IPv6 Configuration

To enable IPv6 for IM and Presence Service, you must perform the following tasks:

- Configure IPv6 on Eth0 for each IM and Presence Service node in the cluster using either the Cisco Unified IM and Presence OS Administration GUI or the Command Line Interface.
- Enable the IPv6 enterprise parameter for the IM and Presence Service cluster.

You must configure IPv6 for both the IM and Presence Service enterprise network and for Eth0 on each IM and Presence Service node for IPv6 to be used; otherwise, the system attempts to use IPv4 for IP traffic. For example, if the enterprise parameter is set to IPv6 and only one of two nodes in the cluster has their Eth0 port set for IPv6, then only the node with the port set to IPv6 is enabled for IPv6. The other node will attempt to use IPv4.

For configuration changes to the IPv6 enterprise parameter to take affect, you must restart the following services on IM and Presence Service:

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Router

For more information about using the Command Line Interface to configure IPv6 parameters, see the *Cisco Unified Communications Manager Administration Guide* and the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

# IPv6 Interactions and Restrictions

Observe the following interactions and restrictions when configuring IPv6 on IM and Presence Service and when interacting with external IPv6 devices and networks:

- You can use IPv6 for your external interfaces on IM and Presence Service even though the connection between IM and Presence Service and Cisco Unified Communications Manager uses IPv4.
- You must configure IPv6 for the IM and Presence Service enterprise network and for Eth0 on each IM and Presence Service node to use IPv6; otherwise, the system attempts to use IPv4 for IP traffic on the external interfaces. For example, if the enterprise parameter is set to IPv6 and only one of two nodes in

the cluster has their Eth0 port set for IPv6, then only the node with the port set to IPv6 is enabled for IPv6. The other node will attempt to use IPv4.

**Note** If for any reason IPv6 gets disabled for either the enterprise parameter or for ETH0 on the IM and Presence Service node, the node can still perform internal DNS queries and connect to the external LDAP or database server if the server hostname that is configured on IM and Presence Service is a resolvable IPv6 address.

- For federation, you must enable IM and Presence Service for IPv6 if you need to support federated links to a foreign Enterprise that is IPv6 enabled. This is true even if there is an ASA installed between the IM and Presence Service node and the federated Enterprise. The ASA is transparent to the IM and Presence Service node.
- If IPv6 is configured for any of the following items on the IM and Presence Service node, the node will not accept incoming IPv4 packets and will not automatically revert to using IPv4. To use IPv4, you must ensure that the following items are configured for IPv4 if they appear in your deployment:
  - Connection to an external database.
  - Connection to an LDAP server.
  - Connection to an Exchange server.
  - Federation deployments.

# Enable IPv6 on Eth0 for IM and Presence Service

Use Cisco Unified IM and Presence Operating System Administration GUI to enable IPv6 on the Eth0 port of each IM and Presence Service node in the cluster to use IPv6. You must reboot the node to apply the changes.

**Note** To complete the IPv6 configuration, you must also enable the IPv6 enterprise parameter for the cluster and set the IPv6 name parameter after configuring Eth0 and rebooting the node.

### Procedure

**Step 1** Choose **Cisco Unified IM and Presence OS Administration** > **Settings** > **IP** > **Ethernet IPv6**. The **Ethernet IPv6 Configuration** window appears.

**Step 2** Check the **Enable IPv6** check box.

**Step 3** Choose the **Address Source**:

- Router Advertisement
- DHCP
- Manual Entry

If you selected **Manual Entry**, enter the **IPv6 Address**, **Subnet Mask**, and the **Default Gateway** values.

**Step 4** Required: Check the **Update with Reboot** check box.

**Tip** Do not check the **Update with Reboot** check box if you want to manually reboot the node at a later time, such as during a scheduled maintenance window; however, the changes you made do not take effect until you reboot the node.

**Step 5** Click **Save**.

If you checked the **Update with Reboot** check box, the node reboots and the changes are applied.

### What to do next

Proceed to enable the IPv6 enterprise parameter for the IM and Presence Service cluster using Cisco Unified CM IM and Presence Administration, and then set the IPv6 name parameter using Common Topology.

# Disable IPv6 on Eth0 for IM and Presence Service

Use Cisco Unified IM and Presence Operating System Administration GUI to disable IPv6 on the Eth0 port of each IM and Presence Service node in the cluster that you do not want to use IPv6. You must reboot the node to apply the changes.

**Note** If you do not want any of the nodes in the cluster to use IPv6, make sure the IPv6 enterprise parameter is disabled for the cluster.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence OS Administration** > **Settings** > **IP** > **Ethernet IPv6**. The **Ethernet IPv6 Configuration** window appears.

**Step 2** Uncheck the **Enable IPv6** check box.

**Step 3** Required: Check the **Update with Reboot** check box.

**Tip** Do not check the **Update with Reboot** check box if you want to manually reboot the node at a later time, such as during a scheduled maintenance window; however, the changes you made do not take effect until you reboot the node.

**Step 4** Choose **Save**.

If you checked the **Update with Reboot** check box, the node reboots and the changes are applied.

# Enable IPv6 Enterprise Parameter

Use Cisco Unified CM IM and Presence Administration to enable the IPv6 enterprise parameter for the IM and Presence Service cluster. You must restart the following services to apply the changes:

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Router

**Tip** To monitor system restart notifications using Cisco Unified CM IM and Presence Administration, select **System** > **Notifications**.

### Before you begin

Ensure that you have configured the following for IPv6 before restarting any services:

- Enable IPv6 for ETH0 on each IM and Presence Service node using Cisco Unified CM IM and Presence Administration.
- Set the IPv6 name parameter using Common Topology.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Enterprise Parameters**. The **Enterprise Parameters Configuration** window appears

**Step 2** Choose **True** in the **IPv6** panel.

**Step 3** Choose **Save**.

### What to do next

Restart the services on the IM and Presence Service node to apply the changes.

# Configure Proxy Server Settings

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Routing** > **Settings**.

**Step 2** Choose **On** for the Method/Event Routing Status.

**Step 3** Choose **Default SIP Proxy TCP Listener** for the Preferred Proxy Server.

**Step 4** Click **Save**.

# Services on IM and Presence Service

## Turn On Services for IM and Presence Service

The following procedure lists the services that you must turn on when you deploy a basic IM and Presence Service configuration. Turn on these services on each node in your IM and Presence Service cluster.

You may need to turn on other optional services depending on the additional features that you deploy on IM and Presence Service. See the IM and Presence Service documentation relating to those specific features for further details. If you have manually stopped any services so that you could configure certain system components or features, use this procedure to manually restart those services.

The Cisco XCP Router service must be running for a basic IM and Presence Service deployment. IM and Presence Service turns on the Cisco XCP Router by default. Verify that this network service is on by choosing **Cisco Unified IM and Presence Serviceability** > **Control Center - Network Services.**

### Procedure

**Step 1** Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Service Activation**.

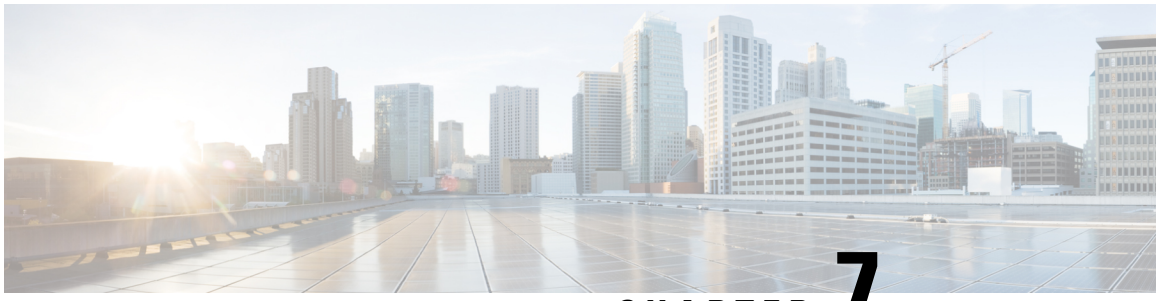
**Step 2** Choose the IM and Presence Service node from the Server menu.

You can also change the status of Cisco Unified Communications Manager services by choosing a Cisco Unified Communications Manager node from this menu.

**Step 3** For a basic IM and Presence Service deployment, turn on the following services:

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service

**Step 4** Click **Save**.



CHAPTER 7

# IP Phone Presence Setup


- Static Route Configuration on IM and Presence Service, on page 79
- Presence Gateway Configuration on IM and Presence Service, on page 84
- Configure SIP Publish Trunk on IM and Presence Service, on page 85
- Configure Cluster-Wide DNS SRV Name for SIP Publish Trunk, on page 85


# Static Route Configuration on IM and Presence Service

If you configure a static route for SIP proxy server traffic, consider the following:

- A dynamic route represents a path through the network that is automatically calculated according to routing protocols and routing update messages.
- A static route represents a fixed path that you explicitly configure through the network.
- Static routes take precedence over dynamic routes.

## Route Embed Templates

You must define a route embed template for any static route pattern that contains embedded wildcards. The route embed template contains information about the leading digits, the digit length, and location of the embedded wildcards. Before you define a route embed template, consider the sample templates we provide below.

When you define a route embed template, the characters that follow the "." must match actual telephony digits in the static route. In the sample route embed templates below, we represent these characters with "x".

### Sample Route Embed Template A

Route embed template: **74..78xxxxx***

With this template, IM and Presence Service will enable this set of static routes with embedded wildcards:

***Table 9: Static Routes Set with Embedded Wildcards - Template A***

| Destination Pattern | Next Hop Destination |
|---|---|
| 74..7812345* | 1.2.3.4:5060 |

| Destination Pattern | Next Hop Destination |
|---|---|
| 74..7867890* | 5.6.7.8.9:5060 |
| 74..7811993* | 10.10.11.37:5060 |

With this template, IM and Presence Service will not enable these static route entries:

- 73..7812345* (The initial string is not '74' as the template defines)
- 74..781* (The destination pattern digit length does not match the template)
- 74…7812345* (The number of wildcards does not match the template)

### Sample Route Embed Template B

Route embed template: **471….xx***

With this template, IM and Presence Service will enable this set of static routes with embedded wildcards:

***Table 10: Static Routes Set with Embedded Wildcards - Template B***

| Destination Pattern | Next Hop Destination |
|---|---|
| 471….34* | 20.20.21.22 |
| 471…55* | 21.21.55.79 |

With this template, IM and Presence Service will not enable these static route entries:

- 47…344* (The initial string is not '471' as the template defines)
- 471…4* (The string length does not match template)
- 471.450* (The number of wildcards does not match template)

# Configure Route Embed Templates on IM and Presence Service

You can define up to five route embed templates. However, there is no limit to the number of static routes that you can define for any route embed template.

A static route that contains an embedded wildcard must match at least one of the route embed templates.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters**.

**Step 2** Choose an IM and Presence Service node.

**Step 3** Choose the Cisco SIP Proxy service.

**Step 4** Define a route embed templates in the RouteEmbedTemplate field in the Routing Parameters (Clusterwide) section. You can define up to five route embed templates.

**Step 5** Choose **Save**.

### What to do next

Proceed to configure static routes on IM and Presence Service.

# Configure Static Routes on IM and Presence Service

The following table lists the static route parameter settings that you can configure for IM and Presence Service.

*Table 11: Static Route Parameters Settings for IM and Presence Service*

| Field | Description |
|---|---|
| Destination Pattern | This field specifies the pattern of the incoming number, up to a maximum of 255 characters.<br>The SIP proxy allows only 100 static routes to have an identical route pattern. If you exceed this limit, IM and Presence Service logs an error.<br>Wildcard Usage<br>You can use "." as a wildcard for a single character and "*" as a wildcard for multiple characters.<br>IM and Presence Service supports embedded '.' wildcard characters in static routes. However, you must define route embed templates for static routes that contain embedded wildcards. Any static route that contains an embedded wildcard must match at least one route embed template. See the route embed template topic (referenced in the Related Topics section below) for information about defining route embed templates.<br>For phones:<br>• A dot can exist at the end of the pattern, or embedded in a pattern. If you embed the dot in a pattern, you must create a route embed template to match the pattern.<br>• An asterisk can only exist at the end of the pattern.<br>For IP addresses and host names:<br>• You can use an asterisk as part of the a host name.<br>• The dot acts as a literal value in a host name.<br>An escaped asterisk sequence, *, matches a literal * and can exist anywhere. |

| Field | Description |
|---|---|
| Description | Specifies the description of a particular static route, up to a maximum of 255 characters. |
| Next Hop | Specifies the domain name or IP address of the destination (next hop) and can be either a Fully Qualified Domain Name (FQDN) or dotted IP address.<br>IM and Presence Service supports DNS SRV-based call routing. To specify DNS SRV as the next hop for a static route, set this parameter to the DNS SRV name. |
| Next Hop Port | Specifies the port number of the destination (next hop). The default port is 5060.<br>IM and Presence Service supports DNS SRV-based call routing. To specify DNS SRV as the next hop for a static route, set the next hop port parameter to 0. |
| Route Type | Specifies the route type: User or Domain. The default value is user.<br>For example, in the SIP URI "sip:19194762030@myhost.com" request, the user part is "19194762030", and the host part is "myhost.com". If you choose User as the route type, IM and Presence Service uses the user-part value "19194762030" for routing SIP traffic. If you choose the Domain as the route type, IM and Presence Service uses "myhost.com" for routing SIP traffic. |
| Protocol Type | Specifies the protocol type for this route, TCP, UDP, or TLS. The default value is TCP. |
| Priority | Specifies the route priority level. Lower values indicate higher priority. The default value is 1.<br>Value range: 1-65535 |

| Field | Description |
|---|---|
| Weight | Specifies the route weight. Use this parameter only if two or more routes have the same priority. Higher values indicate which route has the higher priority.<br>Value range: 1-65535<br>**Example:** Consider these three routes with associated priorities and weights:<br>• 1, 20<br>• 1, 10<br>• 2, 50<br>In this example, the static routes are listed in the correct order. The priority route is based on the lowest value priority, that is 1. Given that two routes share the same priority, the weight parameter with the highest value decides the priority route. In this example, IM and Presence Service directs SIP traffic to both routes configured with a priority value of 1, and distributes the traffic according to weight; The route with a weight of 20 receives twice as much traffic as the route with a weight of 10. Note that in this example, IM and Presence Service will only attempt to use the route with priority 2, if it has tried both priority 1 routes and both failed. |
| Allow Less-Specific Route | Specifies that the route can be less specific. The default setting is On. |
| In Service | Specifies whether this route has been taken out of service.<br>This parameter allows the administrator to effectively take a route out of service (versus removing it completely and re-adding it). |
| Block Route Check Box | Check to block the static route. The default setting is Unblocked. |

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Routing** > **Static Routes**.

**Step 2** Click **Add New**.

**Step 3** Configure the static route settings.

**Step 4** Click **Save**.

# Presence Gateway Configuration on IM and Presence Service

## Presence Gateway Configuration Option

You must configure Cisco Unified Communications Manager as a Presence Gateway on IM and Presence Service to enable the SIP connection that handles the availability information exchange between Cisco Unified Communications Manager and IM and Presence Service.

When configuring the Presence Gateway, specify the FQDN (Fully Qualified Domain Name) or the IP address of the associated Cisco Unified Communications Manager node. Depending on your network this value can be one of the following:

- the FQDN address of the Cisco Unified Communications Manager database publisher node
- a DNS SRV FQDN that resolves to the Cisco Unified Communications Manager subscriber nodes
- the IP address of the Cisco Unified Communications Manager database publisher node

If DNS SRV is an option in your network, configure the following:

1. Configure the Presence Gateway on the IM and Presence Service node with a DNS SRV FQDN of the Cisco Unified Communications Manager subscriber nodes (equally weighted). This will enable IM and Presence Service to share availability messages equally among all the nodes used for availability information exchange.
2. On Cisco Unified Communications Manager, configure the SIP trunk for the IM and Presence Service node with a DNS SRV FQDN of the IM and Presence Service database publisher and subscriber nodes.

If DNS SRV is not an option in your network, and you are using the IP address of the associated Cisco Unified Communications Manager node, you cannot share presence messaging traffic equally across multiple subscriber nodes because the IP address points to a single subscriber node.

### Related Topics

SIP Trunk Configuration on Cisco Unified Communications Manager, on page 51

## Configure Presence Gateway

### Before you begin

- Read the Presence Gateway configuration options topic.
- Depending on your configuration requirements, obtain the FQDN, DNS SRV FQDN, or the IP address of the associated Cisco Unified Communications Manager node.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Gateways**.

**Step 2** Click **Add New**.

**Step 3** Choose **CUCM** for the Presence Gateway Type.

**Step 4** Enter a description of the presence gateway in the Description field.

**Step 5** Specify the FQDN, DNS SRV FQDN, or the IP address of the associated Cisco Unified Communications Manager node in the Presence Gateway field.

**Step 6** Click **Save**.

### What to do next

Proceed to configure the authorization policy on IM and Presence Service.

### Related Topics

Configure Authorization Policy on IM and Presence Service, on page 199
Presence Gateway Configuration Option, on page 84

# Configure SIP Publish Trunk on IM and Presence Service

When you turn on this setting, Cisco Unified Communications Manager publishes phone presence for all line appearances that are associated with users licensed on Cisco Unified Communications Manager for IM and Presence Service.

This procedure is the same operation as assigning a SIP trunk as the CUP PUBLISH trunk in Cisco Unified Communications Manager service parameters.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Settings** > **Standard Configuration**.

**Step 2** Choose a SIP Trunk from the **CUCM SIP Publish Trunk** drop-down list.

**Step 3** Click **Save**.

# Configure Cluster-Wide DNS SRV Name for SIP Publish Trunk

When you configure the cluster-wide IM and Presence Service address on the IM and Presence database publisher node, IM and Presence Service replicates the address on all nodes in the cluster.

Set the SRV port value to 5060 when you configure a cluster-wide IM and Presence Service address.

**Note** Do not use this procedure to change the SRV Cluster Name value if the IM and Presence Service default domain is used in the cluster-wide DNS SRV record. No further action is needed.

### Before you begin

Read the cluster-wide DNS SRV topic.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters.**

**Step 2** Choose the IM and Presence Service node from the **Server** menu.

**Step 3** Choose **Cisco SIP Proxy** from the Service menu.

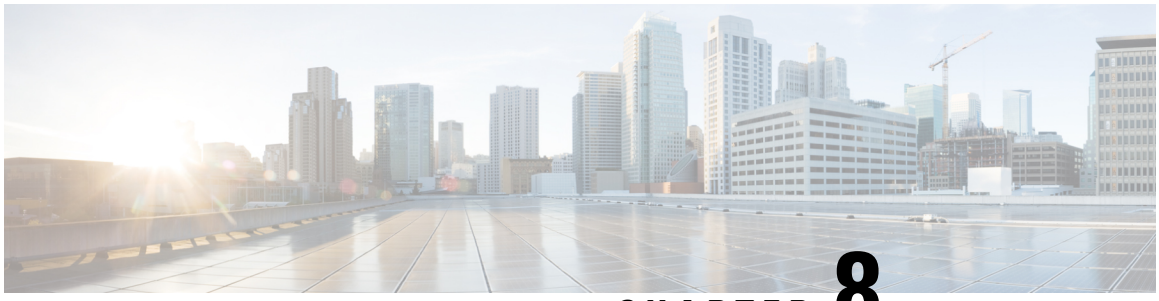
**Step 4** Edit the **SRV Cluster Name** field in the General Proxy Parameters (Clusterwide) section.

By default this parameter is empty.

**Step 5** Click **Save**.

### Related Topics

Cluster-Wide DNS SRV, on page 25
Scalability Options for Deployment, on page 23



CHAPTER 8

# LDAP Directory Integration


- LDAP Server Name, Address, and Profile Configuration, on page 87
- LDAP Directory Integration with Cisco Unified Communications Manager Task List, on page 87
- LDAP Directory Integration for Contact Searches on XMPP Clients, on page 92


## LDAP Server Name, Address, and Profile Configuration

LDAP server name, address, and profile configuration on IM and Presence Service has moved to Cisco Unified Communications Manager. For more information, see the *Cisco Unified Communications Manager Administration Guide, Release 9.0(1)*.

## LDAP Directory Integration with Cisco Unified Communications Manager Task List

The following workflow diagram shows the high-level steps to integrate the LDAP directory with Cisco Unified Communications Manager.

***Figure 9: LDAP Directory Integration with Cisco Unified Communications Manager Workflow***


The following table lists the tasks to perform to integrate the LDAP directory with Cisco Unified Communications Manager. For detailed instructions, see the related tasks.

***Table 12: Task List for LDAP Directory Integration***

| Task | Description |
|---|---|
| Secure Cisco Unified Communications Manager and LDAP Directory Connection | Enable a Secure Socket Layer (SSL) connection for the LDAP server on Cisco Unified Communications Manager.<br>**Tip** You must upload the LDAP SSL certificate as a tomcat-trust certificate on Cisco Unified Communications Manager Release 8.x and later. |

| Task | Description |
|---|---|
| Configure LDAP Synchronization for User Provisioning | You can enable the Cisco Directory Synchronization (DirSync) tool on Cisco Unified Communications Manager to automatically provision users from the corporate directory, or you can manually synchronize user directory information.<br>**Tip** LDAP synchronization does not apply to application users on Cisco Unified Communications Manager. Manually provision application users using the Cisco Unified CM Administration GUI. |
| Upload LDAP Server Certificates | When Cisco Unified Communications Manager LDAP authentication is configured for secure mode (port 636 or 3269), you must upload all LDAP authentication server certificates and Intermediate certificates as "tomcat-trust" to the IM and Presence Service node. |
| Configure LDAP Server Authentication | Enable Cisco Unified Communications Manager to authenticate user passwords against the corporate LDAP directory.<br>**Tip** LDAP authentication does not apply to the passwords of application users. |
| Configure Secure Connection Between IM and Presence Service and LDAP Directory | Perform this task on all IM and Presence Service nodes in the cluster if you configured a secure connection between Cisco Unified Communications Manager and the LDAP directory. |

# Secure Connection Between Cisco Unified Communications Manager and LDAP Directory

You can secure the connection between the Cisco Unified Communications Manager node and the LDAP directory server by enabling a Secure Socket Layer (SSL) connection for the LDAP server on Cisco Unified Communications Manager, and uploading the SSL certificate to Cisco Unified Communications Manager. You must upload the LDAP SSL certificate as a tomcat-trust certificate on Cisco Unified Communications Manager Release 8.x and later.

After you upload the LDAP SSL certificate, you need to restart the following services on Cisco Unified Communications Manager:

- Directory service
- Tomcat service

See the Cisco Unified Communications Manager documentation for details on uploading a certificate to Cisco Unified Communications Manager.

# Configure LDAP Synchronization for User Provisioning

LDAP synchronization uses the Cisco Directory Synchronization (DirSync) tool on Cisco Unified Communications Manager to synchronize information (either manually or periodically) from a corporate LDAP directory. When you enable the DirSync service, Cisco Unified Communications Manager automatically

provisions users from the corporate directory. Cisco Unified Communications Manager still uses its local database, but disables its facility to allow you to create user accounts. You use the LDAP directory interface to create and manage user accounts.

### Before you begin

- Make sure that you install the LDAP server before you attempt the LDAP-specific configuration on Cisco Unified Communications Manager.
- Activate the Cisco DirSync service on Cisco Unified Communications Manager.

### Restrictions

LDAP synchronization does not apply to application users on Cisco Unified Communications Manager. You must manually provision application users in the Cisco Unified CM Administration interface.

### Procedure

**Step 1** Choose **Cisco Unified CM Administration** > **System** > **LDAP** > **LDAP System.**

**Step 2** Click **Add New**.

**Step 3** Configure the LDAP server type and attribute.

**Step 4** Choose **Enable Synchronizing from LDAP Server**.

**Step 5** Choose **Cisco Unified CM Administration** > **System** > **LDAP** > **LDAP Directory**

**Step 6** Configure the following items:

a) LDAP directory account settings
b) User attributes to be synchronized
c) Synchronization schedule
d) LDAP server hostname or IP address, and port number

**Step 7** Check **Use SSL** if you want to use Secure Socket Layer (SSL) to communicate with the LDAP directory.

**Tip**
- If you configure LDAP over SSL, upload the LDAP directory certificate onto Cisco Unified Communications Manager.
- See the LDAP directory content in the Cisco Unified Communications Manager SRND for information about the account synchronization mechanism for specific LDAP products, and general best practices for LDAP synchronization.

### What to do next

Proceed to upload the LDAP authentication server certificates.

### Related Topics

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

# Upload LDAP Authentication Server Certificates

When Cisco Unified Communications Manager LDAP authentication is configured for secure mode (port 636 or 3269), LDAP authentication server certificates, such as Certificate Authority (CA) root and all other Intermediate certificates, must be individually uploaded as “tomcat-trust” to the IM and Presence Service node.

### Procedure

**Step 1** Choose **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management**.

**Step 2** Click **Upload Certificate**.

**Step 3** Choose **tomcat-trust** from the **Certificate Name** menu.

**Step 4** Browse and choose the LDAP server root certificate from your local computer.

**Step 5** Click **Upload File**.

**Step 6** Repeat the above steps for all other intermediate certificates.

### What to do next

Proceed to configure LDAP authentication.

# Configure LDAP Authentication

The LDAP authentication feature enables Cisco Unified Communications Manager to authenticate user passwords against the corporate LDAP directory.

### Before you begin

Enable LDAP synchronization on Cisco Unified Communications Manager.

### Restrictions

LDAP authentication does not apply to the passwords of application users; Cisco Unified Communications Manager authenticates application users in its internal database.

### Procedure

**Step 1** Choose **Cisco Unified CM Administration** > **System** > **LDAP** > **LDAP Authentication**.

**Step 2** Enable LDAP authentication for users.

**Step 3** Configure the LDAP authentication settings.

**Step 4** Configure the LDAP server hostname or IP address, and port number

**Note** To use Secure Socket Layer (SSL) to communicate with the LDAP directory, check **Use SSL**.

If you check the **Use SSL** check box, enter the IP address or hostname or FQDN that matches the Subject CN of the LDAP server's certificate. The Subject CN of the LDAP server's certificate must be either an IP address or hostname or FQDN. If this condition cannot be met, do not check the **Use SSL** check box because it will result in login failures on Cisco Unified CM IM and Presence Administration, Cisco Unified IM and Presence Serviceability, Cisco Unified IM and Presence Reporting, Cisco Jabber login, Third Party XMPP Clients and any other applications on Cisco Unified Communications Manager and IM and Presence Service that connect to LDAP to perform user authentication.

**Tip** If you configure LDAP over SSL, upload the LDAP directory certificate to Cisco Unified Communications Manager.

### What to do next

Configure secure connection between IM and Presence Service and LDAP directory.

# Configure Secure Connection Between IM and Presence Service and LDAP Directory

This topic is only applicable if you configure a secure connection between Cisco Unified Communications Manager and the LDAP directory.

**Note** Perform this procedure on all IM and Presence Service nodes in the cluster.

### Before you begin

Enable SSL for LDAP on Cisco Unified Communications Manager, and upload the LDAP directory certificate to Cisco Unified Communications Manager.

### Procedure

**Step 1** Choose **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management**.

**Step 2** Click **Upload Certificate**.

**Step 3** Choose **tomcat-trust** from the Certificate Name menu.

**Step 4** Browse and choose the LDAP server certificate from your local computer.

**Step 5** Click **Upload File**.

**Step 6** Restart the Tomcat service from the CLI using this command: `utils service restart Cisco Tomcat`

### What to do next

Proceed to integrate the LDAP directory with Cisco Jabber.

# LDAP Directory Integration for Contact Searches on XMPP Clients

These topics describe how to configure the LDAP settings on IM and Presence Service to allow users of third-party XMPP client to search and add contacts from the LDAP directory.

The JDS component on IM and Presence Service handles the third-party XMPP client communication with the LDAP directory. Third-party XMPP clients send queries to the JDS component on IM and Presence Service. The JDS component sends the LDAP queries to the provisioned LDAP servers, and then sends the results back to the XMPP client.

Before you perform the configuration described here, perform the configuration to integrate the XMPP client with Cisco Unified Communications Manager and IM and Presence Service. See topics related to third party XMPP client application integration.

***Figure 10: LDAP Directory Integration for Contact Searches on XMPP Clients Workflow***

The following workflow diagram shows the high-level steps to integrate the LDAP directory for contact searches on XMPP clients.


The following table lists the tasks to perform to integrate the LDAP directory for contact searches on XMPP clients. For detailed instructions, see the related tasks.

***Table 13: Task List for LDAP Directory Integration for Contact Searches on XMPP Clients***

| Task | Description |
|---|---|
| Configure XMPP Client LDAP Server Names and Addresses | Upload the root CA certificate to IM and Presence Service as an xmpp-trust-certificate if you enabled SSL and configured a secure connection between the LDAP server and IM and Presence Service.<br>**Tip** The subject CN in the certificate must match the FQDN of the LDAP server. |
| Configure XMPP Client LDAP Search Settings | You must specify the LDAP search settings that will allow IM and Presence Service to successfully perform contact searches for third-party XMPP clients. You can specify a primary LDAP server and up to two backup LDAP servers.<br>**Tip** Optionally, you can turn on the retrieval of vCards from the LDAP server or allow the vCards to be stored in the local database of IM and Presence Service. |

| Task | Description |
| --- | --- |
| Turn On Cisco XCP Directory Service | You must turn on XCP Directory Service to allow users of a third-party XMPP client to search and add contacts from the LDAP directory.<br>**Tip** Do not turn on the Cisco XCP Directory Service until after you configure the LDAP server and LDAP search settings for third-party XMPP clients; otherwise, the service with stop running. |

# LDAP Account Lock Issue

If you enter the wrong password for the LDAP server that you configure for third-party XMPP clients, and you restart the XCP services on IM and Presence Service, the JDS component will perform multiple attempts to sign in to the LDAP server with the wrong password. If the LDAP server is configured to lock out an account after a number of failed attempts, then the LDAP server may lock the JDS component out at some point. If the JDS component uses the same credentials as other applications that connect to LDAP (applications that are not necessarily on IM and Presence Service), these applications will also be locked out of LDAP.

To fix this issue, configure a separate user, with the same role and privileges as the existing LDAP user, and allow only JDS to sign in as this second user. If you enter the wrong password for the LDAP server, only the JDS component is locked out from the LDAP server.

# Configure LDAP Server Names and Addresses for XMPP Clients

If you choose to enable Secured Sockets Layer (SSL), configure a secure connection between the LDAP server and IM and Presence Service and upload the root Certificate Authority (CA) certificate to IM and Presence Service as an cup-xmpp-trust certificate. The subject common name (CN) in the certificate must match the Fully Qualified Domain Name (FQDN) of the LDAP server.

If you import a certificate chain (more than one certificate from the root node to the trusted node), import all certificates in the chain except the leaf node. For example, if the CA signs the certificate for the LDAP server, import only the CA certificate and not the certificate for the LDAP server.

You can use IPv6 to connect to the LDAP server even though the connection between IM and Presence Service and Cisco Unified Communications Manager is IPv4. If IPv6 gets disabled for either the enterprise parameter or for ETH0 on the IM and Presence Service node, the node can still perform an internal DNS query and connect to the external LDAP server if the hostname of the external LDAP server configured for third-party XMPP clients is a resolvable IPv6 address.

**Tip** You configure the hostname of the external LDAP server for third-party XMPP clients in the **LDAP Server - Third-Party XMPP Client** window.

### Before you begin

Obtain the hostnames or IP addresses of the LDAP directories.

If you use IPv6 to connect to the LDAP server, enable IPv6 on the enterprise parameter and on Eth0 for each IM and Presence Service node in your deployment before you configure the LDAP server.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Application** > **Third-Party Clients** > **Third-Party LDAP Servers**.

**Step 2** Click **Add New**.

**Step 3** Enter an ID for the LDAP server.

**Step 4** Enter the hostname for the LDAP server.

For IPv6 connections, you can enter the IPv6 address of the LDAP server.

**Step 5** Specify the port number on the LDAP server that is listening to the TCP or SSL connection.

The default port is 389. If you enable SSL, specify port 636.

**Step 6** Specify the username and the password for the LDAP server. These values must match the credentials you configure on the LDAP server.

See the LDAP directory documentation or the LDAP directory configuration for this information.

**Step 7** Check **Enable SSL** if you want to use SSL to communicate with the LDAP server.

**Note** If SSL is enabled then the **hostname** value which you enter can be either the hostname or the FQDN of the LDAP server. The value that is used must match the value in the security certificate **CN** or **SAN** fields.

If you must use an IP address, then this value must also be used on the certificate for either the **CN** or **SAN** fields.

**Step 8** Click **Save**.

**Step 9** Start the Cisco XCP Router service on all nodes in the cluster (if this service is not already running).

**Tip**

- If you enable SSL, the XMPP contact searches may be slower because of the negotiation procedures at SSL connection setup, and data encryption and decryption after IM and Presence Service establishes the SSL connection. As a result, if your users perform XMPP contact searches extensively in your deployment, this could impact the overall system performance.
- You can use the certificate import tool to check the communication with the LDAP server hostname and port value after you upload the certificate for the LDAP server. Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Security** > **Certificate Import Tool**.
- If you make an update to the LDAP server configuration for third-party XMPP clients, restart the Cisco XCP Directory Service. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** to restart this service.

### What to do next

Proceed to configure LDAP search settings for XMPP clients.

### Related Topics

Secure Connection Between Cisco Unified Communications Manager and LDAP Directory, on page 88
Configure Secure Connection Between IM and Presence Service and LDAP Directory, on page 91

# Configure LDAP Search Settings for XMPP Clients

You must specify the LDAP search settings that will allow IM and Presence Service to successfully perform contact search for third-party XMPP clients

Third-party XMPP clients connect to an LDAP server on a per-search basis. If the connection to the primary server fails, the XMPP client tries the first backup LDAP server, and if it is not available, it then tries the second backup server and so on. If an LDAP query is in process when the system fails over, the next available server completes this LDAP query.

Optionally you can turn on the retrieval of vCards from the LDAP server. If you turn on vCard retrieval:

- The corporate LDAP directory stores the vCards.
- When XMPP clients search for their own vCard, or the vCard for a contact, the vCards are retrieved from LDAP via the JDS service.
- Clients cannot set or modify their own vCard as they are not authorized to edit the corporate LDAP directory.

If you turn off the retrieval of vCards from LDAP server:

- IM and Presence Service stores the vCards in the local database.
- When XMPP clients search for their own vCard, or the vCard for a contact, the vCards are retrieved from the local IM and Presence Service database.
- Clients can set or modify their own vCard.

The following table lists the LDAP search settings for XMPP clients.

***Table 14: LDAP Search Settings for XMPP Clients***

| Field | Setting |
|---|---|
| LDAP Server Type | Choose an LDAP server type from this list:<br>• Microsoft Active Directory<br>• Generic Directory Server - Choose this menu item if you are using any other supported LDAP server type (iPlanet, Sun ONE or OpenLDAP). |
| User Object Class | Enter the User Object Class value appropriate to your LDAP server type. This value must match the User Object Class value configured on your LDAP server.<br>If you use Microsoft Active Directory, the default value is ‘user’. |
| Base Context | Enter the Base Context appropriate to your LDAP server. This value must match a previously configured domain, and/or an organizational structure on your LDAP server. |

| Field | Setting |
|---|---|
| User Attribute | Enter the User Attribute value appropriate to your LDAP server type. This value must match the User Attribute value configured on your LDAP server.<br>If you use Microsoft Active Directory, the default value is sAMAccountName.<br>If the Directory URI IM address scheme is used and the Directory URI is mapped to either mail or msRTCSIPPrimaryUserAddress, then mail or msRTCSIPPrimaryUserAddress must be specified as the user attribute. |
| LDAP Server 1 | Choose a primary LDAP server. |
| LDAP Server 2 | (Optional) Choose a backup LDAP server. |
| LDAP Server 3 | (Optional) Choose a backup LDAP server. |

### Before you begin

Specify the LDAP server names and addresses for XMPP clients.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Application** > **Third-Party Clients** > **Third-Party LDAP Settings**.

**Step 2** Enter information into the fields.

**Step 3** Check **Build vCards from LDAP** if you want to enable users to request vCards for their contacts and retrieve the vCard information from the LDAP server. Leave the check box unchecked if you want clients to be able to automatically request vCards for users as users join the contact list. In this case, clients retrieve the vCard information from the local IM and Presence Service database.

**Step 4** Enter the LDAP field required to construct the vCard FN field. Clients use the value in the vCard FN field to display the contact's name in the contact list when a user requests a contact's vCard.

**Step 5** In the Searchable LDAP Attributes table, map the client user fields to the appropriate LDAP user fields.

If you use Microsoft Active Directory, IM and Presence Service populates the default attribute values in the table.

**Step 6** Click **Save**.

**Step 7** Start the Cisco XCP Router service (if this service is not already running)

**Tip** If you make an update to the LDAP search configuration for third-party XMPP clients, restart the Cisco XCP Directory Service. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** to restart this service.

### What to do next

Proceed to turn on the Cisco XCP directory service.

# Turn On Cisco XCP Directory Service

You must turn on the Cisco XCP Directory Service to allow users of a third-party XMPP client to search and add contacts from the LDAP directory. Turn on the Cisco XCP Directory Service on all nodes in the cluster.

**Note** Do not turn on the Cisco XCP Directory Service until you configure the LDAP server, and LDAP search settings for third-party XMPP clients. If you turn on the Cisco XCP Directory Service, but you do not configure the LDAP server, and LDAP search settings for third-party XMPP clients, the service will start, and then stop again.

### Before you begin

Configure the LDAP server, and LDAP search settings for third-party XMPP clients.

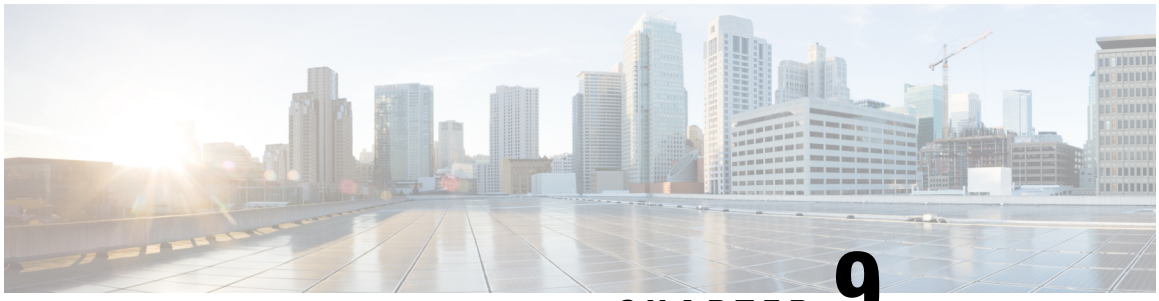
### Procedure

**Step 1** Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Service Activation**.

**Step 2** Choose the IM and Presence Service node from the Server menu.

**Step 3** Choose **Cisco XCP Directory Service**.

**Step 4** Click **Save**.



CHAPTER 9

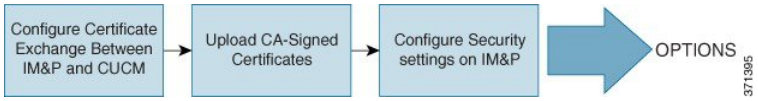
# Security Configuration on IM and Presence Service


- Security Setup Task List, on page 99
- Create Login Banner, on page 100
- Multi-Server Certificate Overview, on page 101
- IM and Presence Service Certificate Types, on page 101
- Certificate Exchange Configuration Between IM and Presence Service and Cisco Unified Communications Manager, on page 104
- Multi-Server CA Signed Certificate Upload to IM and Presence Service, on page 107
- Single-Server CA Signed Certificate Upload to IM and Presence Service , on page 107
- Delete Self-Signed Trust Certificates , on page 117
- SIP Security Settings Configuration on IM and Presence Service, on page 119
- XMPP Security Settings Configuration on IM and Presence Service, on page 120
- FIPS 140-2 Mode Configuration, on page 125


## Security Setup Task List

The following workflow diagram shows the high-level steps to configure security on the IM and Presence Service node deployment.

***Figure 11: Security Setup Workflow***




The following table lists the tasks to perform to set up security on the IM and Presence Service node deployment. For detailed instructions, see the procedures that are related to the tasks outlined in the workflow.

**Note** Optionally, you can create a banner that users acknowledge as part of their login to any IM and Presence Service interface.

*Table 15: Task List for Security Setup on IM and Presence Service*

| Task | Description |
|---|---|
| Configure Certificate Exchange Between IM and Presence Service and Cisco Unified Communications Manager | Perform the following tasks:<br>• Import Cisco Unified Communications Manager certificate to IM and Presence Service node, and then restart the SIP proxy service.<br>**Tip** You can import the certificate using either the Certificate Import Tool or manually using Cisco Unified IM and Presence OS Administration from **Security** > **Certificate Management**.<br>• Download the certificate from IM and Presence Service, and then upload the certificate to Callmanager-trust on Cisco Unified Communications Manager.<br>• Restart the Cisco Unified Communications Manager service.<br>**Note** You must configure a SIP security profile and SIP trunk for IM and Presence Service before you can configure the certificate exchange between Cisco Unified Communications Manager and IM and Presence Service. |
| Upload CA-Signed Certificates | Upload the Certificate Authority (CA) signed certificates to IM and Presence Service for your deployment, which can be either a single-server or a multi-server deployment. Service restarts are required. See the related tasks for details.<br>• tomcat certificate<br>• cup-xmpp certificate<br>• cup-xmpp-s2s certificate<br>**Tip** You can upload these certificates on any IM and Presence Service node in the cluster. When this is done, the certificate and the associated signing certificates are automatically distributed to all the other IM and Presence Service nodes in the cluster. |
| Configure Security Settings on IM and Presence Service | When you import an IM and Presence Service certificate, IM and Presence Service automatically attempts to add the TLS peer subject to the TLS peer subject list, and to the TLS context list. Verify the TLS peer subject and TLS context configuration is set up to your requirements.<br>IM and Presence Service provides increased security for XMPP-based configurations. You can configure the XMPP secure modes on IM and Presence Service using Cisco Unified CM IM and Presence Administration from **System** > **Security** > **Settings**. |

# Create Login Banner

You can create a banner that users acknowledge as part of their login to any IM and Presence Service interface. You create a .txt file using any text editor, include important notifications they want users to be made aware of, and upload it to the Cisco Unified IM and Presence OS Administration page. This banner will then appear on all IM and Presence Service interfaces notifying users of important information before they login, including

legal warnings and obligations. The following interfaces will display this banner before and after a user logs in: Cisco Unified CM IM and Presence Administration, Cisco Unified IM and Presence Operating System Administration, Cisco Unified IM and Presence Serviceability, Cisco Unified IM and Presence Reporting, and IM and Presence Disaster Recovery System.

**Procedure**

**Step 1** Create a .txt file with the contents you want to display in the banner.

**Step 2** Sign in to Cisco Unified IM and Presence Operating System Administration.

**Step 3** Choose **Software Upgrades** > **Customized Logon Message**.

**Step 4** Click **Browse** and locate the .txt file.

**Step 5** Click **Upload File**.

The banner will appear before and after login on most IM and Presence Service interfaces.

**Note** The .txt file must be uploaded to each IM and Presence Service node separately.

# Multi-Server Certificate Overview

IM and Presence Service supports multi-server SAN based certificates for the certificate purposes of tomcat, cup-xmpp, and cup-xmpp-s2s. You can select between a single-server or multi-server distribution to generate a Certificate Signing Request (CSR) for the certificate purposes which support multi-server certificates. The resulting signed multi-server certificate and its associated chain of signing certificates are automatically distributed to the other servers in the cluster on upload of the multi-server certificate to any of the individual servers in the cluster. For more information on multi-server certificates, see the New and Changed Features chapter of the *Release Notes for Cisco Unified Communications Manager, Release 10.5(1)*.

# IM and Presence Service Certificate Types

This section describes the different certificates required for the clients and services on IM and Presence Service.

*Table 16: Certificate Types and Services*

| Certificate Type | Service | Certificate Trust Store | Multi-Server Support | Notes |
|---|---|---|---|---|
| tomcat | Cisco Client Profile Agent<br>Cisco AXL Web Service<br>Cisco Tomcat | tomcat- trust | Yes | Presented to a Cisco Jabber client as part of client authentication for IM and Presence Service.<br>Presented to a web browser when navigating the Cisco Unified CM IM and Presence Administration user interface.<br>The associated trust-store is used to verify connections made by IM and Presence Service for the purposes of authenticating user credentials with a configured LDAP server. |
| ipsec | | ipsec-trust | No | Used when an IPSec policy is enabled. |
| cup | Cisco SIP Proxy<br>Cisco Presence Engine | cup-trust | No | |

| Certificate Type | Service | Certificate Trust Store | Multi-Server Support | Notes |
|---|---|---|---|---|
| cup-xmpp | Cisco XCP Connection Manager<br>Cisco XCP Web Connection Manager<br>Cisco XCP Directory service<br>Cisco XCP Router service | cup-xmpp-trust | Yes | Presented to a Cisco Jabber client, Third-Party XMPP client, or a CAXL based application when the XMPP session is being created.<br>The associated trust-store is used to verify connections made by Cisco XCP Directory service in performing LDAP search operations for third-party XMPP clients.<br>The associated trust-store is used by the Cisco XCP Router service when establishing secure connections between IM and Presence Service servers if the Routing Communication Type is set to Router-to-Router. |
| cup-xmpp-s2s | Cisco XCP XMPP Federation Connection Manager | cup-xmpp-trust | Yes | Presented for XMPP interdomain federation when connecting to externally federated XMPP systems. |

**Related Topics**

XMPP Security Settings Configuration on IM and Presence Service, on page 120
Configure Secure Connection Between IM and Presence Service and LDAP Directory, on page 91

# Certificate Exchange Configuration Between IM and Presence Service and Cisco Unified Communications Manager

This module describes the exchange of self-signed certificates between the Cisco Unified Communications Manager node and the IM and Presence Service node. You can use the Certificate Import Tool on IM and Presence Service to automatically import the Cisco Unified Communications Manager certificate to IM and Presence Service. However, you must manually upload the IM and Presence Service certificate to Cisco Unified Communications Manager.

Only perform these procedures if you require a secure connection between IM and Presence Service and Cisco Unified Communications Manager.

## Prerequisites for Configuring Security

Configure the following items on Cisco Unified Communications Manager:

- Configure a SIP security profile for IM and Presence Service.
- Configure a SIP trunk for IM and Presence Service:
  - Associate the security profile with the SIP trunk.
  - Configure the SIP trunk with the subject Common Name (CN) of the IM and Presence Service certificate.

### Related Topics

SIP Trunk Configuration on Cisco Unified Communications Manager, on page 51

## Import Cisco Unified Communications Manager Certificate to IM and Presence Service

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Security** > **Certificate Import Tool**.

**Step 2** Choose **IM and Presence (IM/P) Service Trust** from the **Certificate Trust Store** menu.

**Step 3** Enter the IP address, hostname or FQDN of the Cisco Unified Communications Manager node.

**Step 4** Enter a port number to communicate with the Cisco Unified Communications Manager node.

**Step 5** Click **Submit**.

**Note** After the Certificate Import Tool completes the import operation, it reports whether or not it successfully connected to Cisco Unified Communications Manager, and whether or not it successfully downloaded the certificate from Cisco Unified Communications Manager. If the Certificate Import Tool reports a failure, see the Online Help for a recommended action. You can also manually import the certificate by choosing **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management**.

### What to do next

Proceed to restart the SIP proxy service.

# Restart SIP Proxy Service

### Before you begin

Import the Cisco Unified Communications Manager certificate to IM and Presence Service.

### Procedure

**Step 1** Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** on IM and Presence Service,

**Step 2** Choose **Cisco SIP Proxy**.

**Step 3** Click **Restart**.

### What to do next

Proceed to download the certificate from IM and Presence Service.

# Download Certificate from IM and Presence Service

### Procedure

**Step 1** Choose **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management** on IM and Presence Service.

**Step 2** Click **Find**.

**Step 3** Choose the **cup.pem** file.

**Step 4** Click **Download** and save the file to your local computer.

**Tip** Ignore any errors that IM and Presence Service displays regarding access to the cup.csr file; The CA (Certificate Authority) does not need to sign the certificate that you exchange with Cisco Unified Communications Manager.

### What to do next

Proceed to upload the IM and Presence Service certificate to Cisco Unified Communications Manager.

# Upload IM and Presence Service Certificate to Cisco Unified Communications Manager

### Before you begin

Download the certificate from IM and Presence Service.

### Procedure

**Step 1** Choose **Cisco Unified OS Administration** > **Security** > **Certificate Management** on Cisco Unified Communications Manager.

**Step 2** Click **Upload Certificate**.

**Step 3** Choose **Callmanager-trust** from the Certificate Name menu.

**Step 4** Browse and choose the certificate (.pem file) previously downloaded from IM and Presence Service.

**Step 5** Click **Upload File**.

### What to do next

Proceed to restart the Cisco Unified Communications Manager CallManager service.

# Restart Cisco Unified Communications Manager Service

### Before you begin

Upload the IM and Presence Service certificate to Cisco Unified Communications Manager.

### Procedure

**Step 1** Choose **Cisco Unified Serviceability** > **Tools** > **Control Center - Feature Services** on Cisco Unified Communications Manager.

**Step 2** Choose **Cisco CallManager**.

**Step 3** Click **Restart**.

### What to do next

Proceed to configure SIP security settings on IM and Presence Service.

### Related Topics

SIP Security Settings Configuration on IM and Presence Service, on page 119

# Multi-Server CA Signed Certificate Upload to IM and Presence Service

This section gives further information on uploading the following types of multi-server CA signed certificates:

- tomcat certificate
- cup-xmpp certificate
- cup-xmpp-s2s certificate

You can upload such certificates on any IM and Presence Service node in the cluster. When this is done the certificate and the associated signing certificates are automatically distributed to all the other IM and Presence Service nodes in the cluster. If a self-signed certificate already exists on any node, for the given certificate purpose (for example, tomcat, cup-xmpp, or cup-xmpp-s2s), it will be overwritten by the new multi-server certificate.

The IM and Presence Service nodes to which a given multi-server certificate and the associated signing certificates are distributed is dependent on the certificate purpose. The cup-xmpp and cup-xmpp-s2s multi-server certificates are distributed to all IM and Presence Service nodes in the cluster. The tomcat multi-server certificate is distributed to all IM and Presence Service nodes in the cluster and to all Cisco Unified Communications Manager nodes in the cluster. For more information on multi-server SAN certificates, see the New and Changed Features chapter of the *Release Notes for Cisco Unified Communications Manager, Release 10.5(1)*.

# Single-Server CA Signed Certificate Upload to IM and Presence Service

This section describes how to upload the following types of CA signed certificates to an IM and Presence Service deployment:

- tomcat certificate
- cup-xmpp certificate
- cup-xmpp-s2s certificate

## CA-Signed Tomcat Certificate Task List

The high-level steps to upload a CA signed Tomcat certificate to IM and Presence Service are:

1. Upload the Root Certificate and Intermediate Certificate of the signing Certificate Authority to IM and Presence Service.
2. Restart the Cisco Intercluster Sync Agent service.
3. Ensure that the CA certificates have been correctly synced to other clusters.

4. Upload the appropriate signed certificate to each IM and Presence Service node.
5. Restart the Cisco Tomcat service on all nodes.
6. Ensure that intercluster syncing is operating correctly.

## Upload Root Certificate and Intermediate Certificate of the Signing Certificate Authority

When you upload the Root and Intermediate Certificates, you must upload each certificate in the certificate chain to IM and Presence Service from the Root Certificate down to the last Intermediate Certificate, as follows:

root > intermediate-1 > intermediate-2 > … > intermediate-N

With each certificate that you upload in the chain, you must specify which previously uploaded certificate signed it. For example:

- For intermediate-1, the root cert was used to sign it.
- For intermediate-2, the intermediate-1 cert was used to sign it.

You must upload the Root Certificate and the Intermediate Certificates, if any, to the trust store of the related leaf certificate on the IM and Presence database publisher node. Complete the following procedure to upload the Root Certificate and the Intermediate Certificate of the signing Certificate Authority (CA) to the IM and Presence Service deployment.

### Procedure

**Step 1** On the IM and Presence database publisher node, choose **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management**.

**Step 2** Click **Upload Certificate/Certificate chain**.

**Step 3** From the Certificate Name drop-down list, choose **tomcat-trust**.

**Step 4** Enter a description for the signed certificate.

**Step 5** Click **Browse** to locate the file for the Root Certificate.

**Step 6** Click **Upload File**.

**Step 7** Upload each Intermediate Certificate in the same way using the **Upload Certificate/Certificate chain** window.

### What to do next

Restart the Cisco Intercluster Sync Agent service.

## Restart Cisco Intercluster Sync Agent Service

After you upload the Root and Intermediate certificates to the IM and Presence database publisher node, you must restart the Cisco Intercluster Sync Agent service on that node. This service restart ensures that the CA certificates are synced immediately to all other clusters.

### Procedure

**Step 1** Log into the Admin CLI.

**Step 2** Run the following command: **utils service restart Cisco Intercluster Sync Agent**

**Note** You can also restart the Cisco Intercluster Sync Agent service from the Cisco Unified Serviceability GUI.

### What to do next

Verify that the CA certificates have synced to the other clusters.

## Verify CA Certificates Have Synchronized to Other Clusters

After the Cisco Intercluster Sync Agent service has restarted, you must ensure that the CA certificate(s) have been correctly synchronized to other clusters. Complete the following procedure on each of the other IM and Presence database publisher nodes.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter**.

**Step 2** Under **Inter-clustering Troubleshooter**, find the test **Verify that each TLS-enabled inter-cluster peer has successfully exchanged security certificates** and verify that is has passed.

**Step 3** If the test shows an error, note the intercluster peer IP address; it should reference the cluster on which you uploaded the CA certificate(s). Continue with the following steps to resolve the issue.

**Step 4** Choose **Presence** > **Inter-Clustering** and click the link associated with the intercluster peer that was identified on the **System Troubleshooter** page.

**Step 5** Click **Force Manual Sync**.

**Step 6** Allow 60 seconds for the Inter-cluster Peer Status panel to auto-refresh.

**Step 7** Verify that the **Certificate Status** field shows "Connection is secure".

**Step 8** If the **Certificate Status** field does not show "Connection is secure", restart the Cisco Intercluster Sync Agent service on the IM and Presence database publisher node and then repeat steps 5 to 7.

- To restart the service from the admin CLI run the following command: **utils service restart Cisco Intercluster Sync Agent**
- Alternatively, you can restart this service from the Cisco Unified IM and Presence Serviceability GUI.

**Step 9** Verify that the **Certificate Status** now shows "Connection is secure". This means that intercluster syncing is correctly established between the clusters and that the CA certificates that you uploaded are synced to the other clusters.

### What to do next

Upload the signed certificate to each IM and Presence Service node.

## Upload Signed Certificate to Each IM and Presence Service Node

When the CA certificates have correctly synced to all clusters, you can upload the appropriate signed certificate to each IM and Presence Service node.

**Note** Cisco recommends that you sign all required tomcat certificates for a cluster and upload them at the same time. This process reduces the time to recover intercluster communications.

### Procedure

**Step 1** Choose **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management**.

**Step 2** Click **Upload Certificate/Certificate chain**.

**Step 3** From the Certificate Name drop-down list, choose **tomcat**.

**Step 4** Enter a description for the signed certificate.

**Step 5** Click **Browse** to locate the file to upload.

**Step 6** Click **Upload File**.

**Step 7** Repeat for each IM and Presence Service node.

For more information about certificate management, see the *Cisco Unified Communications Operating System Administration Guide*.

### What to do next

Restart the Cisco Tomcat service.

## Restart Cisco Tomcat Service

After you upload the tomcat certificate to each IM and Presence Service node, you must restart the Cisco Tomcat service on each node.

### Procedure

**Step 1** Log into the admin CLI.

**Step 2** Run the following command: `utils service restart Cisco Tomcat`

**Step 3** Repeat for each node.

### What to do next

Verify that intercluster syncing is operating correctly.

## Verify Intercluster Syncing

After the Cisco Tomcat service has restarted for all affected nodes within the cluster, you must verify that intercluster syncing is operating correctly. Complete the following procedure on each IM and Presence database publisher node in the other clusters.

**Procedure**

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter**.

**Step 2** Under **Inter-clustering Troubleshooter**, find the test **Verify that each TLS-enabled inter-cluster peer has successfully exchanged security certificates** test and verify that is has passed.

**Step 3** If the test shows an error, note the intercluster peer IP address; it should reference the cluster on which you uploaded the CA certificate(s). Continue with the following steps to resolve the issue

**Step 4** Choose **Presence** > **Inter-Clustering** and click the link associated with the intercluster peer that was identified on the **System Troubleshooter** page.

**Step 5** Click **Force Manual Sync**.

**Step 6** Check the **Also resync peer's Tomcat certificates** checkbox and click **OK**.

**Step 7** Allow 60 seconds for the Inter-cluster Peer Status panel to auto-refresh.

**Step 8** Verify that the **Certificate Status** field shows "Connection is secure".

**Step 9** If the **Certificate Status** field does not show "Connection is secure", restart the Cisco Intercluster Sync Agent service on the IM and Presence database publisher node and then repeat steps 5 to 8.

- To restart the service from the admin CLI run the following command: **`utils service restart Cisco Intercluster Sync Agent`**
- Alternatively, you can restart this service from the Cisco Unified IM and Presence Serviceability GUI.

**Step 10** Verify that the **Certificate Status** now shows "Connection is secure". This means that intercluster syncing is now re-established between this cluster and the cluster for which the certificates were uploaded.

# CA-Signed cup-xmpp Certificate Upload

The high-level steps to upload a CA signed cup-xmpp certificate to IM and Presence Service are:

1. Upload the Root Certificate and Intermediate Certificate of the signing Certificate Authority to IM and Presence Service.
2. Restart the Cisco Intercluster Sync Agent service.
3. Ensure that the CA certificates have been correctly synced to other clusters.
4. Upload the appropriate signed certificate to each IM and Presence Service node.
5. Restart the Cisco XCP Router service on all nodes.

## Upload Root Certificate and Intermediate Certificate of the Signing Certificate Authority

When you upload the Root and Intermediate Certificates, you must upload each certificate in the certificate chain to IM and Presence Service from the Root Certificate down to the last Intermediate Certificate, as follows:

root > intermediate-1 > intermediate-2 > … > intermediate-N

With each certificate that you upload in the chain, you must specify which previously uploaded certificate signed it. For example:

- For intermediate-1, the root cert was used to sign it.
- For intermediate-2, the intermediate-1 cert was used to sign it.

You must upload the Root Certificate and the Intermediate Certificates, if any, to the **cup-xmpp-trust** store on the IM and Presence database publisher node. Complete the following procedure to upload the Root Certificate and the Intermediate Certificate of the signing Certificate Authority (CA) to the IM and Presence Service deployment.

### Procedure

**Step 1** On the IM and Presence database publisher node, choose **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management**.

**Step 2** Click **Upload Certificate/Certificate chain**.

**Step 3** From the Certificate Name drop-down list, choose **cup-xmpp-trust**.

**Step 4** Enter a description for the signed certificate.

**Step 5** Click **Browse** to locate the file for the Root Certificate.

**Step 6** Click **Upload File**.

**Step 7** Upload each Intermediate Certificate in the same way using the **Upload Certificate/Certificate chain** window.

### What to do next

Restart the Cisco Intercluster Sync Agent service.

## Restart Cisco Intercluster Sync Agent Service

After you upload the Root and Intermediate certificates to the IM and Presence database publisher node, you must restart the Cisco Intercluster Sync Agent service on that node. This service restart ensures that the CA certificates are synced immediately to all other clusters.

### Procedure

**Step 1** Log into the Admin CLI.

**Step 2** Run the following command: `utils service restart Cisco Intercluster Sync Agent`

**Note** You can also restart the Cisco Intercluster Sync Agent service from the Cisco Unified Serviceability GUI.

### What to do next

Verify that the CA certificates have synced to the other clusters.

## Verify CA Certificates Have Synchronized to Other Clusters

After the Cisco Intercluster Sync Agent service has restarted, you must ensure that the CA certificate(s) have been correctly synchronized to other clusters. Complete the following procedure on each of the other IM and Presence database publisher nodes.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter**.

**Step 2** Under **Inter-clustering Troubleshooter**, find the test **Verify that each TLS-enabled inter-cluster peer has successfully exchanged security certificates** and verify that is has passed.

**Step 3** If the test shows an error, note the intercluster peer IP address; it should reference the cluster on which you uploaded the CA certificate(s). Continue with the following steps to resolve the issue.

**Step 4** Choose **Presence** > **Inter-Clustering** and click the link associated with the intercluster peer that was identified on the **System Troubleshooter** page.

**Step 5** Click **Force Manual Sync**.

**Step 6** Allow 60 seconds for the Inter-cluster Peer Status panel to auto-refresh.

**Step 7** Verify that the **Certificate Status** field shows "Connection is secure".

**Step 8** If the **Certificate Status** field does not show "Connection is secure", restart the Cisco Intercluster Sync Agent service on the IM and Presence database publisher node and then repeat steps 5 to 7.

- To restart the service from the admin CLI run the following command: **`utils service restart Cisco Intercluster Sync Agent`**
- Alternatively, you can restart this service from the Cisco Unified IM and Presence Serviceability GUI.

**Step 9** Verify that the **Certificate Status** now shows "Connection is secure". This means that intercluster syncing is correctly established between the clusters and that the CA certificates that you uploaded are synced to the other clusters.

### What to do next

Upload the signed certificate to each IM and Presence Service node.

## Upload Signed Certificate to Each IM and Presence Service Node

When the CA certificates have correctly synced to all clusters, you can upload the appropriate signed cup-xmpp certificate to each IM and Presence Service node.

**Note** Cisco recommends that you sign all required cup-xmpp certificates for a cluster and upload them at the same time so that service impacts can be managed within a single maintenance window.

### Procedure

**Step 1** Choose **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management**.
**Step 2** Click **Upload Certificate/Certificate chain**.
**Step 3** From the Certificate Name drop-down list, choose **cup-xmpp**.
**Step 4** Enter a description for the signed certificate.
**Step 5** Click **Browse** to locate the file to upload.
**Step 6** Click **Upload File**.
**Step 7** Repeat for each IM and Presence Service node.

For more information about certificate management, see the *Cisco Unified Communications Operating System Administration Guide* .

### What to do next

Restart the Cisco XCP Router service on all nodes.

## Restart Cisco XCP Router Service On All Nodes

**Caution** A restart of the Cisco XCP Router affects service.

After you upload the cup-xmpp certificate to each IM and Presence Service node, you must restart the Cisco XCP Router service on each node.

### Procedure

**Step 1** Log into the admin CLI.
**Step 2** Run the following command: `utils service restart Cisco XCP Router`
**Step 3** Repeat for each node.

**Note** You can also restart the Cisco XCP Router service from the Cisco Unified IM and Presence Serviceability GUI.

# CA-Signed cup-xmpp-s2s Certificate Upload

The high-level steps to upload a CA signed cup-xmpp-s2s certificate to IM and Presence Service are:

1. Upload the Root Certificate and Intermediate Certificate of the signing Certificate Authority to IM and Presence Service.
2. Ensure that the CA certificates have been correctly synced to other clusters.

3. Upload the appropriate signed certificate to IM and Presence Service federation nodes (this certificate is not required on all IM and Presence Service nodes, only those used for federation).
4. Restart the Cisco XCP XMPP Federation Connection Manager service on all affected nodes.

## Upload Root Certificate and Intermediate Certificate of Signing Certificate Authority

When you upload the Root and Intermediate Certificates, you must upload each certificate in the certificate chain to IM and Presence Service from the Root Certificate down to the last Intermediate Certificate, as follows:

root > intermediate-1 > intermediate-2 > … > intermediate-N

With each certificate that you upload in the chain, you must specify which previously uploaded certificate signed it. For example:

- For intermediate-1, the root cert was used to sign it.
- For intermediate-2, the intermediate-1 cert was used to sign it.

You must upload the Root Certificate and the Intermediate Certificates, if any, to the **cup-xmpp-trust** store on the IM and Presence database publisher node. Complete the following procedure to upload the Root Certificate and the Intermediate Certificate of the signing Certificate Authority (CA) to the IM and Presence Service deployment.

### Procedure

**Step 1** On the IM and Presence database publisher node, choose **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management**.

**Step 2** Click **Upload Certificate/Certificate chain**.

**Step 3** From the Certificate Name drop-down list, choose **cup-xmpp-trust**.

**Step 4** Enter a description for the signed certificate.

**Step 5** Click **Browse** to locate the file for the Root Certificate.

**Step 6** Click **Upload File**.

**Step 7** Upload each Intermediate Certificate in the same way using the **Upload Certificate/Certificate chain** window.

### What to do next

Verify that the CA certificates have synced to other clusters.

## Verify CA Certificates Have Synchronized to Other Clusters

After the Cisco Intercluster Sync Agent service has restarted, you must ensure that the CA certificate(s) have been correctly synchronized to other clusters. Complete the following procedure on each of the other IM and Presence database publisher nodes.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter**.

**Step 2** Under **Inter-clustering Troubleshooter**, find the test **Verify that each TLS-enabled inter-cluster peer has successfully exchanged security certificates** and verify that is has passed.

**Step 3** If the test shows an error, note the intercluster peer IP address; it should reference the cluster on which you uploaded the CA certificate(s). Continue with the following steps to resolve the issue.

**Step 4** Choose **Presence** > **Inter-Clustering** and click the link associated with the intercluster peer that was identified on the **System Troubleshooter** page.

**Step 5** Click **Force Manual Sync**.

**Step 6** Allow 60 seconds for the Inter-cluster Peer Status panel to auto-refresh.

**Step 7** Verify that the **Certificate Status** field shows "Connection is secure".

**Step 8** If the **Certificate Status** field does not show "Connection is secure", restart the Cisco Intercluster Sync Agent service on the IM and Presence database publisher node and then repeat steps 5 to 7.

- To restart the service from the admin CLI run the following command: **`utils service restart Cisco Intercluster Sync Agent`**
- Alternatively, you can restart this service from the Cisco Unified IM and Presence Serviceability GUI.

**Step 9** Verify that the **Certificate Status** now shows "Connection is secure". This means that intercluster syncing is correctly established between the clusters and that the CA certificates that you uploaded are synced to the other clusters.

### What to do next

Upload the signed certificate to each IM and Presence Service node.

## Upload Signed Certificate to Federation Nodes

When the CA certificates have correctly synced to all clusters, you can upload the appropriate signed certificate to each IM and Presence Service federation node. You do not need to upload the certificate to all nodes, only nodes for federation.

**Note** Cisco recommends that you sign all required cup-xmpp-s2s certificates for a cluster and upload them at the same time.

### Procedure

**Step 1** Choose **Cisco Unified IM and Presence OS AdministrationSecurityCertificate Management**.

**Step 2** Click **Upload Certificate/Certificate chain**.

**Step 3** From the Certificate Name drop-down list, choose **cup-xmpp**.

**Step 4** Enter a description for the signed certificate.

**Step 5** Click **Browse** to locate the file to upload.

**Step 6** Click **Upload File**.

**Step 7** Repeat for each IM and Presence Service federation node.

For more information about certificate management, see the *Cisco Unified Communications Operating System Administration Guide*.

### What to do next

Restart the Cisco XCP XMPP Federation Connection Manager service on the affected nodes.

## Restart Cisco XCP XMPP Federation Connection Manager Service

After you upload the cup-xmpp-s2s certificate to each IM and Presence Service federation node, you must restart the Cisco XCP XMPP Federation Connection Manager service on each federation node.

### Procedure

**Step 1** Log into the admin CLI.

**Step 2** Run the following command: **`utils service restart Cisco XCP XMPP Federation Connection Manager`**

**Step 3** Repeat for each federation node.

# Delete Self-Signed Trust Certificates

To support cross navigation for serviceability between nodes in the same cluster, the Cisco Tomcat service trust stores between IM and Presence Service and Cisco Unified Communications Manager are automatically synchronized.

When CA-signed certificates are generated to replace the original self-signed trust certificates on either IM and Presence Service or Cisco Unified Communications Manager the original self-signed trust certificates persist in the service trust store of both nodes. If you want to delete the self-signed trust certificates, you must delete them on both the IM and Presence Service and Cisco Unified Communications Manager nodes.

## Delete Self-Signed Trust Certificates from IM and Presence Service

### Before you begin

**Important** You have configured the IM and Presence Service nodes with CA-signed certificates, and waited 30 minutes for the Cisco Intercluster Sync Agent Service to perform its periodic clean-up task on a given IM and Presence Service node.

### Procedure

**Step 1** Log in to the **Cisco Unified IM and Presence Operating System Administration** user interface, choose **Security** > **Certificate Management**.

**Step 2** Click **Find**.
The **Certificate List** appears.

**Note** The certificate name is composed of two parts, the service name and the certificate type. For example tomcat-trust where tomcat is the service and trust is the certificate type.

The self-signed trust certificates that you can delete are:

- Tomcat — tomcat-trust
- Cup-xmpp — cup-xmpp-trust
- Cup-xmpp-s2s — cup-xmpp-trust
- Cup — cup-trust
- Ipsec — ipsec-trust

**Step 3** Click the link for the self-signed trust certificate you wish to delete.

**Important** Be certain that you have configured a CA-signed certificate for the service associated with the service trust store.

A new window appears that displays the certificate details.

**Step 4** Click **Delete**.

**Note** The **Delete** button only appears for certificates you have the authority to delete.

### What to do next

Repeat the above procedure for each IM and Presence Service node in the cluster and on any intercluster peers to ensure complete removal of unnecessary self-signed trust certificates across the deployment.

If the service is Tomcat, you must check for the IM and Presence Service node's self signed tomcat-trust certificate on the Cisco Unified Communications Manager node. See, Delete Self-Signed Tomcat-Trust Certificates from Cisco Unified Communications Manager, on page 118.

# Delete Self-Signed Tomcat-Trust Certificates from Cisco Unified Communications Manager

There is a self-signed tomcat-trust certificate in the Cisco Unified Communications Manager service trust store for each node in the cluster. These are the only certificates that you delete from the Cisco Unified Communications Manager node.

### Before you begin

Ensure that you have configured the cluster's IM and Presence Service nodes with CA-signed certificates, and you have waited for 30 minutes to allow the certificates to propagate to the Cisco Unified Communications Manager node.

**Procedure**

**Step 1** Log in to the **Cisco Unified Operating System Administration** user interface, choose **Security** > **Certificate Management**.
The **Certificate List** window appears.

**Step 2** To filter the search results, choose **Certificate** and **begins with** from the drop-down lists and then enter tomcat-trust in the empty field. Click **Find**.
The **Certificate List** window expands with the tomcat-trust certificates listed.

**Step 3** Identify the links that contain an IM and Presence Service node's hostname or FQDN in its name. These are self-signed certificates associated with this service and an IM and Presence Service node.

**Step 4** Click the link to an IM and Presence Service node's self-signed tomcat-trust certificate.
A new window appears that shows the tomcat-trust certificate details.

**Step 5** Confirm in the Certificate Details that this is a self-signed certificate by ensuring that the Issuer Name CN= and the Subject Name CN= values match.

**Step 6** If you have confirmed that it is a self-signed certificate and you are certain that the CA-signed certificate has propagated to the Cisco Unified Communications Manager node, click **Delete**.

**Note** The **Delete** button only appears for certificates that you have the authority to delete.

**Step 7** Repeat steps 4, 5, and 6 for each IM and Presence Service node in the cluster.

# SIP Security Settings Configuration on IM and Presence Service

## Configure TLS Peer Subject

When you import an IM and Presence Service certificate, IM and Presence Service automatically attempts to add the TLS peer subject to the TLS peer subject list, and to the TLS context list. Verify the TLS peer subject and TLS context configuration is set up to your requirements.

**Procedure**

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Security** > **TLS Peer Subjects.**

**Step 2** Click **Add New**.

**Step 3** Perform one of the following actions for the Peer Subject Name:

a) Enter the subject CN of the certificate that the node presents.

b) Open the certificate, look for the CN and paste it here.

**Step 4** Enter the name of the node in the Description field.

**Step 5** Click **Save**.

### What to do next

Proceed to configure the TLS context.

## Configure TLS Context

When you import an IM and Presence Service certificate, IM and Presence Service automatically attempts to add the TLS peer subject to the TLS peer subject list, and to the TLS context list. Verify the TLS peer subject and TLS context configuration is set up to your requirements.

### Before you begin

Configure a TLS peer subject on IM and Presence Service.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Security** > **TLS Context Configuration**.

**Step 2** Click **Find**.

**Step 3** Choose **Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context**.

**Step 4** From the list of available TLS peer subjects, choose the TLS peer subject that you configured.

**Step 5** Move this TLS peer subject to Selected TLS Peer Subjects.

**Step 6** Click **Save**.

**Step 7** Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Service Activation**.

**Step 8** Restart the Cisco SIP Proxy service.

**Troubleshooting Tip**

You must restart the SIP proxy service before any changes that you make to the TLS context take effect.

**Related Topics**

Restart SIP Proxy Service, on page 105

# XMPP Security Settings Configuration on IM and Presence Service

## XMPP Security Modes

IM and Presence Service provides increased security for XMPP-based configuration. The following table describes these XMPP security modes. To configure the XMPP security modes on IM and Presence Service, choose **Cisco Unified CM IM and Presence Administration** > **System** > **Security** > **Settings**.

*Table 17: XMPP Secure Mode Descriptions*

| Secure Mode | Description |
|---|---|
| Enable XMPP Client To IM/P Service Secure Mode | If you turn on this setting, IM and Presence Service establishes a secure TLS connection between the IM and Presence Service nodes and XMPP client applications in a cluster. IM and Presence Service turns on this secure mode by default.<br>We recommend that you do not turn off this secure mode unless the XMPP client application can protect the client login credentials in nonsecure mode. If you do turn off the secure mode, verify that you can secure the XMPP client-to-node communication in some other way. |
| Enable XMPP Router-to-Router Secure Mode | If you turn on this setting, IM and Presence Service establishes a secure TLS connection between XMPP routers in the same cluster, or in different clusters. IM and Presence Service automatically replicates the XMPP certificate within the cluster and across clusters as an XMPP trust certificate. An XMPP router will attempt to establish a TLS connection with any other XMPP router that is in the same cluster or a different cluster, and is available to establish a TLS connection. |

| Secure Mode | Description |
|---|---|
| Enable Web Client to IM/P Service Secure Mode | If you turn on this setting, IM and Presence Service establishes a secure TLS connection between the IM and Presence Service nodes and XMPP-based API client applications. If you turn on this setting, upload the certificates or signing certificates for the web client in the cup-xmpp-trust repository on IM and Presence Service.<br>**Caution** If your network and IM and Presence Service node support IPv6, and you enable secure TLS connections to XMPP-based API client applications, you must enable the IPv6 enterprise parameter for the node and enable the IPv6 Ethernet IP setting for Eth0 on each IM and Presence Service node using Cisco Unified IM and Presence Operating System Administration; otherwise, the node attempts to use IPv4 for IP traffic. Any packets that are received from an XMPP-based API client application that has an IPv6 address will not be delivered.<br>The node cannot revert to using IPv4 if the node is configured to use an IPv6 connection to an external database, LDAP server, or Exchange server, or if a federation deployment using IPv6 is configured for the node. |

If you update the XMPP security settings, restart the services. Perform one of these actions:

- Restart the Cisco XCP Connection Manager if you edit **Enable XMPP Client To IM/P Service Secure Mode**. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** to restart this service.
- Restart the Cisco XCP Router if you edit the **Enable XMPP Router-to-Router Secure Mode**. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Network Services** to restart this service.
- Restart the Cisco XCP Web Connection Manager if you edit **Enable Web Client To IM/P Service Secure Mode**. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** to restart this service.

### Related Topics

Configure Secure Connection Between IM and Presence Service and XMPP Clients, on page 123

# Configure Secure Connection Between IM and Presence Service and XMPP Clients

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Security** > **Settings**.

**Step 2** Perform one of the following tasks:

- To establish a secure TLS connection between IM and Presence Service and XMPP client applications in a cluster, choose **Enable XMPP Client To IM/P Service Secure Mode**.

  Cisco recommends that you do not turn off this secure mode unless the XMPP client application can protect the client login credentials in a nonsecure mode. If you do turn off the secure mode, verify that you can secure the XMPP client-to-node communication in some other way.

- To establish a secure TLS connection between IM and Presence Service and XMPP-based API client applications in a cluster, choose **Enable Web Client To IM/P Service Secure Mode**.

  If you turn on this setting, upload the certificates or signing certificates for the web client in the cup-xmpp-trust repository on IM and Presence.

  **Caution** If your network and IM and Presence Service node support IPv6, and you enable secure TLS connections to XMPP-based API client applications, you must enable the IPv6 enterprise parameter for the node and enable the IPv6 Ethernet IP setting for Eth0 on each IM and Presence Service node in the cluster. If the enterprise parameter and Eth0 are not configured for IPv6, the node attempts to use IPv4 for any IPv6 packets that are received from an XMPP-based API client application and those IPv6 packets are not delivered.

  The node cannot revert to using IPv4 if the node is configured to use an IPv6 connection to an external database, LDAP server, or an Exchange server, or if a federation deployment using IPv6 is configured for the node.

**Step 3** Click **Save**.

If you update the XMPP security settings, restart the following service using one of the following actions:

- Restart the Cisco XCP Connection Manager if you edit **Enable XMPP Client To IM/P Service Secure Mode**. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** to restart this service.
- Restart the Cisco XCP Web Connection Manager if you edit **Enable Web Client To IM/P Service Secure Mode**. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** to restart this service.

### What to do next

Proceed to turn on the services that support XMPP clients on the IM and Presence Service node.

### Related Topics

Third-Party Client Integration, on page 15

# Turn On IM and Presence Service Services to Support XMPP Clients

Perform this procedure on each node in your IM and Presence Service cluster.

### Procedure

**Step 1** Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Service Activation**.

**Step 2** Choose the IM and Presence Service node from the **Server** menu.

**Step 3** Turn on the following services:

- Cisco XCP Connection Manager - Turn on this service if you are integrating XMPP clients, or XMPP-based API clients on IM and Presence Service.
- Cisco XCP Authentication Service - Turn on this service if you are integrating XMPP clients, or XMPP-based API clients, or XMPP-based API clients on IM and Presence Service.
- Cisco XCP Web Connection Manager - Optionally, turn on this service if you are integrating XMPP clients, or XMPP-based API clients on IM and Presence Service.

**Step 4** Click **Save**.

**Tip** For XMPP clients to function correctly, make sure you turn on the Cisco XCP Router on all nodes in your cluster.

### Related Topics

Third-Party Client Integration, on page 15

# Enable Wildcards in XMPP Federation Security Certificates

To support group chat between XMPP federation partners over TLS, you must enable wildcards for XMPP security certificates.

By default, the XMPP federation security certificate *cup-xmpp-s2s* contains all domains hosted by the IM and Presence Service deployment. These are added as Subject Alternative Name (SAN) entries within the certificate. You must supply wildcards for all hosted domains within the same certificate. So instead of a SAN entry of “example.com”, the XMPP security certificate must contain a SAN entry of “*.example.com”. The wildcard is needed because the group chat server aliases are sub-domains of one of the hosted domains on the IM and Presence Service system. For example: “conference.example.com”.

**Tip** To view the `cup-xmpp-s2s` certificate on any node, choose **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management** and click on the **cup-xmpp-s2s** link .

### Procedure

**Step 1** Choose **System** > **Security Settings**.

**Step 2** Check **Enable Wildcards in XMPP Federation Security Certificates**.

**Step 3** Click **Save**.

### What to do next

You must regenerate the XMPP federation security certificates on all nodes within the cluster where the Cisco XMPP Federation Connection Manager service is running and XMPP Federation is enabled. This security setting must be enabled on all IM and Presence Service clusters to support XMPP Federation Group Chat over TLS.

# FIPS 140-2 Mode Configuration

## FIPS 140-2 Mode

The Federal Information Processing Standard (FIPS) is a U.S. and Canadian government certification standard that defines requirements that cryptographic modules must follow.

**Warning** At this time, IM and Presence Service has not received FIPS certification. FIPS 140-2 mode is not officially supported until certification is complete.

When you enable FIPS 140-2 mode, IM and Presence Service reboots, runs certification self-tests at start-up, performs the cryptographic modules integrity check, and then regenerates the keying materials. At this point, IM and Presence Service operates in FIPS 140-2 mode.

IM and Presence Service meets FIPS requirements, including the following: it performs startup self-tests and restricts to a list of approved cryptographic functions.

IM and Presence FIPS mode uses FIPS 140-2 level 1 validated OpenSSL FIPS Module version 1.2. The relevant OpenSSL documentation can be found at: http://www.openssl.org/docs/fips/

In IM and Presence Service, you can perform the following FIPS-related tasks:

- Enable FIPS 140-2 mode
- Disable FIPS 140-2 mode
- Check the status of FIPS 140-2 mode

**Note** By default, IM and Presence Service is in non-FIPS mode. You must enable FIPS mode using the CLI. For more information, see the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

# Node Reboot in FIPS 140-2 Mode

When FIPS is enabled or disabled, the IM and Presence Service node is automatically rebooted. When an IM and Presence Service node reboots in FIPS 140-2 mode, it will trigger FIPS startup self-tests in each of the FIPS 140-2 modules after rebooting.

**Caution** If any of these self-tests fail, IM and Presence Service halts. If the startup self-test fails because of a transient error, restarting the IM and Presence Service node fixes the issue. However, if the start self-test error persists, it indicates a critical problem in the FIPS module and the only option it is to use a recovery CD.

# Force Manual Certificate Synchronization

When FIPS is enabled, all certificates are regenerated. However certificates may not be exchanged between intercluster peers. If this situation arises, follow the procedure below to manually sync the certificates between intercluster peers.

**Note** Certificates will not be exchanged between intercluster peers where one peer has FIPS enabled and the other peer does not have FIPS enabled. You can only sync certificates between intercluster peers when all peers are in FIPS mode.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Inter-Clustering**

**Step 2** Select the intercluster peer whose certificate is not present and choose the **Force Manual Sync** option.

**Step 3** Note the configuration details and click **Delete**.

**Step 4** Enable FIPS from the CLI using this command:

```
utils fips enable
```

The node reboots.

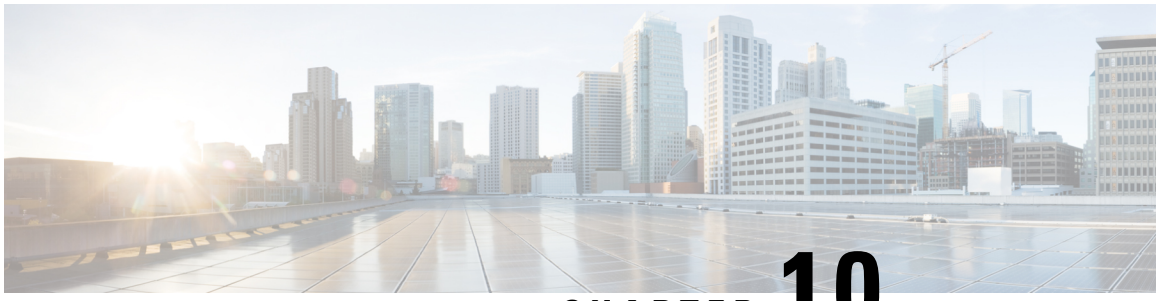
**Step 5** Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Inter-Clustering** and re-add the intercluster peer.

**Step 6** Verify that all certificates are synced.

**Note** This may take several minutes.

**Step 7** If the certificates do not sync after 20 minutes, select the intercluster peer whose certificate is not present and choose the **Force Manual Sync** option.

**Note** Cisco recommends that you allow ten minutes after importing intermediate or root Certificate Authority certificates before importing signed certificates.



CHAPTER 10

# Intercluster Peer Configuration


- Prerequisites for Intercluster Deployment, on page 127
- Intercluster Peer Configuration, on page 128


## Prerequisites for Intercluster Deployment

You configure an intercluster peer between the IM and Presence database publisher nodes in standalone IM and Presence Service clusters. No configuration is required on the IM and Presence Service subscriber nodes in a cluster for intercluster peer connections. Before you configure IM and Presence Service intercluster peers in your network, note the following:

- The intercluster peers must each integrate with a different Cisco Unified Communications Manager cluster.
- You must complete the required multinode configuration in both the home IM and Presence Service cluster, and in the remote IM and Presence Service cluster:
  - Configure the system topology and assign your users as required.
  - Activate the services on each IM and Presence Service node in the cluster.
- You must turn on the AXL interface on all local IM and Presence nodes, and on all remote IM and Presence nodes. IM and Presence Service creates, by default, an intercluster application user with AXL permissions. To configure an intercluster peer, you will require the username and password for the intercluster application user on the remote IM and Presence Service node.
- You must turn on the Sync Agent on the local IM and Presence database publisher node, and on the remote IM and Presence database publisher node. Allow the Sync Agent to complete the user sychronization from Cisco Unified Communications Manager before you configure the intercluster peers.

For sizing and performance recommendations for intercluster deployments, including information on determining a presence user profile, see the IM and Presence Service SRND.

# Intercluster Peer Configuration

## Configure Intercluster Peer

Perform this procedure on the database publisher node of the local IM and Presence Service cluster, and on the database publisher node of the remote IM and Presence Service cluster (with which you want your local cluster to form a peer relationship).

### Before you begin

- Activate the AXL interface on all local IM and Presence Service nodes and confirm that the AXL interface is activated on all remote IM and Presence Service nodes.
- Confirm that the Sync Agent has completed the user synchronization from Cisco Unified Communications Manager on the local and remote cluster.
- Acquire the AXL username and password for the intercluster application user on the remote IM and Presence Service node.
- If you do not use DNS in your network, see topics related to IM and Presence Service default domain and node name values for intercluster deployments.
- Resolve any invalid or duplicate userIDs before proceeding. For more information, see topics related to end-user management and handling.

**Note** For the intercluster peer connection to work properly, the following ports must be left open if there is a firewall between the two clusters:

- 8443 (AXL)
- 7400 (XMPP)
- 5060 (SIP) Only if SIP federation is being used

### Restriction

Cisco recommends that you use TCP as the intercluster trunk transport for all IM and Presence Service clusters.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Inter-Clustering**.

**Step 2** Enter the IP address, FQDN, or hostname of the database publisher node of a remote IM and Presence Service cluster.

**Step 3** Enter the username of the application user on the remote IM and Presence Service node that has AXL permissions.

**Step 4** Enter the associated password of the application user on the remote IM and Presence Service node that has AXL permissions.

**Step 5** Enter the preferred protocol for SIP communication.

**Step 6** (Optional) Enter the External Phone Number Mask value. This is the E.164 mask to apply to Directory Numbers retrieved from the remote cluster.

**Step 7** Click **Save**.

**Step 8** Restart the Cisco XCP Router service on all nodes in the local cluster.

**Step 9** Repeat this procedure on the database publisher node of the remote intercluster peer.

**Tip** If you configure the intercluster peer connection before the Sync Agent completes the user synchronization from Cisco Unified Communications Manager (on either the local or remote cluster), the status of the intercluster peer connection will display as Failed.

If you choose TLS as the intercluster transport protocol, IM and Presence Service attempts to automatically exchange certificates between intercluster peers to establish a secure TLS connection. IM and Presence Service indicates whether the certificate exchange is successful in the intercluster peer status section.

### What to do next

Proceed to turn on the Intercluster Sync Agent.

### Related Topics

Restart Cisco XCP Router Service, on page 58
Node Name Value for Intercluster Deployments, on page 28
IM and Presence Default Domain Value for Intercluster Deployments, on page 29
Default Domain Value for Intercluster Deployments

# Turn On Intercluster Sync Agent

By default, IM and Presence Service turns on the Intercluster Sync Agent parameter. Use this procedure to either verify that the Intercluster Sync Agent parameter is on, or to manually turn on this service.

The Intercluster Sync Agent uses the AXL/SOAP interface for the following:

- to retrieve user information for IM and Presence Service to determine if a user is a local user (on the local cluster), or a user on a remote IM and Presence Service cluster within the same domain.
- to notify remote IM and Presence Service clusters of changes to users local to the cluster.

**Note** You must turn on the Intercluster Sync Agent on all nodes in the IM and Presence Service cluster because in addition to synchronizing user information from the local IM and Presence database publisher node to the remote IM and Presence database publisher node, the Intercluster Sync Agent also handles security between all nodes in the clusters.

### Procedure

**Step 1** Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Network Services**.

**Step 2** Choose the IM and Presence Service node from the Server menu.

**Step 3** Choose **Cisco Intercluster Sync Agent**.

**Step 4** Click **Start**.

### What to do next

Proceed to verify the intercluster peer status.

### Related Topics

Multinode Scalability Feature, on page 23

# Verify Intercluster Peer Status

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Inter-Clustering**.

**Step 2** Choose the peer address from the search criteria menu.

**Step 3** Click **Find**.

**Step 4** Choose the peer address entry that you wish to view.

**Step 5** In the **Intercluster Peer Status** window:

a) Verify that there are check marks beside each of the result entries for the intercluster peer.

b) Make sure that the Associated Users value equals the number of users on the remote cluster.

c) If you choose TLS as the intercluster transport protocol, the Certificate Status item displays the status of the TLS connection, and indicates if IM and Presence Service successfully exchanged security certificates between the clusters. If the certificate is out-of-sync, you need to manually update the tomcat trust certificate (as described in this module). For any other certificate exchange errors, check the Online Help for a recommended action.

**Step 6** Choose **Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter**.

**Step 7** Verify that there are check marks beside the status of each of the intercluster peer connection entries in the InterClustering Troubleshooter section.

# Update Intercluster Sync Agent Tomcat Trust Certificates

If the tomcat certificate status for an intercluster peer is out-of-sync, you need to update the Tomcat trust certificate. In an intercluster deployment this error can occur if you reuse the existing Intercluster Peer Configuration to point to a new remote cluster. Specifically, in the existing Intercluster Peer Configuration window, you change the Peer Address value to point to a new remote cluster. This error can also occur in a fresh IM and Presence Service installation, or if you change the IM and Presence Service host or domain name, or if you regenerate the Tomcat certificate.

This procedure describes how to update the Tomcat trust certificate when the connection error occurs on the local cluster, and the corrupt Tomcat trust certificates are associated with the remote cluster.

**Procedure**

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Inter-Clustering.**

**Step 2** Click **Force Sync** to synchronize certificates with the remote cluster.

**Step 3** In the confirmation window that displays, choose **Also resync peer's Tomcat certificates**.

**Step 4** Click **OK**.

**Note** If there are any certificates that have not synced automatically, go to the Intercluster Peer Configuration window and all certificates marked with an x are the missing certificates which you need to manually copy.

# Delete Intercluster Peer Connections

Use this procedure if you want to remove an intercluster peer relationship.

**Procedure**

**Step 1** Log in to the IM and Presence Service database publisher node.

**Step 2** From Cisco Unified CM IM and Presence Administration, choose **Presence** > **Inter-Clustering**.

**Step 3** Click **Find** and select the intercluster peer that you want to remove.

**Step 4** Click **Delete**.

**Step 5** Restart the **Cisco XCP Router**:

a) Log in to Unified IM and Presence Serviceability and choose **Tools** > **Control Center - Network Services**.
b) From the **Server** list, choose the database publisher node and click **Go**.
c) Under **IM and Presence Services**, select **Cisco XCP Router** and click **Restart**.

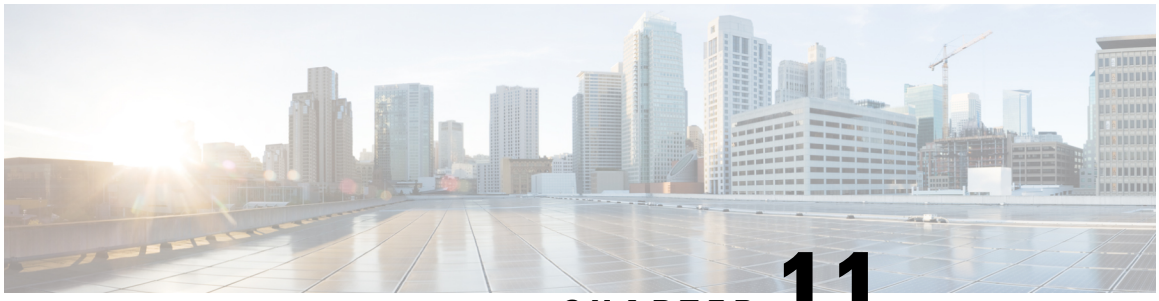
**Step 6** Repeat these steps on the peer cluster.

**Note** If you are removing an intercluster peer from an intercluster network with multiple clusters, you must repeat this procedure for each peer cluster that remains in the intercluster network. This means that, on the cluster that is being removed, there will be as many cycles of **Cisco XCP Router** restarts as there are peer cluster connections that are being broken.

PART III

# Feature Configuration


- Availability and Instant Messaging on IM and Presence Service Configuration , on page 135
- OpenAM Single Sign-On, on page 143



CHAPTER 11

# Availability and Instant Messaging on IM and Presence Service Configuration


- Availability Setup on IM and Presence Service, on page 135
- IM Setup On IM and Presence Service, on page 138
- Stream Management, on page 140


# Availability Setup on IM and Presence Service

## Turn On or Off Availability Sharing for IM and Presence Service Cluster

This procedure describes how to turn on or off availability sharing for all client applications in a IM and Presence Service cluster.

Availability sharing is turned on by default on IM and Presence Service.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Settings** > **Standard Configuration**.

**Step 2** Configure the availability setting. Perform one of the following actions:

- To turn on availability sharing in the IM and Presence Service cluster, check **Enable availability sharing**. If you turn on this setting, IM and Presence Service shares availability information for a user amongst all users in the cluster, based on the policy settings for that user.

  The default policy setting for a user is to allow all other users view their availability. Users configure their policy settings from the Cisco Jabber client.

- To turn off availability sharing for all clients in the IM and Presence Service cluster, uncheck **Enable availability sharing.**. If you turn off this setting, IM and Presence Service does not share any availability to other users in the IM and Presence Service cluster, nor does it share availability information it receives from outside the cluster. Users can only view their own availability status.

**Step 3** Click **Save**.

**Step 4** Restart the following services:

a) Cisco XCP Router

b) Cisco Presence Engine

**Tip**
- When you turn off availability sharing, a user can view their own availability status on the client application; the availability status for all other users are greyed out.
- When you turn off availability sharing, when a user enters a chat room, their availability status shows a status of "Unknown" with a green icon.

# Configure Ad-Hoc Presence Subscription Settings

**Note** These settings allow users to initiate ad-hoc presence subscriptions to users that are not on their contact list.

**Procedure**

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Settings** > **Standard Configuration**.

**Step 2** Check **Enable ad-hoc presence subscriptions** to turn on ad-hoc presence subscriptions for Cisco Jabber users.

**Step 3** Set the maximum number of active ad-hoc subscriptions that IM and Presence Service permits at one time. If you configure a value of zero, IM and Presence Service permits an unlimited number of active ad-hoc subscriptions.

**Step 4** Set the time-to-live value (in seconds) for the ad-hoc presence subscriptions.

When this time-to-live value expires, IM and Presence Service drops any ad-hoc presence subscriptions and no longer temporarily monitors the availability status for that user.

**Note** If the time-to-live value expires while the user is still viewing an instant message from a ad-hoc presence subscription, the availability status that displays may not be current.

**Step 5** Click **Save**.

You do not have to restart any services on IM and Presence Service for this setting, however Cisco Jabber users will have to sign out, and sign back in to retrieve the latest ad-hoc presence subscriptions settings on IM and Presence Service.

# Configure Maximum Contact List Size Per User

You can configure the maximum contact list size for a user; this is the number of contacts the user can add to their contact list. This setting applies to the contact list on Cisco Jabber client applications and on third-party client applications.

Users who reach the maximum number of contacts are unable to add new contacts to their contact list, nor can other users add them as a contact. If a user is close to the maximum contact list size, and the user adds a group of contacts that pushes the contact list over the maximum number, IM and Presence Service does not add the surplus contacts. For example, if the maximum contact list size on IM and Presence Service is 200. A user has 195 contacts and attempts to add 6 new contacts to the list, IM and Presence Service adds five contacts and does not add the sixth contact.

**Tip** The System Troubleshooter in Cisco Unified CM IM and Presence Administration indicates if there are users who have reached the contact list limit.

If you are migrating users to IM and Presence Service, Cisco recommends that you set the Maximum Contact List Size and Maximum Watchers settings to Unlimited while importing user contact lists. This ensures that each migrated user contact list is fully imported. After all users have migrated, you can reset the Maximum Contact List Size and Maximum Watchers settings to the preferred values.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Settings**.

**Step 2** Edit the value of the **Maximum Contact List Size (per user)** setting.

The default value is 200.

**Tip** Check the **No Limit** check box to allow an unlimited contact list size.

**Step 3** Click **Save**.

**Step 4** Restart the Cisco XCP Router service.

### Related Topics

Restart Cisco XCP Router Service, on page 58

# Configure Maximum Number of Watchers Per User

You can configure the number of watchers for a user, specifically the maximum number of people that can subscribe to see the availability status for a user. This setting applies to the contact list on Cisco Jabber clients and on third-party clients.

If you are migrating users to IM and Presence Service, Cisco recommends that you set the Maximum Contact List Size and Maximum Watchers settings to Unlimited while importing user contact lists. This ensures that each migrated user contact list is fully imported. After all users have migrated, you can reset the Maximum Contact List Size and Maximum Watchers settings to the preferred values.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Settings**.

**Step 2** Edit the value of the **Maximum Watchers (per user)** setting.

The default value is 200.

**Tip** Check the **No Limit** check box to allow an unlimited number of watchers.

**Step 3** Click **Save**.

**Step 4** Restart the Cisco XCP Router service.

# IM Setup On IM and Presence Service

## Turn On or Off Instant Messaging for IM and Presence Service Cluster

This procedure describes how to turn on or off instant message capabilities for all client applications in a IM and Presence Service cluster. Instant message capabilities is turned on by default on IM and Presence Service.

⚠

**Caution** When you turn off instant message capabilities on IM and Presence Service, all group chat functionality (ad hoc and persistent chat) will not work on IM and Presence Service. We recommend that you do not turn on the Cisco XCP Text Conference service or configure an external database for persistent chat on IM and Presence Service.

### Procedure

**Step 1** Log in to **Cisco Unified CM IM and Presence Administration**, choose **Messaging** > **Settings**.

**Step 2** Configure the instant messaging setting. Do one of the following actions:

- To turn on instant message capabilities for client applications in the IM and Presence Service cluster, check **Enable instant messaging.**. If you turn on this setting, local users of client applications can send and receive instant messages.
- To turn off instant message capabilities for client applications in the IM and Presence Service cluster, uncheck **Enable instant messaging.**.

  **Note** If you turn off this setting, local users of client applications cannot send and receive instant messages. Users can only use the instant messaging application for availability and phone operations. If you turn off this setting, users do not receive instant messages from outside the cluster.

**Step 3** Click **Save**.

**Step 4** Restart the Cisco XCP Router service.

## Turn On or Off Offline Instant Messaging

By default IM and Presence Service stores (locally) any instant messages that are sent to a user when they are offline, and IM and Presence Service delivers these instant messages to the user the next time they sign in to

the client application. You can turn off (suppress) this feature so IM and Presence Service does not store offline instant messages.

**Note** IM and Presence Service limits offline messages to 100 per user up to a maximum of 30000 per node.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **Settings**.

**Step 2** Configure the offline instant messaging. Perform one of the following actions:

- To turn off the storage of offline instant messages on IM and Presence Service, check **Suppress Offline Instant Messaging.**. If you check this setting, any instant messages that are sent to a user when they are offline, IM and Presence Service does not deliver these instant messages to the user the next time they sign in to the client application.
- To turn on the storage of offline instant messages on IM and Presence Service, uncheck **Suppress Offline Instant Messaging.**. If you uncheck this setting, any instant messages that are sent to a user when they are offline, IM and Presence Service delivers these instant messages to the user the next time they sign in to the client application.

**Step 3** Click **Save**.

# Allow Clients to Log Instant Message History

You can prevent or allow users to log instant message history locally on their computer. On the client side, the application must support this functionality; it must enforce the prevention of instant message logging.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **Settings**.

**Step 2** Configure the log instant message history setting as follows:

- To allow users of client applications to log instant message history on IM and Presence Service, check **Allow clients to log instant message history (on supported clients only)**.
- To prevent users of client applications from logging instant message history on IM and Presence Service, uncheck **Allow clients to log instant message history (on supported clients only)**.

**Step 3** Click **Save**.

# Allow Cut and Paste in Instant Messages

You can prevent or allow users to log instant message history locally on their computer. On the client side, the application must support this functionality; it must enforce the prevention of instant message logging.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **Settings**.

**Step 2** Configure the cut and paste in instant messages setting as follows:

- To allow users of client applications to cut and paste in instant messages, check **Allow cut & paste in instant messages**.
- To prevent users of client applications from cutting and pasting in instant messages, uncheck **Allow cut & paste in instant messages**.

**Step 3** Click **Save**.

# Stream Management

The IM and Presence Service supports Stream Management for instant messaging. Stream Management is implemented using the XEP-0198 specification, which defines an Extensible Messaging and Presence Protocol (XMPP) extension for active management of an XML stream between two XMPP entities, including features for stanza acknowledgements and stream resumption. For more information about XEP-0198, see the specification at http://xmpp.org/extensions/xep-0198.html

If there is a temporary loss of communication between IM and Presence Service and Cisco Jabber, Stream Management ensures that any instant messages that are sent during the communications outage are not lost. A configurable timeout period determines how such messages are handled:

- If Cisco Jabber reestablishes communication with IM and Presence Service within the timeout period, the messages are resent.
- If Cisco Jabber does not reestablish communication with IM and Presence Service within the timeout period, the messages are returned to the sender.
- Messages that are sent after the timeout period lapses are stored offline and delivered when Cisco Jabber resumes communication with IM and Presence Service.

Stream Management is enabled by default on a cluster-wide basis. However, you can use the Stream Management service parameters to configure the feature.

# Configure Stream Management

Use this procedure to cofigure Stream Management (XEP-0198) on the IM and Presence Service.

### Procedure

**Step 1** From Cisco Unified CM IM and Presence Administration, choose **System** > **Service Parameters**.

**Step 2** From the **Server** drop-down, choose an IM and Presence node.

**Step 3** From the **Service** drop-down, choose **Cisco XCP Router**.

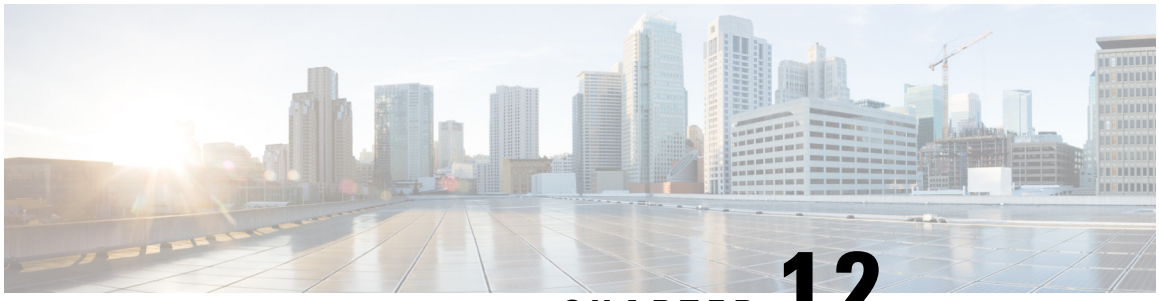
**Step 4** Set the **Enable Stream Management** service parameter to **Enabled**.

**Step 5** Under **Stream Management Parameters (Clusterwide)**, configure any of the Stream Management parameters:

*Table 18: Stream Management Service Parameters*

| Service Parameter | Description |
|---|---|
| Enable Stream Management | Enables or disables Stream Management cluster-wide. The default setting is Enabled. |
| Stream Management Timeout | The timeout controls how long a session (whose connection has been severed) will allow for a resume (in seconds) before giving up. If the client attempts to negotiate a longer timeout (or does not specify a desired timeout) this maximum will apply.<br>Any messages that are sent after this timeout ends and before Cisco Jabber logs in again with IM and Presence Service are stored offline and resent after relogin.<br>The range is 30 seconds—90 seconds. The default value is 60 seconds. |
| Stream Management Buffer | Defines the maximum number of packets (packet history) that will be kept in buffer for a stream management-enabled session. A stream resume will fail if the client needs more history than what is available in the buffer.<br>The range is 5—150 packets with a default value of 100 packets. |
| Acknowledgement Request Rate | Defines the number of stanzas that the server sends before asking the client to provide the count of the last stanza received. A smaller number makes for more network traffic, but helps the server prune the stanza history buffer and reduces memory used.<br>The range is 1—64 stanzas with a default value of 5.<br>**Note** A smaller Acknowledgement Request Rate leads to increased network traffic, but reduced memory use. |

**Step 6** Click **Save**.



CHAPTER 12

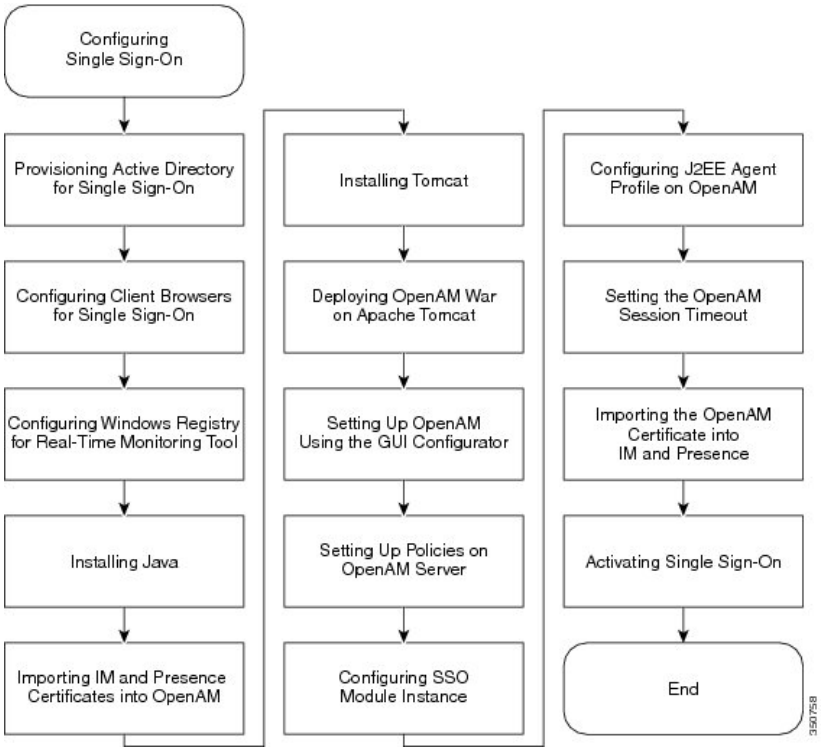
# OpenAM Single Sign-On


- Single Sign-On Setup Task List, on page 143
- Single Sign-On Setup Preparation, on page 145
- Single Sign-On Setup and Management Tasks, on page 147


## Single Sign-On Setup Task List

The following figure provides the sequence of tasks that are required to successfully configure SSO. Cisco recommends that you complete each task outlined in this flow in the order indicated.

***Figure 12: Task Flow for Single Sign-On setup***




The following table lists the tasks to configure Single Sign-On.

*Table 19: Task List for Single Sign-On Setup*

| Item | Task |
|---|---|
| 1 | Provision a new user account for the OpenAM server to be used for Single Sign-On on the Active Directory (AD) server.<br>**Note** Ensure the Windows Server 2008 supported tools are installed before proceeding. |
| 2 | Configure client browsers for Single Sign-On. See topics related to third-party software and system requirements for a list of web browsers and supported versions. |
| 3 | Configure Microsoft Windows Registry for Real-Time Monitoring Tool (RTMT). |
| 4 | Install Java Runtime Environment (JRE).<br>**Note** A Java keystore and the associated security certificates are required for secure connections to the OpenAM server, which runs on an Apache Tomcat. The procedure to install Java are different depending if you use self-signed or Certificate Authority (CA) signed security certificates. |
| 5 | Import IM and Presence Service certificate into OpenAM. Do this for each IM and Presence Service node that is to use Single Sign-On. |
| 6 | Install the Apache Tomcat Web Container on the OpenAM Windows server. |
| 7 | Deploy OpenAM War on Apache Tomcat. |
| 8 | Set up OpenAM using the GUI Configurator. You access the OpenAM web-based administration interface using a web browser by entering the FQDN of the OpenAM server. |
| 9 | Set up policies on the OpenAM server. You must follow the policy rules that are defined in the procedure.<br>**Note** You must use the FQDN of the IM and Presence Service node to access the Cisco Unified CM IM and Presence Administration/User interface. Do not use the hostname of the node. |
| 10 | Configure SSO module instance. A single module instance can be shared by multiple IM and Presence Service nodes for SSO if the same Active Directory domain is used throughout the deployment. |
| 11 | Configure J2EE agent profile on OpenAM. You must configure an associated J2EE Agent Profile on the OpenAM server for the J2EE Agent of each IM and Presence Service node using SSO. |
| 12 | Set the OpenAM session timeout to a value that is higher than the session timeout parameter setting for the IM and Presence Service node. |
| 13 | Import the OpenAM certificate into the tomcat-trust trust store for each IM and Presence Service node using SSO. |

| Item | Task |
|---|---|
| 14 | Activate Single Sign-On.<br>Enabling SSO affects service. Cisco highly recommends that you enable SSO during a maintenance window. |

You can perform these additional tasks that are not required to setup up Single Sign-On:

- Disable Single Sign-On
- Uninstall OpenAM on Windows
- Set the debug level
- Troubleshoot Single Sign-On

### Related Topics

Disable Single Sign-On, on page 173
Uninstall OpenAM on Windows, on page 173
Set Debug Level, on page 174
Troubleshooting Single Sign-On

# Single Sign-On Setup Preparation

## Third-Party Software and System Requirements for Single Sign-On

The Single Sign-On (SSO) feature makes use of a third-party application from ForgeRock called OpenAM. Support for the OpenAM application is available only from ForgeRock. The software requirements and configuration guidelines to enable the SSO feature to work with OpenAM are provided. The installation of OpenAM on a Windows Server is also outlined.

Advanced OpenAM configurations, such as deploying OpenAM behind load balancers or the use of session replication between OpenAM servers, have not been validated. For information about these advanced features, see http://www.cisco.com/en/us/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf.

The SSO feature requires the following third-party applications:

- Microsoft Windows Server 2008 R2
- Microsoft Active Directory
- ForgeRock Open Access Manager (OpenAM) Version 9.0

**Note** The SSO feature uses Active Directory and OpenAM in combination to provide SSO access to web-based client applications.

These third-party products must meet the following configuration requirements:

- Active Directory must be deployed in a Windows domain-based network configuration, not just as an LDAP server.
- The OpenAM server must be accessible on the network to all client systems and the Active Directory server.
- The Active Directory (Domain Controller) server, Windows clients, IM and Presence Service nodes, and OpenAM server must be in the same domain.
- DNS must be enabled in the domain.
- The clocks of all the entities participating in SSO must be synchronized.

See the third-party product documentation for more information about those products.

The following table provides a list of the software applications and versions that were used and tested in the procedures that appear in this chapter. In order for you to receive Cisco support, Cisco recommends that you adhere to these suggested requirements during your configuration.

***Table 20: Software Versions***

| Component | Version |
|---|---|
| Active Directory | Windows Server 2008 R2 Enterprise |
| Desktop Operating System for end user clients | Windows 7 Professional (SP1) |
| OpenAM | OpenAM Release 10.0<br>http://forgerock.org/openam-archive.html<br>For more information:<br>https://wikis.forgerock.org/confluence/display/openam/OpenAM+Release+Documentation |
| OpenAM underlying Operating System | Windows Server 2008 R2 Enterprise |
| Apache Tomcat on which OpenAM is loaded | Tomcat 6.0.2.0, Tomcat 7.0.29<br>http://archive.apache.org/dist/tomcat/tomcat-7/v7.0.29/bin |
| Java Development Kit (JDK) of OpenAM underlying Operating System | JDK 7 Update |
| Web browser | Internet Explorer 8, 9 and Mozilla Firefox 10, 11 |

# Important Information Before Single Sign-On Setup

**Note** From Release 10.0(1) and later, Agent Flow SSO is not compatible with FIPS mode.

To help ensure that the configuration of SSO runs as smoothly as possible, Cisco recommends that you gather the following information before you configure SSO:

- Ensure that the installed base operating system (such as Windows server) for the OpenAM system is running.
- Make a note of the Fully Qualified Domain Name (FQDN) of the Windows Active Directory (AD) server to which the OpenAM will be integrating.
- Make a note of the FQDN of the Windows server on which OpenAM is to be installed.
- Ensure that the IM and Presence Web Application timeout is set consistently across all IM and Presence nodes in the cluster and make note of that timeout value. You can use the Cisco Unified CM IM and Presence Administration CLI to verify the timeout value by entering the following command: show webapp session timeout. For more information, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.
- Ensure that Cisco Unified Communications Manager has been configured to sync users from Active Directory (AD) using "sAMAccountName" as the LDAP Attribute for User ID. For more information, see the "DirSync Service" section in the *Cisco Unified Communications Manager System Guide*.

# Single Sign-On Setup and Management Tasks

## Provision Active Directory for Single Sign-On

### Before you begin

Ensure that you have Windows Server 2008 support tools installed. Support tools are installed on Windows Server 2008 by default.

### Procedure

**Step 1** Log in to the Active Directory (AD) server.

**Step 2** From the **Start** menu, choose **Programs** > **Administration Tools** and choose **Active Directory Users and Computers**.

**Step 3** Right-click **Users** and choose **New** > **User**.

**Step 4** In the **User logon name** field, enter the OpenAM server hostname.

**Note** The OpenAM server hostname should not include the domain name.

**Step 5** Click **Next**.

**Step 6** Enter and confirm a password.

This password is required in Step 10.

**Step 7** Uncheck the **User must change password at next login** check box.

**Step 8** Click **Next**.

**Step 9** Click **Finish** to finish creating the new user account.

**Step 10** Create a keytab file on the AD server using the following command from the command prompt.

```
ktpass -princ HTTP/<hostname>.<domainname>@<DCDOMAIN> -pass <password> -mapuser <userName>
 -out <hostname>.HTTP.keytab -ptype KRB5_NT_PRINCIPAL -target <DCDOMAIN>
```

**Example:**

```
ktpass -princ HTTP/server1.cisco.com@CISCO.COM -pass cisco!123 -mapuser server1 -out
server1.HTTP.keytab -ptype KRB5_NT_PRINCIPAL -target CISCO.COM
```

where:

| Parameter | Description |
|---|---|
| hostname | The hostname (not the FQDN) of your OpenAM server. For example, server1 |
| domainname | The AD domain name. For example, cisco.com. |
| DCDOMAIN | The AD domain name, entered in block capitals. In this example, CISCO.COM. |
| password | The password value that was specified when you created the user account for the OpenAM server earlier in this procedure. |
| userName | The AD account name entered in Step 4. This value should be the OpenAM server hostname. In this example, server1. |

**Note** Record the *-princ* value for use in later procedures.

**Step 11** After successful creation of the keytab file, copy the keytab file to a location on the OpenAM server; this path will later be specified in OpenAM configuration. Create a directory under `C:\>` and copy the above keytab file. For example, `C:/keytab/server1.HTTP.keytab`.

# Client Browser Setup for Single Sign-On

To use SSO for a browser-based client application, you must configure the web browser. The following sections describe how to configure client browsers to use SSO.

## Configure Internet Explorer for Single Sign-On

The SSO feature supports Windows clients running Internet Explorer. Perform the following procedure to configure Internet Explorer to use SSO.

**Tip** For information about supported web browsers, see topics related to third-party software and system requirements for Single Sign-On.

**Procedure**

**Step 1** Choose **Tools** > **Internet Options** > **Advanced** tab.

**Step 2** Click **Enable Integration Windows Authentication**.

**Step 3** Click **OK** to save the changes.

**Step 4** Restart Internet Explorer.

**Step 5** Choose **Tools** > **Internet Options** > **Security** > **Local Intranet** and click **Custom Level**.

**Step 6** Under **User Authentication**, check **Automatic Logon Only in Intranet Zone**.

**Step 7** Click **OK**.

**Step 8** Click **Sites**.

**Step 9** Check **Automatically detect intranet network**.

**Step 10** Click **Advanced**.

**Step 11** Fill in the **Add this web site to the zone** field with the FQDN of the OpenAM server using the following format: https://OpenAM_FQDN.

**Step 12** Click **Add**.

**Step 13** Click **Close**.

**Step 14** Click **OK**.

**Step 15** Uncheck **Enable Protected Mode**.

**Step 16** Click **Apply**.

**Step 17** Click **OK**.

**Step 18** Restart Internet Explorer.

**Step 19** Open the Windows Registry Editor. Perform one of the following actions:

- For Windows XP or Windows 2008, choose **Start** > **Run** and type *regedit*.
- For Windows Vista and Windows 7.0, click **Start** and type *regedit*. For Windows Vista, you must click **Continue**.

**Step 20** Under registry key *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA*, right-click and choose **New** > **DWORD (32-bit) value** and rename it to be *SuppressExtendedProtection*.

Only an administrator can set the DWORD.

**Step 21** Set the following values:

- Base: hexadecimal
- Value data: 002

The newly created DWORD appears in the LSA directory list as follows:

- Name: SuppressExtendedProtection
- Type: REG_DWORD
- Value: 0x00000002 (2)

**Related Topics**

Third-Party Software and System Requirements for Single Sign-On, on page 145

## Configure Firefox for Single Sign-On

The SSO feature supports Windows clients running Firefox.

**Tip** For a list of supported web browsers, see topics related to third-party software and system requirements for Single Sign-On.

**Procedure**

**Step 1** Open Firefox and enter the following URL: **about:config**

**Step 2** Scroll down to **network.negotiate-auth.trusted-uris**, right-click that Preference Name, and choose **Modify**.

**Step 3** Set the string value to your domain (for example, cisco.com).

**Step 4** Click **OK**.

**Related Topics**

Third-Party Software and System Requirements for Single Sign-On, on page 145

# Configure Windows Registry for the Real-Time Monitoring Tool

Configuring SSO for the Real-Time Monitoring Tool (RTMT) is optional. To achieve this configuration, you must create a new registry key on your Desktop client (Windows XP or Windows 7).

**Note** An administrator must set the `allowtgtsessionkey` registry key entry for the Desktop client.

This new registry key should be stored at either of the locations below, depending on your Operating system:

**Procedure**

**Step 1** Go to either of the following locations, depending on your operating system:

- Windows XP - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos`
- Windows Vista/Windows 7 - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters`

**Step 2** Right-click the folder, choose **New** > **DWORD (32-bit) Value**, and rename it to be *allowtgtsessionkey*.

**Step 3** Right-click the newly created registry key and choose **Modify**.

**Step 4** In the **Value data** field, enter `1`.

# Install Java

OpenAM requires a Java Runtime Environment (JRE) to operate. The following procedure provides details for installing the JRE on your Windows server, forming the OpenAM base system.

### Procedure

**Step 1** Go to http://www.oracle.com/technetwork/java/archive-139210.html.

**Step 2** Download the recommended version of the JDK installation file by choosing the executable file that corresponds to your server architecture (Windows x86 or Windows x64).

**Note** For a list of recommended software versions, see topics related to third-party software and system requirements for Single Sign-On.

**Step 3** Double-click the downloaded file to begin the installation of the JDK and accept the default values provided in the Installation wizard.

**Note** Make a note of the installation directory. This value indicates the location of the Java JRE and can be used to infer the JDK directory path. Example values may be as follows, depending on the JDK values that are used:

- `jre-path=C:\Program Files\Java\jre7`
- `jdk-path=C:\Program Files\Java\jdk1.7.0_03`

**Step 4** A Java keystore and the associated security certificates are required to facilitate secure connections to the OpenAM server, which runs on Apache Tomcat. Perform one of the following actions:

- If you use a self-signed security certificate for OpenAM/Tomcat, proceed to Step 5.
- If you use a Certificate Authority (CA) signed security certificate for OpenAM/Tomcat, proceed to Step 11.

**Step 5** Create the Java keystore by opening a Windows command prompt on the Windows Server, and executing the following command: `C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -genkey -alias tomcat -keyalg RSA -validity 1825 -keystore C:\keystore`

This command creates the Java keystore file at the following location: `C:\keystore`. The keytool command is located in the <jdk-path>/bin directory, the exact path to the keytool command in the preceding command may vary depending on the JDK version used. For information about the keytool command, see http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html.

**Step 6** When you are prompted for a keystore password, enter a valid keystore password. For example, "cisco!123". Make a note of the keystore password as it is required to access the keystore.

**Note** Do not use example values on the production server; Use a unique password value for the keystore. This password will be visible in plain text in the Apache Tomcat configuration files and utilities.

**Step 7** When you are prompted to enter the first name and last name, enter the FQDN (hostname.domainname) of the OpenAM server.

You are also prompted to enter your organization unit name, organization name, city or locality, state or province, and two-letter country code.

**Step 8** When you are prompted for a Tomcat password, press RETURN to use the same keystore password value for the Tomcat private key. The Java keystore is created at the location specified in the keytool command. For example, `C:\keystore`.

**Step 9** You can view the Tomcat certificate in the keystore using the following command:

**Example:**

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -list -v -alias tomcat -keystore
C:\keystore
```

**Step 10** *If you chose to use a self-signed security certificate for Tomcat, proceed to the end of this procedure and consider this task complete.*

**Step 11** Create a Java keystore to store Certificate Authority (CA)-signed security certificates for OpenAM/Tomcat. Open a command prompt on the Windows Server and execute the following command:

**Example:**

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -genkey -alias tomcat -keyalg RSA
-validity 1825 -keystore C:\keystore
```

This command creates the Java keystore file at the following location: C:\keystore. The keytool command is located in the <jdk-path>/bin directory, the exact path to the keytool command in the example provided above may vary depending on the JDK version used. For information about the keytool command, see http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html.

**Step 12** When you are prompted for a keystore password, enter a valid keystore password. For example, “cisco!123”. Make a note of the keystore password as it is required to access the keystore.

Do not use example values on the production server; Use a unique password value for the keystore. This password will be visible in plain text in the Apache Tomcat configuration files and utilities.

**Step 13** When you are prompted to enter the first name and last name, enter the FQDN (hostname.domainname) of the OpenAM server.

You are also prompted to enter your organization unit name, organization name, city or locality, state or province, and two-letter country code.

**Step 14** When you are prompted for a Tomcat password, press RETURN to use the same keystore password value for the Tomcat private key. The Java keystore is created at the location specified in the keytool command. For example, `C:\keystore`.

**Step 15** You can view the Tomcat certificate in the keystore using the following command:

**Example:**

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -list -v -alias tomcat -keystore
C:\keystore
```

**Step 16** Generate a certificate signing request (CSR) for this OpenAM/Tomcat instance. Open a command prompt on the Windows Server and execute the following command .

**Example:**

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -certreq -keyalg RSA -alias tomcat
-file certreq.csr -keystore C:\keystore
```

**Step 17** Submit the CSR to your CA, request the CA to sign the CSR and create a certificate. Obtain and copy the following certificates to the Windows Server that is going to be the OpenAM server:

- CA signing or root certificate
- Intermediate signing certificates (if applicable)
- Newly signed OpenAM/Tomcat certificate

**Note** Refer to the CA documentation for instructions about completing these tasks.

**Step 18** Import the CA signing or root certificate into the Java keystore that was created in Step 11. Open a command prompt on the Windows Server and execute the following command, answering "yes" to the prompt, "Trust this certificate?":

**Example:**

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -import -alias
root -trustcacerts -file <filename_of_the_CA_root_certificate> -keystore
C:\keystore
```

**Step 19** You can view the CA signing certificate in the keystore using the following command:

**Example:**

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -list -v -alias
root -keystore C:\keystore
```

**Step 20** Import any other intermediate signing certificates (if applicable) into the Java keystore that was created in Step 11. Open a command prompt on the Windows Server and execute the following command, answering "yes" to the prompt, "Trust this certificate?":

**Example:**

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -import -alias
inter01 -trustcacerts -file
<filepath_of_the_intermediate_signing_certificate> -keystore C:\keystore
```

The -alias option must be updated with a value unique to the Java keystore, otherwise the import operation will result in an error similar to the following: "Certificate not imported, alias<inter01> already exists."

**Step 21** You can view any of the intermediate signing certificates in the keystore using the following command:

**Example:**

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -list -v -alias
inter01 C:\keystore
```

The -alias option must be updated with the corresponding alias value for the intermediate certificates you wish to view. The above example uses a sample alias value of "inter01".

**Step 22** Import the newly signed certificate OpenAM/Tomcat certificate into the Java keystore that was created in Step 11. Open a command prompt on the Windows Server and execute the following command:

**Example:**

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -import -alias
tomcat -file <new_certificate_filepath> -keystore C:\keystore
```

**Step 23** You can view the new OpenAM/Tomcat certificate in the keystore using the following command:

**Example:**

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -list -v -alias
tomcat -keystore C:\keystore
```

The issuer of this new Tomcat certificate is the CA or one of the intermediate CAs (if applicable).

**Related Topics**

Third-Party Software and System Requirements for Single Sign-On, on page 145
Import OpenAM Certificate Into IM and Presence Service, on page 166

# Import IM and Presence Certificates Into OpenAM

OpenAM must communicate with a J2EE Agent component that exists on each IM and Presence Service node for which SSO is enabled. This communication is over an encrypted channel and therefore the necessary security certificates must be imported onto OpenAM.

The OpenAM server must trust the security certificate presented by each IM and Presence Service node for the encrypted communication channel to be established. OpenAM trusts a security certificate by importing the required security certificates into the OpenAM keystore. A given IM and Presence Service node can present one of two types of security certificate:

- Self-signed certificate
- CA-signed certificate

**Note** The IM and Presence Service Tomcat certificate and tomcat-trust trust store contain the security certificates of interest for secure communication with OpenAM. The other IM and Presence Service certificates and associated trust stores are not relevant for SSO (for example, cup, cup-xmpp, cup-xmpp-s2s or ipsec).

If your SSO-enabled IM and Presence Service deployment is configured to use self-signed certificates, each of the self-signed certificates must be imported into OpenAM.

If your SSO-enabled IM and Presence Service deployment is configured to use CA-signed certificates, the CA root certificate and any associated intermediate certificates must be imported into OpenAM. If you are also using a CA-signed certificate for your OpenAM/Tomcat instance, the required CA root and intermediate certificates may already be imported into the OpenAM keystore.

This procedure provides the details on how to identify the type of security certificate being used by the IM and Presence Service node and how to import the certificates into the OpenAM keystore that was created when you installed Java.

### Procedure

**Step 1** Sign in to Cisco Unified IM and Presence Operating System Administration for the IM and Presence Service node for which SSO is to be enabled.

**Step 2** Choose **Security** > **Certificate Management**.

**Step 3** Click **Find**.

**Step 4** Locate the entry with **Certificate Name** of **tomcat**.

**Step 5** Examine the Description column of the tomcat certificate.

**Step 6** If the description states that the tomcat certificate is **Self-signed certificate generated by system**, this indicates that the IM and Presence Service node is using a self-signed certificate. If this description is not present, a CA-signed certificate can be assumed.

- If the certificate is self-signed, proceed to Step 7.
- If the certificate is CA-signed, proceed to Step 13.

**Step 7** Click the **tomcat.pem** link.

**Step 8** Click **Download** to download the tomcat.pem file.

**Step 9** Copy the **tomcat.pem** file to the OpenAM server.

**Step 10** Import the **tomcat.pem** file as a trusted certificate into the keystore that was created on the OpenAM server when you installed Java. Open a command prompt on the Windows server (OpenAM) and execute the following command, updating the command with the values for your keytool command path and keystore location as applicable for your environment, and answer **Yes** to the prompt "Trust this certificate?": `C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keystool.exe" -import -alias cup01 -trustcacerts -file <full_filepath_of_the_tomcat.pem> -keystore C:\keystore`

**Note** The -alias option must be updated with a value unique to the Java keystore, otherwise the import operation will result in an error similar to the following: "Certificate not imported, alias <cup01> already exists."

**Step 11** You can view the **tomcat.pem** in the keystore using the following command, updating the command with the values for your keytool command path and keystore location as applicable for your environment:

```
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keystool.exe -list -v -alias cup01 -keystore C:\keystore
```

**Note** The -alias option must match the value used in Step 10, otherwise the keystore entry may not be found.

**Step 12** Skip to Step 16.

**Step 13** Identify the CA root certificates and any intermediate certificates that were used to sign your IM and Presence Service Tomcat certificate. Download the required certificates (CA root certificates and any intermediate certificates) from your CA to your OpenAM server.

**Step 14** Import these certificates into the keystore on the OpenAM server as trusted certificates. Open a command prompt on the Windows server (OpenAM) and execute the following command for each downloaded certificate, updating the command with the values for your keytool command path and keystore location as applicable for your environment, and answer "yes" to the prompt "Trust this certificate?".

```
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -import -alias root_ca -trustcacerts -file <full_filepath_of_the_certificate> -keystore C:\keystore
```

**Note** The -alias option must be updated with a value unique to the Java keystore, otherwise the import operation will result in an error similar to the following: "Certificate not imported, alias <root_ca> already exists."

**Step 15** You can view the certificate in the keystore using the following command, updating the command with the values for your keytool command path and keystore location as applicable for your environment:

```
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keystool.exe -list -v -alias root_ca -keystore C:\keystore
```

**Note** The -alias option must match the value used in Step 14, otherwise the keystore entry may not be found.

**Step 16** Repeat this procedure for each IM and Presence node for which SSO is to be enabled.

**Note** In the case of CA-signed certificates used on the IM and Presence Service node, it is not necessary to import the same CA and intermediate certificate into the OpenAM keystore more than once. If you find that an IM and Presence Service node has been signed by the same CA and intermediate certificate, there is no need to import those certificates into the OpenAM keystore again.

# Install Tomcat

OpenAM requires that the Apache Tomcat Web Container be installed on the OpenAM Windows server base system. This procedure provides details on how to install Apache Tomcat on the OpenAM Windows server base system. See the following table for descriptions of the variables referred to in this procedure.

***Table 21: Variable Descriptions***

| Variable | Description |
|---|---|
| <certstore-path> | The file path to the Java keystore used by Java applications and Apache Tomcat. Trusted server public certificates are stored in this keystore. See Steps 5 or 11 of the following procedure to determine the file path for the Java keystore. |
| <certstore-password> | The password used to access the Java keystore located at <certstore-path>. See Step 6 or 12 of the following procedure to determine the value used for the Java keystore password: |

### Procedure

**Step 1** Download the recommended version of Apache Tomcat to your Windows server that forms the OpenAM base system. For a list of recommended software and versions, see topics related to third-party software and system requirements for Single Sign-On .

**Note** Download the 32bit/64bit Windows Service Installer executable file.

**Step 2** Double-click the downloaded file to begin the installation of Apache Tomcat.

**Step 3** From the Apache Tomcat Setup wizard, click **Next**.

**Step 4** In the **License Agreement** dialog box, click **I Agree**.

**Step 5** In the **Choose Components** dialog box, choose **Minimum** as the type of install and click Next.

**Step 6** In the **Configuration** dialog box, accept the default settings and click Next.

**Step 7** In the **Java Virtual Machine** dialog box, ensure the installed JRE path is set to the value of jre-path.

**Note** If you are using the recommended version of Java, the path will display by default. If you are not using the recommended version of Java, ensure that the path entered matches the path that was used when you installed Java.

**Step 8** Click **Next**.

**Step 9** In the **Choose Install Location** dialog box, accept the default settings and click **Install**. Note the Tomcat install location, because it is required later

**Note** The installation location is referred to as **tomcat-dir** later in this procedure.

**Step 10** Click **Finish**.

**Step 11** Configure Apache Tomcat to start automatically.

a) Choose **Start** > **All Programs** > **Apache Tomcat 7.0 Tomcat7** > **Configure Tomcat**.
b) From the **General** tab, set the **Startup type** as **Automatic**.
c) Click **Apply**.
d) Click **OK**.

**Step 12** Configure the Apache Tomcat runtime parameters:

a) Choose **Start** > **All Programs** > **Apache Tomcat 7.0 Tomcat7** > **Configure Tomcat**.
b) From the **Java** tab, add the following Java options:

```
-Djavax.net.ssl.trustStore=<certstore-path>
-Djavax.net.ssl.trustStorePassword=<certstore-password>
-XX:MaxPermSize=256m
```

**Tip** See the parameter table at the beginning of this procedure for variable descriptions.

**Example:**

```
-Djavax.net.ssl.trustStore=C:\keystore
-Djavax.net.ssl.trustStorePassword=cisco!123
-XX:MaxPermSize=256m
```

c) Set the **Initial memory pool** to 512.
d) Set the **Maximum memory pool** to 1024.
e) Click **Apply**.
f) Click **OK**.

**Step 13** Using a Text Editor, open the server.xml file under `<tomcat-dir>\conf` folder. See Step 9 to determine the value for <tomcat-dir>.

**Example:**

An example value is `"C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf"`

**Step 14** Comment out the 8080 connector port. Enter the code as follows:

**Example:**

```
<!-- <Connector port=”8080” protocol=”HTTP/1.1”
connectionTimeout=”20000”
redirectPort=”8443” /> -->
```

**Step 15** Uncomment the 8443 connector port. Remove the <!- - code at the beginning and - -> at the end of the 8443 connector. You must add three more attributes to the connector configuration:

- keystoreFile (location of the keystore file that was created when you installed Java. In this example, it was created under `C:\keystore`)
- keystorePass
- keystoreType

Enter the code as follows:

**Example:**

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="<certstore-path>"
keystorePass="<certstore-password>"
keystoreType"JKS"/>
```

**Tip** See the parameter table at the beginning of this procedure for variable descriptions.

**Step 16** Save the server.xml file.

**Step 17** Start the Tomcat service.

a) **Start** > **All Programs** > **Apache Tomcat 7.0 Tomcat7** > **Configure Tomcat**
b) From the **General** tab, click **Start**. If the Tomcat service was already running, click **Stop**, then **Start**.

**Step 18** To test the configuration, launch a web browser on the Windows Server that contains the Tomcat instance and go to `https://localhost:8443/tomcat.gif`. The web browser may present warning dialogs about insecure connections because the web browser does not trust the security certificates that are presented by the Tomcat instance. Either examine the certificates and add them to your local certificate store so that the browser trusts them or proceed to the web application (less secure option) using the available browser controls. If the configuration is correct, the Tomcat logo appears in the web browser window.

**Step 19** Configure Windows firewall to allow incoming connections to Apache Tomcat.

a) Choose **Start** > **Administrative Tools** > **Windows Firewall and Advanced Security**.
b) Choose **Windows Firewall and Advanced Security** > **Inbound Rules**.
c) Right-click **Inbound Rules**.
d) Click **New Rule**.
e) From the **What type of rule would you like to create** list of options, choose **Port**.
f) Click **Next**.
g) From the **Does this rule apply to TCP or UDP?** list of options, choose **TCP**.
h) From the **Does this rule apply to all local ports or specific local ports?** list of options, choose **Specific local ports**.
i) Enter 8443 and click **Next**.
j) From the **What action should be taken when a connection matches the specified conditions?** list of options, choose **Allow the connection**.
k) Click **Next**.
l) From the **When does the rule apply?** list of options, choose **Domain** only.
m) Click **Next**.
n) Enter a name and description of your choosing and click **Finish**.

**Step 20** To test the configuration, log in to another host on the network, launch a web browser on the Windows server that contains the Tomcat instance and go to `https://<openam-fqdn>:8443/tomcat.gif`, where `<openam-fqdn>` is the Fully Qualified Domain Name of the Windows Server that contains the Tomcat instance. The web browser may present warning dialogs about insecure connections because the web browser does not trust the security certificates that are presented by the Tomcat instance. Either examine the certificates and add them to your local certificate store so that the browser trusts them or proceed to the web application anyway (this is less secure) using the available browser controls. If the configuration is correct, the Tomcat logo appears loaded into the web browser window.

# Deploy OpenAM War On Apache Tomcat

**Procedure**

**Step 1** Download the recommended OpenAM release from the ForgeRock website.

**Tip** See topics related to third-party software and system requirements for Single Sign-On for details.

**Step 2** Extract the .zip file and locate the opensso.war file that is contained within it.

**Step 3** Copy the WAR file to the Windows server that is to be your OpenAM server. This Windows server should be running the previously configured Tomcat service.

**Step 4** Stop the Apache Tomcat service if it is running:

a) Choose **Start** > **All Programs** > **Apache Tomcat 7.0 Tomcat7** > **Configure Tomcat**.

b) From the **General** tab, click **Stop**.

**Step 5** Deploy the WAR file on the Windows server that contains the Tomcat instance by copying the WAR file to the following location: `<tomcat-dir>\webapps`.

**Example:**

```
C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps
```

**Note** For a description of the `<tomcat-dir>` variable, see topics related to installing the Tomcat.

**Step 6** Start the Apache Tomcat service:

a) Choose **Start** > **All Programs** > **Apache Tomcat 7.0 Tomcat7** > **Configure Tomcat Tomcat7**

b) From the **General** tab, click **Start**.

**Note** The WAR file will fully deploy within a couple minutes. Under the webapps folder, a new folder is created with the same name as the WAR file but with the .war extension removed.

**Step 7** Verify your configuration by launching a web browser and entering `https://<openam-fqdn>:8443/<war-file-name>`, where `<openam-fqdn>` is the FQDN of the Windows server that contains the OpenAM/Tomcat instance and `<war-file-name>` is the name of the OpenAM WAR file with the .war extension removed. If the configuration is correct, the OpenAM administration interface should load in the web browser window.

**Related Topics**

Third-Party Software and System Requirements for Single Sign-On, on page 145

# Set Up OpenAM Using GUI Configurator

The following procedure specifies a method of configuring OpenAM. If you have an existing OpenAM server or a solid understanding of OpenAM, you can configure the server differently.

OpenAM server and J2EE Policy Agents require FQDNs for the hostname of the machines on which you will perform your installations. To avoid problems with installation, configuration, and usage, Cisco highly recommends that you avoid using hostnames like “localhost” or numeric IP addresses like “192.168.1.2”.

OpenAM provides a web-based administration interface that must be accessed using a web browser, for example Mozilla Firefox. When accessing OpenAM for the first time, you must use the FQDN of the OpenAM server in the URL, for example, `https://server1.cisco.com:8443/opensso`, where the sample URL value assumes that the OpenAM WAR file is deployed as `opensso`.

OpenAM configuration and logging information is typically stored in two directories that can be found in the home directory of the user running the OpenAM/Tomcat instance, for example:

- `C:\opensso` (where the folder name matches the deployed URI for the OpenAM WAR file. For example, opensso.)
- `C:\.openssocfg`

If a problem occurs during the configuration, the Configurator displays an error message. If possible, correct the error and retry the configuration. The following log file directories may provide useful information.

- Tomcat Web Container logs: `tomcat-dir\logs`
- OpenAM Install log: `C:\opensso` (where the folder name matches the deployed URI for the OpenAM WAR file. For example, opensso.)

By default, OpenAM is deployed under `C:\opensso` on Windows platforms.

### Procedure

**Step 1** Open the web browser and navigate to the OpenAM server using the following URL: `https://<fqdn of openam server>:8443/<WAR filename>`.

**Example:**

`https://server1.cisco.com:8443/opensso`

**Note** When you access OpenAM for the first time, you are directed to the Configurator to perform the initial configuration of the OpenAM. The Configuration Options window appears when you access the OpenAM for the first time.

**Step 2** Choose **Create Default Configuration**.

**Note** If you encounter an error, repeat steps 1 and 2 on your local machine.

**Step 3** In the **OpenSSO Configurator** window, specify and confirm passwords for the OpenAM administrator (amAdmin) and the default policy agent user (UrlAccessAgent). The default policy agent user is not used later in this example configuration; amAdmin is used each time you log in to OpenAM to change the configuration.

**Note** amAdmin is only a suggested value for the OpenAM Administrator.

**Step 4** Click **Create Configuration**.

You are notified when the configuration is complete.

**Step 5** Choose **Proceed to Login**.

**Step 6** Log in to your deployed OpenAM web application using the previously configured username and password for “amAdmin”.

**Step 7** From the **Access Control** tab, click **/(Top Level Realm)**.

**Step 8** From the **Authentication** tab, click **Core**.

**Step 9** Click **All Core Settings**.

**Step 10** Set the **User Profile** to **Ignored**.

**Step 11** Click **Save** to update the profile.

**Step 12** Log out of the OpenAM GUI.

# Set Up Policies On OpenAM Server

Set up policies on the OpenAM server using the policy rules detailed in the following table.

***Table 22: Policy Rules***

| Service Type | Name | Resource Name | Action |
|---|---|---|---|
| URL Policy Agent (with resource name) | <hostname>-01 | `https://<IMP FQDN>/*` | Enable GET, Value = Allow Enable POST , Value = Allow |
| | <hostname>-02 | `https://<IMP FQDN>/*?*` | |
| | <hostname>-03 | `https://<IMP FQDN>/*?*?*` | |
| | <hostname>-04 | `https://<IMP FQDN>:8443/*` | |
| | <hostname>-05 | `https://<IMP FQDN>:8443/*?*` | |
| | <hostname>-06 | `https://<IMP FQDN>:8443/*?*?*` | |

When you apply the policy rules as defined in this procedure, the IM and Presence Administration/User interfaces can only be accessed with the web browser using the following URL formats:

- `https://<IMP FQDN>` - For example, `https://IMP-Node-01.cisco.com`
- `https://<IMP FQDN>:8443` - For example `https://IMP-Node-01.cisco.com:8443/`

It is *not* possible to access the Cisco Unified CM IM and Presence Administration/User interface using a URL that only specifies a hostname such as `https://<IMP HOSTNAME>` (for example, `https://IMP-Node-01/`).

### Procedure

**Step 1** Log in to the OpenAM Administration interface.

**Step 2** From the **Access Control** tab, choose **/ (Top Level Realm)**.

**Step 3** From the **Policies** tab, click **New Policy**.

**Step 4** In the **Name** field, enter the PolicyName (for example, IMPPolicy) and click **OK**.

IMPPolicy is only a suggested value. You can use any valid name value. This value is not required later in this configuration

**Step 5** Choose the new policy, IMPPolicy, for editing.

**Step 6** Click **Rules**.

**Step 7** Add the rules in the following order:

a) Under the **Rules** section, click **New.**
b) Choose **Service Type** as **URL Policy Agent (with resource name)**
c) Click **Next**.
d) In the **Name** field, enter the suggested rule Name from the Policy Rules table above, replacing <hostname> with the actual hostname of the IM and Presence node.
e) In the ResourceName field provided, enter the corresponding Resource Name for this rule, replacing <IMP FQDN> with the actual Fully Qualified Domain Name of the IM and Presence node.
f) Check the **GET** action with a value of **Allow.**
g) Check the **POST** action with a value of **Allow.**
h) Click **Finish** to complete the rule update.
i) Click **`Save`** to save the policy update.
j) Repeat this entire step for each rule in the above table, then click **Finish**.

You must add this set of six rules for each IM and Presence Service node that is enabled for SSO.

**Step 8** You must add a single Subject to the policy. Add the Subject as follows:

a) Under the **Subjects** section, click **New.**
b) Choose **Authenticated Users** as Subject Type.
c) Click **Next**.
d) Enter **`IMPSubject`** as the **Name** value.

IMPSubject is only a suggested value. You can use any valid value. This value is not required later in this configuration.

e) Click **Finish** to complete the Subject update.
f) Click **Save** to save the policy update.

Only a single Subject is required for this policy even if multiple IM and Presence Service nodes are enabled for Single Sign-On.

**Step 9** You must add a single Condition to the policy. Add the Condition as follows:

a) Under the **Conditions** section, click **New.**
b) Choose **Active Session Time** as Condition Type.
c) Click **Next**.
d) Enter **`IMPTimeOutCondition`** as the **Name** value.

IMPTimeOutCondition is only a suggested value. You can use any valid name value. This value required later in this configuration.

e) Enter **`120`** as the **Maximum Session Time (minutes)**.
f) Ensure the **Terminate Session** field is set to **No.**
g) Click **Finish** to complete the Subject update.
h) Click **Save** to save the policy update.

Note that only a single Condition is required for this policy, even if multiple IM and Presence Service nodes are enabled for SSO.

# Set Up SSO Module Instance

This single module instance can be shared by multiple IM and Presence Service nodes that are configured for SSO as long as the same Active Directory domain is used throughout the deployment. Deployment scenarios involving more than one Active Directory domain are not covered in this documentation.

### Procedure

**Step 1** Log in to the OpenAM administration interface.

**Step 2** From the **Access Control** tab, click **Top Level Realm**.

**Step 3** From the **Authentication** tab, click **Module Instances**.

**Step 4** In the **Module Instances** window, click **New.**

**Step 5** Enter a name for the new login module instance (for example, IMPKRB) and choose **Windows Desktop SSO** from the **Type** list.

**Step 6** Click **OK**.

This module instance name will be used later when enabling SSO on the IM and Presence node.

**Step 7** Click **Save**.

**Step 8** In the **Module Instances** window, choose the name of the new login module (for example, IMPKRB) and provide the following information:

| Parameter | Description |
|---|---|
| Service Principal | This value should exactly match the value specified that was specified when you provisioned the Active Directory for Single Sign-On. For example, -princ value.<br>For example, `HTTP/server1.cisco.com@CISCO.COM` (using openAM server name and domain). |
| Keytab File Name | This value should be the location of the keytab file that was created when you provisioned the Active Directory for Single Sign-On.<br>For example, `C:\keytab\server1.HTTP.keytab` (on Windows platform). |
| Kerberos Realm | Domain for OpenAM server. For example, `CISCO.COM`. |
| Kerberos Server Name (Active Directory) | Provide the FQDN of the AD server. The AD server is normally the Kerberos Domain Controller. If multiple Kerberos Domain Controllers exist for failover purposes, all Kerberos Domain Controllers can be set using a colon (:) as the separator. For example, `ad.cisco.com` . |
| Authentication Level | For example, 22 |

**Step 9** Click **Save**.

The module instance is created and called IMPKRB.

**Step 10** Validate that the SSO Module is working correctly by logging in to a Windows Desktop session as a valid Windows user (a valid end user that exists in the AD; do not use the Administrator account). Access the following URL:

**Note** The browser must be configured for SSO.

`https://<openam-FQDN>:8443/<war-file-name>/UI/Login?module=<SSO_Module>`

Where:

| Parameter | Description |
|---|---|
| *<openam-FQDN>* | The FQDN of the OpenAM server. |
| *<war-file-name>* | The name of the deployed OpenAM WAR file, for example opensso. |
| *<SSO_Module>* | The name of the WindowsDesktopSSO module. |

A screen notifies you that login was successful.

# Set Up J2EE Agent Profile On OpenAM Server

The J2EE Agent is an internal component that is instantiated on each IM and Presence Service node with SSO enabled. You must configure an associated J2EE Agent Profile on the OpenAM server for each J2EE Agent. As such, a J2EE Agent Profile is required for every IM and Presence Service node with SSO enabled. If multiple nodes are to be configured for SSO, a J2EE Agent Profile must be created for each additional node.

The following table lists the J2EE profile agent parameters required for the IM and Presence Service node.

***Table 23: J2EE Profile Agent Setup Parameter Descriptions***

| Parameter | Description |
|---|---|
| Name | Name of the J2EE Policy Agent. For example, <*hostname-j2ee-agent*> where *hostname* is the hostname of the IM and Presence Service node, for example, impNode01-j2ee-agent. |
| Password | Password of the J2EE Policy Agent.<br>**Note** The password will be used when you enable SSO on IM and Presence Service. |
| Configuration | Controls where the J2EE Policy Agent configuration is stored.<br>Choose **Centralized** |
| Server URL | The complete URL of the OpenAM server.<br>For example, `https://<OpenAM FQDN>:8443/opensso` where `opensso` is the name of the OpenAM WAR file with the .war extension removed |

| Parameter | Description |
|---|---|
| Agent URL | The URL of the J2EE Policy Agent to which OpenAM publishes notifications.<br>For example, `https://<IMP FQDN>:8443/agentapp`<br>**Note** The value "`agentapp`" is the key item from the sample URL above. If you use the `agentapp` value, enter `agentapp` when you were prompted to **Enter the relative path where the policy agent should be deployed**. |

The following table lists the login form URIs for each web GUI application on IM and Presence Service.

*Table 24: Login Form URIs for Web GUI Applications On IM and Presence Service*

| Application | Sample value |
|---|---|
| Cisco Unified CM IM and Presence Administration | `/cupadmin/WEB-INF/pages/logon.jsp` |
| Cisco Unified IM and Presence Serviceability | `/ccmservice/WEB-INF/pages/logon.jsp` |
| Cisco Unified IM and Presence Reporting | `/cucreports/WEB-INF/pages/logon.jsp` |
| Cisco Unified IM and Presence OS Administration | `/cmplatform/WEB-INF/pages/logon.jsp` |
| IM and Presence Disaster Recovery System | `/drf/WEB-INF/pages/logon.jsp` |
| Real-Time Monitoring Tool (RTMT) | `/ast/WEB-INF/pages/logon.jsp` |
| Cisco Client Profile Agent | `/ssoservlet/WEB-INF/pages/logon.html` |

### Procedure

**Step 1** Log in to OpenAM administration interface.

**Step 2** From the **Access Control** tab, click **/(Top Level Realm)**.

**Step 3** From the **Agents** tab, choose the **J2EE** tab.

**Step 4** In the **Agents** section, click **New**.

**Step 5** Enter the J2EE setup parameters.

**Step 6** Click **Create**.

A J2EE Agent with the name of <hostname-j2ee-agent> is created.

**Step 7** Choose the J2EE agent that you created.

**Step 8** From the **Application** tab, under the **Login Processing** section, add the Login Form URIs for each web GUI application on IM and Presence Service.

**Step 9** Click **Save**.

**Step 10** From the **OpenAM Services** tab, add OpenSSO Login URL as `https://<OpenAM FQDN>:8443/<war-file-name>/UI/Login?module=<SSO_Module>`.

**Tip** The *<SSO_Module>* value you enter should match the value you entered when you set up the SSO module instance. For example, `https://server1.cisco.com:8443/opensso/UI/Login?module=IMPKRB`.

**Step 11** In the text area, remove all URLs other than the Login URL. Only the Login URL specified in the previous step should be listed in the text area.

**Step 12** Click **Save**.

**Step 13** Click **Back to Main Page**.

**Step 14** Repeat Steps 4 through 13 to create a J2EE Profile Agent for every other IM and Presence Service node to be enabled for SSO.

# Set OpenAM Session Timeout

The OpenAM session timeout must be set to a value that is higher than the session timeout parameter that is set on the IM and Presence Service node. To determine the session timeout value on the IM and Presence Service node, enter the following command using the CLI:

**show webapp session timeout**

### Procedure

**Step 1** Log in to the OpenAM Administration interface.

**Step 2** From the **Configuration** tab, choose **Global**.

**Step 3** Click **Session**.

**Step 4** Click **Dynamic Attributes**.

**Step 5** Enter a value in the **Maximum Idle Time** field.

**Step 6** Click **Save**.

# Import OpenAM Certificate Into IM and Presence Service

IM and Presence Service nodes with SSO communicate with the OpenAM server over an encrypted channel. Establishing an encrypted communication channel requires each IM and Presence Service node with SSO to trust the security certificate presented by the OpenAM server. An IM and Presence Service node trusts a security certificate by importing the required security certificates into the tomcat-trust trust store.

The required procedure is dependent on the security configuration that you used when you created the Java keystore for the OpenAM Server.

- Use a self-signed security certificate for OpenAM/Tomcat instance
- Use a CA signed security certificate for OpenAM/Tomcat instance

**Caution** Importing OpenAM certificates affects service; Cisco highly recommends that you import the OpenAM certificates during a maintenance window.

**Note** For information about importing certificates, see *Cisco Unified System Maintenance Guide for IM and Presence*.

### Procedure

**Step 1** Sign in to the Cisco Unified CM IM and Presence Administration for the IM and Presence database publisher node that is to be enabled with SSO.

**Step 2** Choose **System** > **Security** > **Certificate Import Tool**.

**Step 3** Choose **Tomcat Trust** as the **Certificate Trust Store**.

**Step 4** Enter the Fully Qualified Domain Name of the OpenAM server as the **Peer Server**.

**Step 5** Enter 8443 as the **Peer Server Port**.

**Step 6** Click **Submit**.

The Certificate Import Tool executes two tests:

- **Verify reachability of the specified certificate server (pingable)** - checks that the OpenAM server is reachable by this IM and Presence node. If this test fails, it may be due to the firewall on the OpenAM base Windows system blocking the ping operation. See topics related to importing the OpenAM certificate into IM and Presence Service to allow a ping through a Windows firewall.
- **Verify SSL connectivity to the specified certificate server** - checks if this IM and Presence node can securely connect to the OpenAM server. If this test fails due to "Missing certificates", the required certificates are missing and a secure connection can not be established. If this test fails, proceed to the next step. If this test passes, proceed to Step 15.

  **Note** If this test fails with the message "The Troubleshooter has encountered an internal error", troubleshoot the certificate failure before you continue to the next step.

**Step 7** Click **Configure** to open the Certificate Viewer. The Certificate Viewer provides a visual representation of the certificate chain presented by OpenAM during a TLS connection handshake. This indicates which certificates must be imported into this IM and Presence Service node.

**Step 8** Inspect the certificates in the chain and ensure that you trust the issuers.

**Step 9** Check **Accept Certificate Chain** and click **Save**.

The required certificates from the chain are now imported into the tomcat-trust trust store of this IM and Presence Service node.

**Step 10** Click **Close**.

The Certificate Import Tool reports that the "Certificates verified successfully".

**Step 11** Restart the Cisco Intercluster Sync Agent service on this node using the following CLI command:**utils service restart Cisco Intercluster Sync Agent**.

**Step 12** Restart the Tomcat service on this node using the following CLI command: **utils service restart Cisco Tomcat**

**Step 13** Repeat Steps 11 and 12 for each IM and Presence Service subscriber node in this cluster.

**Step 14** Verify the secure connection by using the Certificate Import Tool on each subscriber node in this cluster.

a) Sign in to Cisco Unified CM IM and Presence Administration of the IM and Presence Service subscriber node that is being configured for SSO.
b) Choose **System** > **Security** > **Certificate Import Tool**.
c) Choose **Tomcat Trust** as the **Certificate Trust Store**
d) Enter the FQDN of the OpenAM server as the **Peer Server**.
e) Enter **8443** as the **Peer Server Port**.

**Step 15** Repeat this procedure for all IM and Presence Service clusters for which you will be enabling SSO.

**Related Topics**

Important Information Before Single Sign-On Setup, on page 146
Certificate Failure, on page 248

# Activate Single Sign-On

When enabling SSO, you must perform the following tasks in the order indicated.

**Caution** Enabling SSO affects service; Cisco highly recommends that you enable SSO during a maintenance window.

## Configure Access Permissions Before Enable SSO

It is important to understand the user access permissions that should be in place before and after SSO is enabled. Understanding the permissions can help avoid situations in which users have incorrect permissions when accessing IM and Presence Service applications.

*Table 25: Prerequisites for Enabling Single-Sign On*

| Application | Notes |
|---|---|

| | |
|---|---|
| Cisco Unified CM IM and Presence Administration<br>• Cisco Unified CM IM and Presence Administration<br>• IM and Presence Serviceability<br>• IM and Presence Reporting | Before enabling SSO, ensure that an end user who is a member of the necessary User Groups exists in order to facilitate administration access.<br>The default administrator application user that was created at the time of installation has the following:<br>Groups:<br>• Standard Audit Users<br>• Standard CCM Super Users<br>Roles:<br>• Standard AXL API Access<br>• Standard Admin Rep Tool Admin<br>• Standard Audit Log Administration<br>• Standard CCM Admin Users<br>• Standard CCMADMIN Administration<br>• Standard CUReporting<br>• Standard EM Authentication Proxy Rights<br>• Standard SERVICEABILITY Administration<br>• Standard SSO Config Admin<br>Any end user that is a member of the above User Groups with those Roles will have full access rights to IM and Presence Service, similar to that of the default administrator.<br>To view the default application user on IM and Presence Service, choose **Cisco Unified CM Administration** > **User Management** > **Application User** > **Find**. Choose the default application user (that was created during install) to view their details.<br>To assign an end user to these groups on IM and Presence Service, choose **Cisco Unified CM Administration** > **User Management** > **User Settings** > **Access Control Group** > **Find**. Choose a group and click **Add End Users**. Search for the desired end user, choose the user, and click **Add End Users to Group**. |

| | |
|---|---|
| Cisco Unified IM and Presence Operating System Administration<br>• IM and Presence Operating System Administration<br>• IM and Presence Disaster Recovery System | Normally, the default administrator application user does not have access to these web applications. These web applications are only accessible by the Cisco Unified IM and Presence Operating System administrator. This administrator has access to the Administration CLI in addition to these web applications.<br>After SSO is enabled for these applications, the applications are accessible by any end user that has the same permissions as the default administrator application user. |
| Real-Time Monitoring Tool | Before enabling SSO, ensure that an end user exists that is a member of the necessary user groups to allow administrative access to the Real-Time Monitoring Tool.<br>Refer to the note for Cisco Unified CM IM and Presence Administration above. |

## Enable Single Sign-On Using GUI

This Cisco Unified IM and Presence Operating System Administration application is split into three components:

- Status
- Server Settings
- Select Applications

**Status**

A warning message displays indicating that the change in SSO settings causes Tomcat to restart.

The following error messages may display when you enable the SSO application:

- Invalid Open Access Manager (OpenAM) server URL - This error message displays when you enter an invalid OpenAM server URL.
- Invalid profile credentials - This error message displays when you enter a wrong profile name or wrong profile password or both.
- Security trust error - This error message displays when this IM and Presence Service node does not trust the certificate chain presented by the OpenAM server.

**Note** If you see any of the above error messages while enabling SSO, then the status changes to that error.

**Server Settings**

You can edit the server settings only when SSO is disabled for all applications.

**Select Applications**

You can enable or disable SSO on any of the following applications:

- Cisco Unified CM IM and Presence Administration – Enables SSO for Cisco Unified CM IM and Presence Administration, Cisco Unified IM and Presence Serviceability, and Cisco Unified IM and Presence Reporting.

- Cisco Unified IM and Presence Operating System Administration – Enables SSO for Cisco Unified IM and Presence Operating System Administration and Disaster Recovery System.
- RTMT – Enables the web application for the Real-Time Monitoring Tool.
- Cisco UP Client Profile Agent – Enables SSO for the Cisco UP Client Profile Agent service. This option is only applicable to customers using Common Access Card (CAC) sign-on.

**Procedure**

**Step 1** Choose **Cisco Unified IM and Presence Operating System Administration** > **Security** > **Single Sign On**.

**Step 2** Enter the URL of the Open Access Manager (OpenAM) server:

**Example:**

```
https://server1.cisco.com:8443/opensso
```

**Step 3** Enter the relative path where the policy agent should be deployed. The relative path must be alphanumeric, such as *agentapp* for example.

**Step 4** Enter the name of the profile that is configured for this policy agent, for example " cupnode01-j2ee-agent".

**Step 5** Enter the password of the profile name.

**Step 6** Enter the login Module instance name that is configured for Windows Desktop SSO, such as IMPKRB. See topics related to setting up the SSO module instance for more information..

**Step 7** Click **Save**.

**Step 8** In the **Confirmation** dialog box, click **OK** to restart Tomcat.

**Related Topics**

Set Up J2EE Agent Profile On OpenAM Server, on page 164
Set Up SSO Module Instance, on page 163

# Deactivate Single Sign-On

If you choose to disable SSO, you must perform the following tasks in the order indicated.

## Configure Access Permissions Before Disable SSO

If SSO is disabled for any IM and Availability web application that supports SSO, all users accessing that application need to provide a username and password. Cisco recommends that if you are an IM and Presence Service administrator intending to disable SSO for any IM and Availability web applications, ensure that users can access the application after SSO is disabled. This action is important to avoid inadvertently locking out the active IM and Presence Service administration account.

***Table 26: Prerequisites for Disabling Single Sign-On***

| Application | Notes |
|---|---|

| | |
|---|---|
| Cisco Unified CM IM and Presence Administration (Cisco Unified CM IM and Presence Administration, IM and Presence Serviceability, IM and Presence Reporting) | Before disabling SSO, ensure that an application user exists with a known username/password and that this user is a member of the necessary User Groups.<br>The default administrator application user that was created at the time of installation has the following:<br>Groups:<br>• Standard Audit Users<br>• Standard CCM Super Users<br>Roles:<br>• Standard AXL API Access<br>• Standard Admin Rep Tool Admin<br>• Standard Audit Log Administration<br>• Standard CCM Admin Users<br>• Standard CCMADMIN Administration<br>• Standard CUReporting<br>• Standard EM Authentication Proxy Rights<br>• Standard SERVICEABILITY Administration<br>• Standard SSO Config Admin<br>Any application user that is a member of the above User Groups with those Roles will have full access rights to IM and Presence Service if SSO is disabled.<br>To view the application users on IM and Presence, select **Cisco Unified CM Administration** > **User Management** > **Application User** > **Find**. Select a user to view their details. |
| Cisco Unified IM and Presence Operating System Administration (IM and Presence Operating System Administration, IM and Presence DRS) | Before disabling SSO, ensure that an OS Administration user exists with a known username/password and that this user has access to the Cisco Unified IM and Presence Operating System Administration CLI. After SSO is disabled, this user has access rights to the Cisco Unified IM and Presence Operating System Administration GUIs. |
| Real-Time Monitoring Tool | Before disabling SSO, ensure that an application user with a known username/password exists and that this user has the same access rights as the user specified for Cisco Unified CM IM and Presence Administration (Cisco Unified CM IM and Presence Administration, IM and Presence Serviceability, and IM and Presence Reporting). |

## Disable Single Sign-On

You can disable SSO using either the GUI, as described in this procedure, or the CLI. For information about how to disable SSO using the CLI, see the **utils sso disable** command in the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

### Procedure

**Step 1** Choose **Cisco Unified OS Administration** > **Security** > **Single Sign On**.

**Step 2** Deselect all applications that were previously enabled for SSO.

**Step 3** Click **Save**.

**Step 4** In the **Confirmation** dialog box, click **OK** to restart Tomcat.

# Uninstall OpenAM on Windows

### Before you begin

Ensure that you have completed the following tasks before you uninstall OpenAM:

- Configure access permissions before disabling SSO.
- Disable Single Sign-On

### Procedure

**Step 1** Access the OpenAM server Windows desktop and choose **Start** > **All Programs** > **Apache Tomcat 7.0 Tomcat7** > **Configure Tomcat**.

**Note** This menu path assumes you are using Tomcat 7.

**Step 2** From the **General** tab, click **Stop** to stop the Tomcat service if it is running on the OpenAM server.

**Step 3** Delete the OpenAM configuration data. This data is typically stored in two directories that can be found in the home directory of the user running the Tomcat instance. For example, `C:\opensso` (where the folder name matches the deployed URI for the OpenAM WAR file such as `opensso`) and `C:\.openssocfg`.

**Step 4** Delete the deployed OpenAM WAR file and the WAR file itself from the following location on the OpenAM/Tomcat instance: `tomcat-dir\webapps`.

**Example:**

```
C:\Program Files\Apache Software Foundation\Tomcat 7\webapps
```

**Tip** See topics related to Tomcat installation for a description of the tomcat-dir variable.

**Step 5** Access the Windows desktop of the OpenAM server and choose **Start** > **All Programs** > **Apache Tomcat 7.0 Tomcat7** > **Configure Tomcat**.

**Step 6** From the **General** tab, click **Start** to start the Tomcat service.

**Related Topics**

Configure Access Permissions Before Disable SSO, on page 171
Disable Single Sign-On, on page 173
Install Tomcat, on page 156

# Set Debug Level

You can gather additional debug information the IM and Presence Service node by setting the log level for the J2EE Policy Agent accordingly. The log level for this component is configured on the OpenAM server itself. The default log level is Error. You can change the log level to Message to provide additional debug information. Cisco recommends that you use the Message log level only for short periods of time, because the associated log files can grow quite large.

**Procedure**

**Step 1** Sign in to OpenAM (`https://<OpenAM FQDN>:8443/opensso`) from your web browser (for example, Mozilla Firefox).

**Step 2** From the **Access Control** menu, choose **Top Level Realm** > **Agents** > **J2EE**.

**Step 3** Under the **General** heading, choose **Agent Debug Level**.

**Step 4** Under the **Agent Debug Level**, specify the desired level (**Message** or **Error**).

**Step 5** Click **Save.**

**Step 6** On the IM and Presence Service node, restart the Cisco Tomcat service.

a) Access the IM and Presence Administration CLI.
b) Execute the following command: **utils service restart Cisco Tomcat**.

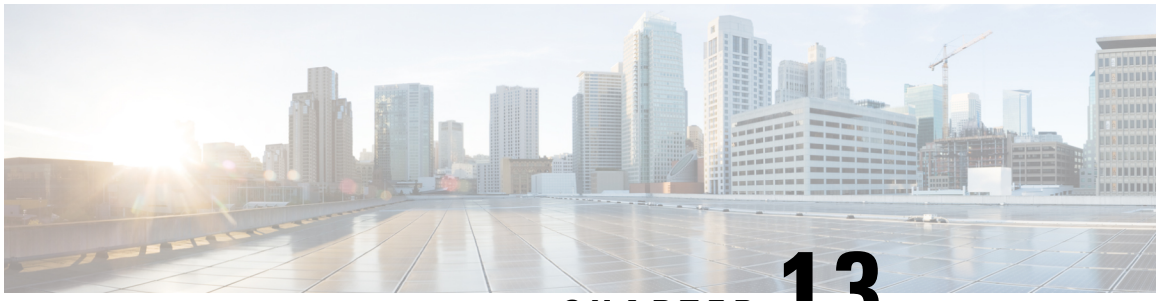
**Step 7** Retrieve the logs using Cisco Unified Real Time Monitoring Tool for IM and Presence Service by browsing and downloading the logs for the Cisco SSO component.

**Note** If users experience problems while SSO is enabled, you must disable SSO and then re-enable it in order to access the debug.out logs from Cisco Unified Real Time Monitoring Tool.

# PART IV

# Administration


- Chat Setup and Management, on page 177
- End User Setup and Handling, on page 197
- User Migration, on page 213
- Multilingual Support Configuration For IM and Presence Service, on page 221



CHAPTER 13

# Chat Setup and Management


- Chat Deployments, on page 177
- Chat Administration Settings, on page 179
- Chat Node Alias Management, on page 185
- Chat Room Management, on page 190
- Group Chat and Persistent Chat Interactions and Restrictions, on page 194


# Chat Deployments

You can set up chat for different deployment scenarios. Sample deployment scenarios are available.

## Chat Deployment Scenario 1

| | |
|---|---|
| Deployment Scenario: | You do not want to include the Cluster ID in the chat node alias. Instead of the system-generated alias `conference-1-mycup.cisco.com`, you want to use the alias `primary-conf-server.cisco.com`. |
| **Configuration Steps:** | **1.** Choose **Messaging** > **Group Chat and Persistent Chat** to turn off the system-generated alias. (This is on by default).<br>**2.** Edit the alias and change it to `primary-conf-server.cisco.com`. |
| Notes: | When you turn off the old system-generated alias, `conference-1-mycup.cisco.com` reverts to a standard, editable alias listed under Group Chat Server Aliases. This maintains the old alias and the chat room addresses associated with that alias. |

## Chat Deployment Scenario 2

| | |
|---|---|
| Deployment Scenario: | You want to:<br>• change the Domain from cisco.com to linksys.com and use conference-1-mycup.linksys.com instead of conference-1-mycup.cisco.com.<br>• maintain the address of existing persistent chat rooms in the database so that users can still find old chat rooms of type xxx@conference-1-mycup.cisco.com. |

| | |
|---|---|
| **Configuration Steps**: | 1. Log in to **Cisco Unified CM IM and Presence Administration**, choose **Presence** > **Settings Topology** > **Advanced Configuration**.<br>2. See the related topics for more information about how to edit the default IM and Presence Service domain. |
| | |
| Notes: | When you change the domain, the fully qualified cluster name (FQDN) automatically changes from conference-1-mycup.cisco.com to conference-1-mycup.linksys.com. The old system-generated alias conference-1-mycup.cisco.com reverts to a standard, editable alias listed under Group Chat Server Aliases. This maintains the old alias and the chat room addresses associated with that alias. |

### Related Topics

IM and Presence Service Default Domain Configuration

# Chat Deployment Scenario 3

| | |
|---|---|
| Deployment Scenario: | You:<br>• want to change the Cluster ID from mycup to ireland to use conference-1-ireland.cisco.com instead of conference-1-mycup.cisco.com.<br>• do not need to maintain the address of existing persistent chat rooms in the database. |
| **Configuration Steps**: | 1. Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Settings** > **Standard Configuration**.<br>2. Edit the Cluster ID and change it to ireland.<br>3. Choose **Messaging** > **Group Chat Server Alias Mapping**.<br>4. Delete the old alias conference-1-mycup.cisco.com. |
| Notes: | When you change the Cluster ID, the fully qualified cluster name (FQDN) automatically changes from conference-1-mycup.cisco.com to conference-1-ireland.cisco.com. The old system-generated alias conference-1-mycup.cisco.com reverts to a standard, editable alias listed under Group Chat Server Aliases. This maintains the old alias and the chat room addresses associated with that alias. Because (in this example) the Administrator has no need to maintain the old alias address, it is appropriate to delete it. |

# Chat Deployment Scenario 4

| | |
|---|---|
| Deployment Scenario: | You want to:<br>• delete a node associated with an existing alias from the System Topology, for example, conference-3-mycup.cisco.com.<br>• add a new node with a new node ID (node id: 7) to the System Topology, for example, conference-7-mycup.cisco.com.<br>• maintain the address of chat rooms that were created using the old alias. |

| | |
|---|---|
| **Configuration Steps**: | Option 1<br>1. Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **Group Chat Server Alias Mapping**.<br>2. Click **Add New** to add the additional alias, conference-3-mycup.cisco.com.<br>Option 2<br>1. Choose **Messaging** > **Group Chat and Persistent Chat** and turn off the default system-generated alias, conference-7-mycup.cisco.com. (This is on by default).<br>2. Edit the alias and change it to conference-3-mycup.cisco.com. |
| Notes: | When you add the new node to the System Topology, the system automatically assigns this alias to the node: conference-7-mycup.cisco.com.<br>Option 1<br>• If you add an additional alias, the node is addressable via both aliases, conference-7-mycup.cisco.com and conference-3-mycup.cisco.com.<br>Option 2<br>• If you turn off the old system-generated alias, conference-7-mycup.cisco.com reverts to a standard, editable alias listed under Group Chat Server Aliases. |

# Chat Administration Settings

## Change IM Gateway Settings

You can configure IM Gateway settings for IM and Presence Service.

The SIP-to-XMPP connection on the IM and Presence Service IM Gateway is enabled by default. This allows IM interoperability between SIP and XMPP clients so that users of SIP IM clients can exchange bi-directional IMs with users of XMPP IM clients. We recommend that you leave the IM Gateway Status parameter on; however, you can turn off the IM Gateway Status parameter to prevent XMPP and SIP clients from communicating with each other.

You can also change the default inactive timeout interval of IM conversations, as well as select the error message that gets displayed if the IM fails to get delivered.

**Restriction**

SIP clients cannot participate in chat rooms because this is an XMPP-specific feature.

**Procedure**

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters**.

**Step 2** Choose an IM and Presence Service node from the **Server** menu.

**Step 3** Choose **Cisco SIP Proxy** as the service on the **Service Parameter Configuration** window.

**Step 4** Do one of the following actions:

a) Set IM Gateway Status to **On** in the SIP XMPP IM Gateway (Clusterwide) section to enable this feature.

b) Set IM Gateway Status to **Off** in the SIP XMPP IM Gateway (Clusterwide) section to disable this feature.

**Step 5** Set the Inactive Timeout interval (in seconds) of IM conversations maintained by the gateway. The default setting is 600 seconds, which is appropriate to most environments.

**Step 6** Specify the error message that you want users to see if the IM fails to deliver. Default error message: Your IM could not be delivered.

**Step 7** Click **Save**.

### What to do next

Proceed to configure the persistent chat room settings.

# Enable File Transfer

Administrators can enable or disable IM and Presence Service node support for file transfer capability (XEP-0096). Enabling file transfer support allows XMPP clients to extend file transfer capabilities to end users.

**Note** File transfer between a local user and an intercluster peer contact is only possible if both clusters have the feature enabled.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters**.

**Step 2** From the **Server** menu, choose an IM and Presence Service node .

**Step 3** In the **Service Parameter Configuration** window, choose Cisco XCP Router as the service.

**Step 4** From the **Enable file transfer** drop-down list, click **On** or **Off**.

**Step 5** Click **Save**.

**Step 6** Restart the Cisco XCP Router Service on every node in the cluster.

### Related Topics

Restart Cisco XCP Router Service, on page 58

# Limit Number Of Sign-In Sessions

Administrators can limit the number of sign-in sessions per user on the Cisco XCP Router. This parameter is applicable to XMPP clients only.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration > System > Service Parameters**.

**Step 2** Choose an IM and Presence Service node from the **Server** menu.

**Step 3** Choose **Cisco XCP Router** as the service in the **Service Parameter Configuration** window.

**Step 4** Enter a parameter value in the **Maximum number of logon sessions per user** in the **XCP Manager Configuration Parameters (Clusterwide)** area.

**Step 5** Click **Save**.

**Step 6** Restart the Cisco XCP Router Service.

### Related Topics

Restart Cisco XCP Router Service, on page 58

# Configure Persistent Chat Room Settings

You need only configure persistent chat settings if you use persistent chat rooms as opposed to temporary (ad-hoc) chat rooms. This configuration is specific to persistent chat and has no impact on IM archiving for regulatory compliance.

### Restriction

SIP clients cannot participate in chat rooms because this is an XMPP-specific feature.

### Before you begin

- To use persistent chat rooms, you must configure a unique external database instance per node.
- If you use an external database for persistent chat logging, consider the size of your database. Archiving all the messages in a chat room is optional, and will increase traffic on the node and consume space on the external database disk. In large deployments, disk space could be quickly consumed. Ensure that your database is large enough to handle the volume of information.
- Before you configure the number of connections to the external database, consider the number of IMs you are writing offline and the overall volume of traffic that results. The number of connections that you configure will allow the system to scale. While the default settings on the UI suit most installations, you may want to adapt the parameters for your specific deployment.
- The heartbeat interval is typically used to keep connections open through firewalls. Do not set the Database Connection Heartbeat Interval value to zero without contacting Cisco support.

### Procedure

**Step 1** Select **Cisco Unified Communications Manager IM and Presence Administration** > **Messaging** > **Group Chat and Persistent Chat**.

**Step 2** Check **Enable Persistent Chat**.

**Note** This is a cluster-wide setting. If persistent chat is enabled on any node in the cluster, clients in any cluster will be able to discover the Text Conference instance on the node and chat rooms hosted on that node.

Users on a remote cluster can discover Text Conference instances and rooms on the local cluster even if Persistent Chat is not enabled on the remote cluster.

**Step 3** (Optional) Specify how to store chat room messages, if required:

a) Check **Archive all room messages** if you want to archive all the messages that are sent in the room. This is a cluster-wide setting that applies to all persistent chat rooms.

b) Enter the number of connections to the database that you to want to use for processing requests. This is a cluster-wide setting that applies to all connections between chat nodes and associated databases.

c) Enter the number of seconds after which the database connection should refresh. This is a cluster-wide setting that applies to all connections between chat nodes and associated databases.

**Step 4** Select from the list of preconfigured external databases and assign the appropriate database to the chat node.

**Tip** Click the hyperlink if you need to edit the chat node details in the **Cluster Topology Details** window.

**Step 5** If you are deploying Cisco Jabber, leave the **Rooms are anonymous by default** and **Room owners can change whether or not rooms are anonymous** check boxes unchecked. Chat fails with Cisco Jabber if either option is selected.

**Step 6** If you update any of the Persistent Chat settings, choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** to restart the Cisco XCP Text Conference Manager service.

- If you turn on the **Archive all messages in a room** setting, Cisco recommends that you monitor the performance of each external database used for persistent chat. You should anticipate an increased load on the database server(s).
- If you enable persistent chat rooms, but do not establish the correct connection with the external database, the TC service will shut down. Under these circumstances, you will lose the functionality of all chat rooms - both temporary and persistent. If a chat node establishes a connection (even if other chat nodes fail), it will still start.

### What to do next

Proceed to turn on Cisco XCP Text Conference Manager.

### Related Topics

Change IM Gateway Settings, on page 179
Chat Node Alias Management, on page 185

# Enable Persistent Chat

Configure persistent chat settings only if you use persistent chat rooms as opposed to temporary (ad hoc) chat rooms. This configuration is specific to persistent chat and has no impact on IM archiving for regulatory compliance.

### Before you begin

- To use persistent chat rooms, you must configure a unique external database instance for each node.

**Important** You must have an external database assigned for each node.

- If you are using an Oracle external database, you need to update the patch for the known Oracle defect: ORA-22275. If this is not done persistent chat rooms will not work properly.
- If you use an external database for persistent chat logging, consider the size of your database. Archiving all the messages in a chat room is optional, and will increase traffic on the node and consume space on the external database disk. In large deployments, disk space could be quickly consumed. Ensure that your database is large enough to handle the volume of information.
- Archiving all room joins and leaves is optional, because it increases traffic and consumes space on the external database server.
- Before you configure the number of connections to the external database, consider the number of IMs you are writing and the overall volume of traffic that results. The number of connections that you configure will allow the system to scale. While the default settings on the UI suit most installations, you may want to adapt the parameters for your specific deployment.
- The heartbeat interval is typically used to keep connections open through firewalls. Do not set the Database Connection Heartbeat Interval value to zero without contacting Cisco support.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **Group Chat and Persistent Chat**.

**Step 2** Check the check box to **Enable Persistent Chat**.

**Step 3** (Optional) Check the check box **Archive all room joins and exits**, if you want to log all instances of users joining and leaving a room. This is a cluster-wide setting that applies to all persistent chat rooms.

**Step 4** (Optional) Check the check box **Archive all room messages**, if you want to archive all the messages that are sent in the room. This is a cluster-wide setting that applies to all persistent chat rooms.

**Step 5** (Optional) Check the check box **Allow only group chat system administrators to create persistent chat rooms**, if you want to ensure that persistent chat rooms are created only by group chat system administrators. This is a cluster-wide setting that applies to all persistent chat rooms.

To configure group chat system administrators, choose **Messaging** > **Group chat system administrators**.

**Step 6** Enter the maximum number of persistent chat rooms that are allowed in the **Maximum number of persistent chat rooms allowed** field. The default value is set to 1500.

**Important** You must ensure that there is sufficient space on the external database. Having a large number of chat rooms impacts resources on the external database.

**Step 7** Enter the number of connections to the database that you to want to use for processing requests in the **Number of connections to the database** field. The default is set to 5. This is a cluster-wide setting that applies to all connections between chat nodes and associated databases.

**Step 8** Enter the number of seconds after which the database connection should refresh in the **Database connection heartbeat interval (seconds)** field. The default is set to 300. This is a cluster-wide setting that applies to all connections between chat nodes and associated databases.

**Step 9** Enter the number of minutes after which the chat room should time out in the **Timeout value for persistent chat rooms (minutes)** field. The default is set to 0. The timeout is used to check whether a chat room is idle and empty. If the room is found to be idle and empty, the room is closed. With the default value set to 0, the idle check is disabled.

**Step 10** Choose from the list of preconfigured external databases and assign the appropriate database to the chat node.

- If you turn on the **Archive all room joins and exits** setting, Cisco recommends that you monitor the performance of each external database that is used for persistent chat. Expect an increased load on the database servers.
- If you turn on the **Archive all room messages** setting, Cisco recommends that you monitor the performance of each external database that is used for persistent chat. Expect an increased load on the database servers.
- If you enable persistent chat rooms but do not establish the correct connection with the external database, the chat node will fail. Under these circumstances, you will lose the functionality of all chat rooms, both temporary and persistent. If a chat node establishes a connection (even if other chat nodes fail), it will still start.
- To edit the Cisco Unified Communications Manager IM and Presence Service node details in the **Cluster Topology Details** window, click the hyperlink.

**Step 11** Click **Save**.

**Step 12** Restart the Cisco XCP Router on all nodes in the cluster by choosing **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Network Services**.

Note the following:

- If the Cisco XCP Text Conference Manager service was already running, it will automatically restart when you restart the Cisco XCP Router.
- If the Cisco XCP Text Conference Manager service was not already running, you must start it after the Cisco XCP Router has restarted. To start the Cisco XCP Text Conference Manager service, choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services**.

**Note** After you have enabled persistent chat, if you subsequently want to update any of the persistent chat settings, only the following non-dynamic settings require a Cisco XCP Text Conference Manager restart:

- Number of connections to the database
- Database connection heartbeart interval (seconds)

### Related Topics

Restart Cisco XCP Text Conference Manager Service

# Configure Group Chat System Administration

**Procedure**

**Step 1** Choose **Messaging** > **Group Chat System Administrators**.

**Step 2** Check **Enable Group Chat System Administrators**.

You must restart the Cisco XCP Router when the setting is enabled or disabled. Once the System Administrator setting is enabled, you can add system administrators dynamically.

**Step 3** Click **Add New**.

**Step 4** Enter an IM address.

**Example:**

The IM address must be in the format of name@domain .

**Step 5** Enter a nickname.

**Step 6** Enter a description.

**Step 7** Click **Save**.

# Group Chat and Persistent Chat Default Settings Configuration and Reversion

You can change the default enhanced ad hoc and persistent chat settings. To revert all settings back to their default values, click **Set to Default**.

**Note** To allow chat room owners to change a setting, check the **Room owners can change** check box on the node. The room owner can then configure such settings as they wish and those settings are applicable to the room they are creating. The availability of configuring these settings from the client also depends on the client implementation and whether the client is providing an interface in which to configure these settings.

# Chat Node Alias Management

## Chat Node Aliases

Aliases create a unique address for each chat node so that users (in any domain) can search for specific chat rooms on specific nodes, and join chat in those rooms. Each chat node in a system must have a unique alias.

**Note** This chat node alias, `conference-3-mycup.cisco.com`, for example, will form part of the unique ID for each chat room created on that node, `roomjid@conference-3-mycup`.cisco.com

You can assign your aliases cluster-wide, in these ways:

- System-generated - allows the system to automatically assign a unique alias to each chat node.You do not have do to anything further to address your chat node if you enable the system-generated aliases. The system will auto-generate one alias per chat node by default using the following naming convention: `conference-x-clusterid.domain`, where:
  - conference - is a hardcoded keyword
  - x- is the unique integer value that denotes the node ID
  - Example: `conference-3-mycup.cisco.com`
- Manually - You may choose to override the default system-generated alias if the `conference-x-clusterid.domain` naming convention does not suit your customer deployment, for example, if you do not want to include the Cluster ID in your chat node alias. With manually-managed aliases, you have complete flexibility to name chat nodes using aliases that suit your specific requirements.
- Additional Aliases - You can associate more than one alias with each chat node on a per-node basis. Multiple aliases per node allows users to create additional chat rooms using these aliases. This applies whether you assign a system-generated alias or manage your aliases manually.

# Key Considerations

Changing chat node aliases can make the chat rooms in the database unaddressable and prevent your users from finding existing chat rooms.

Note these results before you change the constituent parts of aliases or other node dependencies:

- Cluster ID - This value is part of the fully qualified cluster name (FQDN). Changing the Cluster ID (choose **System** > **Presence Topology: Settings**) causes the FQDN to incorporate the new value and the system-managed alias to automatically change across the cluster. For manually-managed aliases, it is the responsibility of the Administrator to manually update the alias list if the Cluster ID changes.
- Domain - This value is part of the FQDN. Changing the Domain (choose **Presence** > **Presence Settings**) causes the FQDN to incorporate the new value and the system-managed alias to automatically change across the cluster. For manually-managed aliases, it is the responsibility of the Administrator to manually update the alias list if the Domain changes.
- Connection between the chat node and external database - The chat node will not start if persistent chat is enabled and you do not maintain the correct connection with the external database.
- Deletion of a chat node — If you delete a node associated with an existing alias from the Presence Topology, chat rooms created using the old alias may not be addressable unless you take further action.
- To ensure that the user has access to all the old chat rooms, take a backup of all the existing aliases before deleting a node and assign the same alias to a new node.

We recommend that you do not change existing aliases without considering the wider implications of your changes, namely:

- Make sure that you maintain the address of old chat nodes in the database so that users can locate existing chat rooms via the old alias, if required

- If there is federation with external domains, you may need to publish the aliases in DNS to inform the users in those domains that the aliases have changed and new addresses are available. This depends on whether or not you want to advertise all aliases externally.

### Related Topics

Chat Deployment Scenario 1, on page 177

# Turn On or Off System-Generated Chat Node Aliases

Chat node aliases allow users in any domain to search for specific chat rooms on specific nodes, and join in those chat rooms. IM and Presence Service automatically assign a unique, system-generated alias to each chat node by default. No further configuration is needed to address your chat node when system-generated aliases are used. The system automatically generates one alias per chat node using the default naming convention `conference-x-clusterid.domain`.

If you want to manually assign chat node aliases, you must turn off the default system-generated alias setting. If you turn off a system-generated alias, the existing alias (`conference-x-clusterid.domain`) reverts to a standard, editable alias listed under Conference Server Aliases. See topics related to manually managed chat node aliases for more information. For best practice guidelines, see the sample chat deployment scenarios

### Before you begin

- Review the topics about chat node aliases and key considerations.
- You cannot edit or delete a system-generated alias, for example, `conference-3-mycup.cisco.com`.

### Procedure

**Step 1** Log in to **Cisco Unified CM IM and Presence Administration**, choose **Messaging** > **Group Chat and Persistent Chat**.

**Step 2** Enable or disable system-generated aliases:

a) To enable the system to automatically assign chat room aliases to nodes using the naming convention `conference-x-clusterid.domain`, check **System Automatically Manages Primary Group Chat Server Aliases**

**Tip** Choose **Messaging** > **Group Chat Server Alias Mapping** to verify that the system-generated alias is listed under Primary Group Chat Server Aliases.

b) To disable system-generated aliases, uncheck **System Automatically Manages Primary Group Chat Server Aliases**.

### What to do next

- Even if you configure a system-generated alias for a chat node, you can associate more than one alias with the node if required.
- If you are federating with external domains, you may want to inform federated parties that the aliases have changed and new aliases are available. To advertise all aliases externally, configure DNS and publish the aliases as DNS records.

- If you update any of the system-generated alias configuration, perform one of these actions:
- Restart the Cisco XCP Text Conference Manager. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** to restart this service

### Related Topics

Chat Deployment Scenario 1, on page 177
Configure Persistent Chat Room Settings, on page 181

# Manage Chat Node Aliases Manually

You can manually add, edit, or delete chat node aliases. To manually manage chat node aliases, you must turn off the default setting, which uses system-generated aliases. If you turn off a system-generated alias, the existing alias (**conference-x-clusterid.domain**) reverts to a standard, editable alias listed under Conference Server Aliases. This maintains the old alias and the chat room addresses associated with that alias.

You can manually assign multiple aliases to chat nodes. Even if a system-generated alias already exists for a chat node, you can associate additional aliases to the node manually.

For manually-managed aliases, it is the responsibility of the administrator to manually update the alias list if the Cluster ID or domain changes. System-generated aliases will incorporate the changed values automatically.

**Note** Although it is not mandatory, we recommend that you always include the domain when you assign a new chat node alias to a node. Use this convention for additional aliases, newalias.domain. Choose **Presence Settings** > **Advanced Settings** in **Cisco Unified CM IM and Presence Administration** to see the domain.

### Before you begin

Review topics related to chat node aliases and key considerations.

### Procedure

**Step 1** Log in to **Cisco Unified CM IM and Presence Administration**, choose **Messaging** > **Group Chat and Persistent Chat**.

**Step 2** Uncheck **System Automatically Manages Primary Group Chat Server Aliases**.

**Step 3** All the existing chat node aliases are listed together under Group Chat Server Aliases. To view the alias list, perform these actions:

a) Choose **Messaging** > **Group Chat Server Alias Mapping**.
b) Click **Find**.

**Step 4** Complete one or more of the following actions as required:

Edit an existing alias (old system-generated or user-defined alias)

a) Click the hyperlink for any existing alias that you want to edit.
b) Edit the alias for the node in the Group Chat Server Alias field. Make sure the alias is unique for the node.
c) Choose the appropriate node to which you want to assign this changed alias.

Add a new chat node alias

a) Click **Add New**.
b) Enter a unique alias for the node in the Group Chat Server Alias field.
c) Choose the appropriate node to which you want to assign the new alias.

Delete an existing alias

a) Check the check box for the alias that you want to delete.
b) Click **Delete Selected**.

**Troubleshooting Tips**

- Every chat node alias must be unique. The system will prevent you from creating duplicate chat node aliases across the cluster.
- A chat node alias name cannot match the IM and Presence domain name.
- Delete old aliases only if you no longer need to maintain the address of chat rooms via the old alias.
- If you are federating with external domains, you may want to inform federated parties that the aliases have changed and new aliases are available. To advertise all aliases externally, configure DNS and publish the aliases as DNS records.
- If you update any of the chat node alias configuration, restart the Cisco XCP Text Conference Manager.

**What to do next**

- Proceed to turn on the Cisco XCP Text Conference Manager.

**Related Topics**

Chat Deployments, on page 177

# Turn on Cisco XCP Text Conference Manager

This procedure applies if you configure the persistent chat room settings, or manually add one or more aliases to a chat node. You must also turn on this service if you want to enable ad hoc chat on a node.

**Before you begin**

If persistent chat is enabled, an external database must be associated with the Text Conference Manager service, and the database must be active and reachable or the Text Conference Manager will not start. If the connection with the external database fails after the Text Conference Manager service has started, the Text Conference Manager service will remain active and functional, however, messages will no longer be written to the database and new persistent rooms cannot be created until the connection recovers.

**Procedure**

**Step 1** Log in to **Cisco Unified IM and Presence Serviceability**, choose **Tools** > **Control Center - Feature Services**.

**Step 2** Choose the node from the Server drop-down list and click **Go**.

**Step 3** Click the radio button next to the Cisco XCP Text Conference Manager service in the IM and Presence Service section to turn it on or click **Restart** to restart the service.

**Step 4** Click **OK** when a message indicates that restarting may take a while.

**Step 5** (Optional) Click **Refresh** if you want to verify that the service has fully restarted.

**Related Topics**

Configure Persistent Chat Room Settings, on page 181

# Chat Room Management

## Set Number of Chat Rooms

Use room settings to limit the number of rooms that users can create. Limiting the number of chat rooms will help the performance of the system and allow it to scale. Limiting the number of rooms can also help mitigate any possible service-level attacks.

**Procedure**

**Step 1** To change the maximum number of chat rooms that are allowed, enter a value in the field for **Maximum number of rooms allowed**.

**Step 2** Click **Save**.

## Configure Member Settings

Member settings allow system-level control over the membership in chat rooms. Such a control is useful for users to mitigate service-level attacks that can be prevented by administrative actions such as banning. Configure the member settings as required.

**Procedure**

**Step 1** Check **Rooms are for members only by default** if you want rooms to be created as members-only rooms by default. Members-only rooms are accessible only by users on a white list configured by the room owner or administrator. The checkbox is unchecked by default.

**Note** The white list contains the list of members who are allowed in the room. It is created by the owner or administrator of the members-only room.

**Step 2** Check **Room owners can change whether or not rooms are for members only** if you want to configure the room so that room owners are allowed to change whether or not rooms are for members only. The check box is checked by default.

**Note** A room owner is the user who creates the room or a user who has been designated by the room creator or owner as someone with owner status (if allowed). A room owner is allowed to change the room configuration and destroy the room, in addition to all other administrator abilities.

**Step 3** Check **Only moderators can invite people to members-only rooms** if you want to configure the room so that only moderators are allowed to invite users to the room. If this check box is unchecked, members can invite other users to join the room. The check box is checked by default.

**Step 4** Check **Room owners can change whether or not only moderators can invite people to members-only rooms** if you want to configure the room so that room owners can allow members to invite other users to the room. The check box is checked by default.

**Step 5** Check **Users can add themselves to rooms as members** if you want to configure the room so that any user can request to join the room at any time. If this check box is checked, the room has an open membership. The check box is unchecked by default.

**Step 6** Check **Room owners can change whether users can add themselves to rooms as members** if you want to configure the room so that room owners have the ability to change the setting that is listed in Step 5 at any time. The check box is unchecked by default.

**Step 7** Click **Save**.

# Configure Availability Settings

Availability settings determine the visibility of a user within a room.

**Procedure**

**Step 1** Check **Members and administrators who are not in a room are still visible in the room** if you want to keep users on the room roster even if they are currently offline. The check box is checked by default.

**Step 2** Check **Room owners can change whether members and administrators who are not in a room are still visible in the room** if you want to allow room owners the ability to change the visibility of a member or administrator. The check box is checked by default.

**Step 3** Check **Rooms are backwards-compatible with older clients** if you want the service to function well with older Group Chat 1.0 clients. The check box is unchecked by default.

**Step 4** Check **Room owners can change whether rooms are backwards-compatible with older clients** if you want to allow room owners the ability to control backward compatibility of the chat rooms. The check box is unchecked by default.

**Step 5** Check **Rooms are anonymous by default** if you want the room to display the user nickname but keep the Jabber ID private. The check box is unchecked by default.

**Step 6** Check **Room owners can change whether or not rooms are anonymous** if you want to allow room owners to control the anonymity level of the user Jabber ID. The check box is unchecked by default.

**Step 7** Click **Save**.

# Configure Invite Settings

Invite settings determine who can invite users to a room based on the user's role. Roles exist in a moderator-to-visitor hierarchy so, for instance, a participant can do anything a visitor can do, and a moderator can do anything a participant can do.

**Procedure**

**Step 1** From the drop-down list for **Lowest participation level a user can have to invite others to the room**, choose one:

- **Visitor** allows visitors, participants, and moderators the ability to invite other users to the room.
- **Participant** allows participants and moderators the ability to invite other users to the room. This is the default setting.
- **Moderator** allows only moderators the ability to invite other users to the room.

**Step 2** Check **Room owners can change the lowest participation level a user can have to invite others to the room** to allow room owners to change the settings for the lowest participation level that is allowed to send invitations. The check box is unchecked by default.

**Step 3** Click **Save**.

# Configure Occupancy Settings

**Procedure**

**Step 1** To change the system maximum number of users that are allowed in a room, enter a value in the field for **How many users can be in a room at one time**. The default value is set to 1000.

**Note** The total number of users in a room should not exceed the value that you set. The total number of users in a room includes both normal users and hidden users.

**Step 2** To change the number of hidden users that are allowed in a room, enter a value in the field for **How many hidden users can be in a room at one time**. Hidden users are not visible to others, cannot send a message to the room, and do not send presence updates. Hidden users can see all messages in the room and receive presence updates from others. The default value is 1000.

**Step 3** To change the default maximum number of users that are allowed in a room, enter a value in the field for **Default maximum occupancy for a room**. The default value is set to 50 and cannot be any higher than the value that is set in Step 1.

**Step 4** Check **Room owners can change default maximum occupancy for a room** if you want to allow room owners to change the default maximum room occupancy. The check box is checked by default.

**Step 5** Click **Save**.

# Configure Chat Message Settings

Use Chat Message settings to give privileges to users based on their role. For the most part, roles exist in a visitor-to-moderator hierarchy. For example, a participant can do anything a visitor can do, and a moderator can do anything a participant can do.

### Procedure

**Step 1** From the drop-down list for **Lowest participation level a user can have to send a private message from within the room**, choose one:

- **Visitor** allows visitors, participants, and moderators to send a private message to other users in the room. This is the default setting.
- **Participant** allows participants and moderators to send a private message to other users in the room.
- **Moderator** allows only moderators to send a private message to other users in the room.

**Step 2** Check **Room owners can change the lowest participation level a user can have to send a private message from within the room** if you want to allow room owners to change the minimum participation level for private messages. The check box is checked by default.

**Step 3** From the drop-down list for **Lowest participation level a user can have to change a room's subject**, choose one:

a) **Participant** allows participants and moderators to change the room's subject. This is the default setting.
b) **Moderator** allows only moderators to change the room's subject.

Visitors are not permitted to change the room subject.

**Step 4** Check **Room owners can change the lowest participation level a user can have to change a room's subject** if you want to allow room owners to change the minimum participation level for updating a room's subject. The check box is checked by default.

**Step 5** Check **Remove all XHTML formatting from messages** if you want to remove all Extensible Hypertext Markup Language (XHTML) from messages. The check box is unchecked by default.

**Step 6** Check **Room owners can change XHTML formatting setting** if you want to allow room owners to change the XHTML formatting setting. The check box is unchecked by default.

**Step 7** Click **Save**.

# Configure Moderated Room Settings

Moderated rooms provide the ability for moderators to grant and revoke the voice privilege within a room (in the context of Group Chat, voice refers to the ability to send chat messages to the room). Visitors cannot send instant messages in moderated rooms.

### Procedure

**Step 1** Check **Rooms are moderated by default** if you want to enforce the role of moderator in a room. The check box is unchecked by default.

**Step 2** Check **Room owners can change whether rooms are moderated by default** if you want to allow room owners the ability to change whether rooms are moderated. The check box is checked by default.

**Step 3** Click **Save**.

# Configure History Settings

Use History settings to set the default and maximum values of messages that are retrieved and displayed in the rooms, and to control the number of messages that can be retrieved through a history query. When a user joins a room, the user is sent the message history of the room. History settings determine the number of previous messages that the user receives.

### Procedure

**Step 1** To change the maximum number of messages that users can retrieve from the archive, enter a value in the field for **Maximum number of messages that can be retrieved from the archive**. The default value is set to 100. It serves as a limit for the next setting.

**Step 2** To change the number of previous messages displayed when a user joins a chat room, enter a value in the field for **Number of messages in chat history displayed by default**. The default value is set to 15 and cannot be any higher than the value that is set in Step 1.

**Step 3** Check **Room owners can change the number of messages displayed in chat history** if you want to allow room owners to change the number of previous messages displayed when a user joins a chat room. The check box is unchecked by default.

**Step 4** Click **Save**.

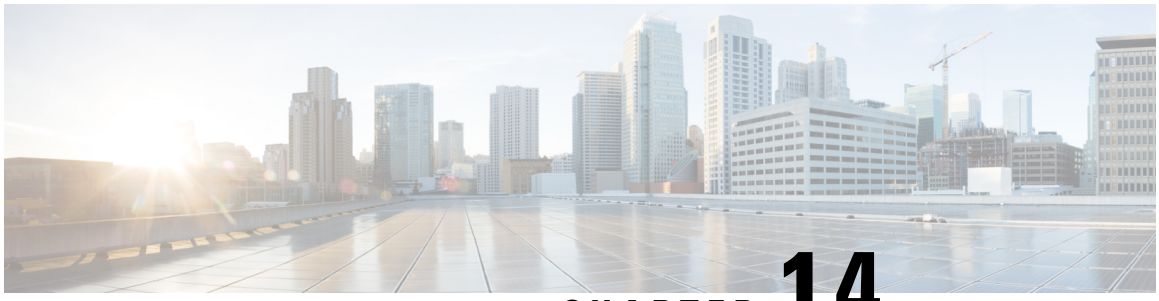
# Group Chat and Persistent Chat Interactions and Restrictions

*Table 27: Group Chat and Persistent Chat Interactions and Restrictions*

| Feature Interaction | Restriction |
|---|---|
| Archiving room joins | Archiving room joins and leaves is optional because it will increase traffic and consume space on the external database server. |
| Chat with anonymous rooms | If you are deploying chat via Cisco Jabber (either group chat or persistent chat), make sure that the **Rooms are anonymous by default** and **Room owners can change whether or not rooms are anonymous** options are not selected in the **Group Chat and Persistent Chat Settings** window. If either check box is checked, chat will fail |
| Database Connection Issues | If the connection with the external database fails after the Text Conference Manager service has started, the Text Conference Manager service will remain active and functional, however, messages will no longer be written to the database and new persistent rooms cannot be created until the connection recovers. |

| Feature Interaction | Restriction |
|---|---|
| OVA Requirements | If you are deploying Persistent Chat or Intercluster Peering, the minimum OVA size that you can deploy for these features is the 5000 user OVA. It's recommended that you deploy at least the 15,000 user OVA. Centralized Deployments may require the 25,000 user OVA, depending on the size of the user base. For additional details on OVA options and user capacities, refer to the following site:<br>**Note** It's strongly recommended to deploy at least the 15,000 user OVA on all IMP nodes.<br>https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html |
| External Database connectivity and Cisco XCP Text Conferencing service | In a split-brain scenario, When the subscriber or publisher detects its peer Text Conferencing service or any node is down, then the subscriber or publisher attempts a transition from normal to backup.<br>During this operation if loading of the peer's chat rooms fails to connect to external database, then the Cisco XCP Text Conferencing service will shutdown. |
| Number of Persistent chat rooms supported if High Availability is configured | The maximum number of Persistent Chat Rooms supported on an IM&P deployment is 5000 per subcluster.<br>If High Availability is enabled, it is recommended to create a maximum of 2500 rooms per node. (though the system allows to create upto maximum of 5000 rooms per node). If more than 2500 rooms are configured per node in a High Availability deployment, then during failover, there would be more than 5000 rooms hosted on the backup node. This might result in unexpected performance issues depending on the traffic load.<br>The load of 5000 rooms on the system also depends on the number of participants in the room, the rate of message exchange in the rooms and the size of messages. Use Cisco Collaboration Sizing tool to ensure you have the right OVA setup for your Persistent Chat Deployment. For Information on Collaboration Sizing tool, Please refer: https://cucst.cloudapps.cisco.com/landing<br>It is recommended to have your rooms balanced equally among both the nodes in a subcluster. And if you have more than one subcluster in a IM&P Cluster, it is recommended to also load balance the rooms across all the subclusters. Currently IM&P doesn't have a mechanism to automatically load balance the rooms. The responsibility of load balancing the room lies with the users creating the rooms. During room creation, users have to ensure that they use the jabber feature to automatically select a random node for a room creation. |

| Feature Interaction | Restriction |
| --- | --- |
| Making ad hoc chat rooms private | Ad hoc chat rooms are public by default, but can be configured to be for members only with the following configuration:<br>**1.** From Cisco Unified CM IM and Presence Administration, choose **Messaging** > **Group Chat and Persistent Chat**.<br>**2.** Check the **Rooms are for members only by default** check box.<br>**3.** Uncheck the **Room owners can change whether or not rooms are for members onl**y check box.<br>**4.** Uncheck the **Only moderators can invite people to members-only rooms** check box.<br>**5.** Click **Save**.<br>**6.** Restart the Cisco XCP Text Conference service. |



CHAPTER 14

# End User Setup and Handling


- End User Setup and Handling on IM and Presence Service, on page 197
- Authorization Policy Setup On IM and Presence Service, on page 197
- Bulk Rename User Contact IDs, on page 200
- Bulk Export User Contact Lists, on page 201
- Bulk Import Of User Contact Lists, on page 202
- Duplicate User ID and Directory URI Management, on page 207


# End User Setup and Handling on IM and Presence Service

You can setup the authorization policy for IM and Presence Service end users, perform bulk user contact list imports and exports, as well as manage duplicate and invalid end user instances.

For information about assigning users to IM and Presence Service nodes and to set up end users for IM and Presence Service, see the following guides:

- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager Bulk Administration Guide*
- *Installing Cisco Unified Communications Manager*

# Authorization Policy Setup On IM and Presence Service

## Automatic Authorization On IM and Presence Service

IM and Presence Service authorizes all presence subscription requests that it receives from SIP-based clients in the local enterprise. A local user running a SIP-based client automatically receives the availability status for contacts in the local enterprise, without being prompted to authorize these subscriptions on the client. IM and Presence Service only prompts the user to authorize the subscription of a contact in the local enterprise if the contact is on the blocked list for the user. This is the default authorization behavior for SIP-based clients on IM and Presence Service, and you cannot configure this behavior.

In the XMPP network, it is standard behavior for the node to send all presence subscriptions to the client, and the client prompts the user to authorize or reject the subscription. To allow enterprises to deploy IM and

Presence Service with a mix of SIP-based and XMPP-based clients (to align the authorization policy for both client types), Cisco provides the following automatic authorization setting on IM and Presence Service:

- When you turn on automatic authorization, IM and Presence Service automatically authorizes all presence subscription requests it receives from both XMPP-based clients and SIP-based in the local enterprise. This is the default setting on IM and Presence Service.
- When you turn off automatic authorization, IM and Presence Service only supports XMPP-based clients. For XMPP-based clients, IM and Presence Service sends all presence subscriptions to the client, and the client prompts the user to authorize or reject the presence subscription. SIP-based clients will not operate correctly on IM and Presence when you turn off automatic authorization.

**Caution** If you turn off automatic authorization, SIP-based clients are not supported. Only XMPP-based clients are supported when you turn off automatic authorization.

# User Policy and Automatic Authorization

In addition to reading the automatic authorization policy, IM and Presence Service reads the policy settings for the user to determine how to handle presence subscription requests. Users configure the policy settings from the Cisco Jabber client. A user policy contains the following configuration options:

- Blocked list - a list of local and external (federated) users that will always see the availability status of the user as unavailable regardless of the true status of the user. The user can also block a whole federated domain.
- Allowed list - a list of local and external users that the user has approved to see their availability. The user can also allow a whole external (federated) domain.
- Default policy - the default policy settings for the user. The user can set the policy to block all users, or allow all users.

Note that if you turn off automatic authorization, IM and Presence Service automatically authorizes subscription requests a user that is on the contact list of another user. This applies to users in the same domain, and users in different domains (federated users). For example:

- UserA wishes to subscribe the view the availability status of UserB. Automatic authorization is off on IM and Presence Service, and UserB is not in the Allowed or Blocked list for the UserA.
- IM and Presence Service sends the presence subscription request to the client application of UserB, and the client application prompts userB to accept or reject the subscription.
- UserB accepts the presence subscription request, and UserB is added to the contact list of UserA.
- UserA is then automatically added to the contact list for UserB without being prompted to authorize the presence subscription.

IM and Presence Service will automatically add UserA to the contact list of UserB even if the policy for UserB (i) blocks the external domain, or (ii) the default policy for the user is block all, or (iii) “ask me” is chosen.

If you deploy interdomain federation between a local IM and Presence Service enterprise and a supported external enterprise, IM and Presence Service does not apply the automatic authorization setting to presence subscription requests received from external contacts, unless the user has applied a policy on that external

contact or domain. On receipt of a presence subscription request from an external contact, IM and Presence Service will only send the subscription request to the client application if the user chooses “ask me” to be prompted to set their own Allow/Block policy for external contacts, and if the external contact or domain is not in either the Allowed or Blocked list for the user. The client application prompts the user to authorize or reject the subscription.

**Note** IM and Presence Service uses common user policies for both availability and instant messages.

**Related Topics**

http://www.cisco.com/en/US/products/ps6837/products_user_guide_list.html
IM and Presence Service Configuration Guides

# Configure Authorization Policy on IM and Presence Service

You can turn on automatic authorization so that IM and Presence Service automatically authorizes all presence subscription requests it receives from both XMPP-based clients and SIP-based in the local enterprise. If you turn off automatic authorization, IM and Presence Service only supports XMPP-based clients and sends all presence subscriptions to the client where the user is prompted to authorize or reject the presence subscription.

**Tip** See the Online Help topic in the Cisco Unified CM IM and Presence Administration interface for a definition of all the parameters on this window.

**Procedure**

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Settings.**

**Step 2** Configure the authorization policy. Perform one of the following actions:

- To turn on automatic authorization, check **Allow users to view the availability of other users without being prompted for approval**.
- To turn off automatic authorization, uncheck **Allow users to view the availability of other users without being prompted for approval.**.

**Step 3** Click **Save**.

**Step 4** Restart the Cisco XCP Router service.

**What to do next**

Proceed to configure the SIP publish trunk on IM and Presence Service.

**Related Topics**

Restart Cisco XCP Router Service, on page 58
IM Setup On IM and Presence Service, on page 138

# Bulk Rename User Contact IDs

The IM and Presence Service Bulk Assignment Tool allows you to rename the contact ID (JID) in user contact lists from one format to another. For example, you can rename a user's contact ID from firstname.lastname@domain.com to userid@domain.com and the Bulk Administration Tool will update each user's contact list with the new contact ID.

**Caution** Bulk rename of contact IDs is used in the migration of users from a Microsoft server (for example Lync) to IM and Presence Service Service. See the *Partitioned Intradomain Federation Guide* on Cisco.com for detailed instructions of how this tool should be used as part of the user migration process. Using this tool in any other circumstances is not supported.

Before you can run this job, you must upload a file containing a list of contact IDs and the corresponding new format of each of those contact IDs. The file must be a CSV file with the following format:

**<Contact ID>, <New Contact ID>**

where **<Contact ID>** is the existing contact ID and **<New Contact ID>** is the new format of the contact ID.

From Release 10.0 the **<Contact ID>** is the user's IM address as it appears on the **Presence Topology User Assignment window**.

The following is a sample CSV file with one entry:

```
Contact ID, New Contact ID
john.smith@example.com, jsmith@example.com
```

Complete the following procedure to upload the CSV file and rename the contact IDs for a list of users.

### Procedure

**Step 1** Upload the CSV file with the list of contact IDs that you want to rename in all contact lists. Do the following:

a) On the IM and Presence database publisher node, choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Upload/Download Files**.
b) Click **Add New**.
c) Click **Browse** to locate and choose the CSV file.
d) Choose **Contacts** as the Target.
e) Choose **Rename Contacts – Custom File** as the Transaction Type.
f) Click **Save** to upload the file.

**Step 2** On the publisher node, choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Contact List** > **Rename Contacts**.

**Step 3** In the **File Name** field, choose the file that you uploaded.

**Step 4** Choose one of the following actions:

- Click **Run Immediately** to execute the Bulk Administration job immediately.
- Click **Run Later** to schedule a time to execute the Bulk Administration job. For more information about scheduling jobs in the Bulk Administration Tool, see the Online Help in Cisco Unified CM IM and Presence Administration.

**Step 5** Click **Submit**. If you chose to run the job immediately, the job runs after you click Submit.

# Bulk Export User Contact Lists

The IM and Presence Service Bulk Administration Tool (BAT) allows you to export the contact lists of users who belong to a particular node or presence redundancy group to a CSV data file. You can then use BAT to import the user contact lists to another node or presence redundancy group in a different cluster. The BAT user contact list export and import features facilitate the moving of users between clusters. See topics related to bulk imports of user contact lists for more information.

**Note** Users on contact lists who do not have an IM address, will not be exported.

BAT allows you to find and choose the users whose contact lists you want to export. The user contact lists are exported to a CSV file with the following format:

```
<User ID>,<User Domain>,<Contact ID>,<Contact Domain>,<Nickname>,<Group Name>
```

The following table describes the parameters in the export file.

| Parameter | Description |
|---|---|
| User ID | The user ID of the IM and Presence Service user.<br>**Note** This value is the user portion of the user's IM address. |
| User Domain | The Presence domain of the IM and Presence Service user.<br>**Note** This value is the domain portion of the user's IM address.<br>**Example 1:** bjones@example.com—bjones is the user ID and example.com is the user domain.<br>**Example 2:** bjones@usa@example.com—bjones@usa is the user ID and example.com is the user domain. |
| Contact ID | The user ID of the contact list entry. |
| Contact Domain | The Presence domain of the contact list entry. |
| Nickname | The nickname of the contact list entry.<br>If the user has not specified a nickname for a contact, the Nickname parameter will be blank. |
| Group Name | The name of the group to which the contact list entry is to be added.<br>If a user's contacts are not sorted into groups, the default group name will be specified in the Group Name field. |

The following is a sample CSV file entry:

```
userA,example.com,userB,example.com,buddyB,General
```

Complete the following procedure to export user contact lists with BAT and download the export file.

**Procedure**

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Contact List** > **Export**.

**Step 2** Use the selection criteria to find the users whose contact lists you want to export. See the Online Help topic in the Cisco Unified CM IM and Presence Administration interface for more information about finding and selecting users.

**Step 3** Click **Next**.

**Step 4** In the **File Name** field, enter a name for the CSV file.

**Step 5** Choose one of the following:

- Click **Run Immediately** to execute the Bulk Administration job immediately.
- Click **Run Later** to schedule a time to execute the Bulk Administration job. For more information about scheduling jobs in BAT, see the Online Help in Cisco Unified CM IM and Presence Administration.

**Step 6** Click **Submit**. If you chose to run the job immediately, the job runs after you click Submit.

**Step 7** To download the export file after the job has run, choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Upload/Download Files**.

**Step 8** Find and choose the export file that you want to download.

**Step 9** Click **Download Selected**.

# Bulk Import Of User Contact Lists

You can use the IM and Presence Service Bulk Assignment Tool (BAT) to import user contact lists into IM and Presence Service. With this tool, you can prepopulate contact lists for new IM and Presence Service client users or add to existing contact lists. To import user contact lists, you must provide BAT with an input file that contains the user contact lists.

The input file must be a CSV file in the following format:

```
<User ID>,<User Domain>,<Contact ID>,<Contact Domain>,<Nickname>,<Group Name>
```

The following is a sample CSV file entry:

```
userA,example.com,userB,example.com,buddyB,General
```

The following table describes the parameters in the input file.

*Table 28: Description of Input File Parameters*

| Parameter | Description |
|---|---|
| User ID | This is a mandatory parameter.<br>The user ID of the IM and Presence Service user. It can have a maximum 132 characters.<br>**Note** This value is the user portion of the user's IM address. |
| User Domain | This is a mandatory parameter.<br>The Presence domain of the IM and Presence Service user. It can have a maximum of 128 characters.<br>**Note** This value is the domain portion of the user's IM address.<br>**Example 1:** `bjones@example.com`—bjones is the user ID and example.com is the user domain.<br>**Example 2:** `bjones@usa@example.com`—bjones@usa is the user ID and example.com is the user domain. |
| Contact ID | This is a mandatory parameter.<br>The user ID of the contact list entry. It can have a maximum of 132 characters. |
| Contact Domain | This is a mandatory parameter.<br>The Presence domain of the contact list entry. The following restrictions apply to the format of the domain name:<br>• Length must be less than or equal to 128 characters<br>• Contains only numbers, upper- and lowercase letters, and hyphens (-)<br>• Must not start or end with hyphen (-)<br>• Length of label must be less than or equal to 63 characters<br>• Top-level domain must be characters only and have at least two characters |
| Nickname | The nickname of the contact list entry. It can have a maximum of 255 characters. |

| Parameter | Description |
|---|---|
| Group Name | This is a mandatory parameter.<br>The name of the group to which the contact list entry is to be added. It can have a maximum of 255 characters. |

**Note** If you are moving users to another node or presence redundancy group in a different cluster, you can use BAT to generate the CSV file for chosen users. See topics related to bulk exports of user contact lists for more information.

Complete the following steps to import user contact lists into IM and Presence Service:

- Check the maximum contact list size.
- Upload the input file using BAT.
- Create a new bulk administration job.
- Check the results of the bulk administration job.

### Before You Begin

Before you import the user contact lists, you must complete the following:

1. Provision the users on Cisco Unified Communications Manager.
2. Ensure that the users are licensed on Cisco Unified Communications Manager for the IM and Presence Service.

**Note** The default contact list import rate is based on the virtual machine deployment hardware type. You can change the contact list import rate by choosing **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters** > **Cisco Bulk Provisioning Service**. However, if you increase the default import rate, this will result in higher CPU and memory usage on IM and Presence Service.

# Check Maximum Contact List Size

Before you import contact lists to IM and Presence Service, check the Maximum Contact List Size and Maximum Watchers settings. The system default value is 200 for Maximum Contact List Size and 200 for Maximum Watchers.

Cisco recommends that you set the Maximum Contact List Size and Maximum Watchers settings to Unlimited while importing user contact lists to IM and Presence Service. This ensures that each migrated user contact list is fully imported. After all users have migrated, you can reset the Maximum Contact List Size and Maximum Watchers settings to the preferred values.

**Note** It is possible to exceed the maximum contact list size without losing data when importing contact lists using BAT; however, Cisco recommends temporarily increasing the Maximum Contact List Size setting or setting the value to Unlimited for the import. You can reset the maximum value after the import is complete.

You only need to check the maximum contact list size on those clusters that contain users for whom you wish to import contacts. When you change Presence settings, the changes are applied to all nodes in the cluster; therefore you only need to change these settings on the IM and Presence database publisher node within the cluster.

### What To Do Next

Upload the input file using BAT.

### Related Topics

Configure Maximum Contact List Size Per User, on page 136
Configure Maximum Number of Watchers Per User, on page 137

# Upload Input File Using BAT

The following procedure describes how to upload the CSV file using BAT.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Upload/Download Files**.

**Step 2** Click **Add New**.

**Step 3** Click **Browse** to locate and choose the CSV file.

**Step 4** Choose **Contact Lists** as the Target.

**Step 5** Choose **Import Users' Contacts – Custom File** as the Transaction Type.

**Step 6** Click **Save** to upload the file.

### What to do next

Create a new bulk administration job.

# Create New Bulk Administration Job

The following procedure describes how to create a new bulk administration job in Cisco Unified CM IM and Presence Administration.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Contact List** > **Update**.

**Step 2** From the File Name drop-down list, choose the file to import.

**Step 3** In the Job Description field, enter a description for this Bulk Administration job.

**Step 4** Choose one of the following:

- Click **Run Immediately** to execute the Bulk Administration job immediately.
- Click **Run Later** to schedule a time to execute the Bulk Administration job. For more information about scheduling jobs in BAT, see the Online Help in Cisco Unified CM IM and Presence Administration.

**Step 5** Click **Submit**. If you chose to run the job immediately, the job runs after you click Submit.

### What to do next

Check the results of the bulk administration job.

# Check Results of Bulk Administration Job

When the Bulk Administration job is complete, the IM and Presence Service BAT tool writes the results of the contact list import job to a log file. The log file contains the following information:

- The number of contacts that were successfully imported.
- The number of internal server errors that were encountered while trying to import the contacts.
- The number of contacts that were not imported (ignored). The log file lists a reason for each ignored contact at the end of the log file. The following are the reasons for not importing a contact:
  - Invalid format - invalid row format, for example, a required field is missing or empty
  - Invalid contact domain - the contact domain is in an invalid format. See topics related to bulk import of user contact lists for the valid format of the contact domain
  - Cannot add self as a contact - you cannot import a contact for a user if the contact is the user
  - User’s contact list is over limit - the user has reached the maximum contact list size and no more contacts can be imported for that user
  - User is not assigned to local node - the user is not assigned to the local node
- The number of contacts in the CSV file that were unprocessed due to an error that caused the BAT job to finish early. This error rarely occurs.

Complete the following procedure to access this log file.

Procedure

**Procedure**

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Job Scheduler**.

**Step 2** Click **Find** and choose the job ID of the contact list import job.

**Step 3** Click the **Log File Name** link to open the log.

# Duplicate User ID and Directory URI Management

The Cisco IM and Presence Data Monitor service checks for duplicate user IDs and empty or duplicate directory URIs across all IM and Presence Service intercluster nodes. If any errors are detected, IM and Presence Service raises an alarm in the software. Cisco recommends that you take immediate action to remedy these errors to avoid communications disruptions for these users.

You can monitor the status of duplicate user IDs and directory URI checks from the System Troubleshooter using Cisco Unified CM IM and Presence Administration GUI. You can also set the time interval for user ID and directory URI checks using the GUI.

To gather specific information about which users caused these alarms, use the Command Line Interface. Use the Real-Time Monitoring Tool to monitor system alarms and alerts.

For more information about using the command line interface to validate user IDs or directory URIs, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*. For information about using the Real-Time Monitoring Tool, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

## User ID and Directory URI Monitoring

The Cisco IM and Presence Data Monitor service checks the Active directory entries for duplicate user IDs and empty or duplicate directory URIs for all IM and Presence Service intercluster nodes. Duplicate user IDs or directory URIs are not possible within a cluster; however, it is possible to unintentionally assign the same user ID or directory URI value to users on different clusters in an intercluster deployment.

You can use the System Troubleshooter in Cisco Unified CM IM and Presence Administration GUI to monitor the status of duplicate user IDs and directory URI checks. The time interval for these user ID and directory URI checks are set using Cisco Unified CM IM and Presence Administration GUI. The valid range is from 5 minutes to 1440 minutes (12 hours). The default is 30 minutes.

If errors are detected, IM and Presence Service raises an alarm in the software.

**DuplicateDirectoryURI**
: This alert indicates that there are multiple users within the intercluster deployment that are assigned the same directory URI value when the Directory URI IM Address scheme is configured.

**DuplicateDirectoryURIWarning**
: This warning indicates that there are multiple users within the intercluster deployment that are assigned the same directory URI value when the *userID@Default_Domain* IM Address scheme is configured.

**DuplicateUserid**
: This alert indicates there are duplicate user IDs assigned to one or more users on different clusters within the intercluster deployment.

**InvalidDirectoryURI**
This alert indicates that one or more users within the intercluster deployment are assigned an empty or invalid directory URI value when the Directory URI IM Address scheme is configured.

**InvalidDirectoryURIWarning**
This warning indicates that one or more users within the intercluster deployment are assigned an empty or invalid directory URI value when the *userID@Default_Domain* IM Address scheme is configured.

To gather specific information about which users have these alarm conditions, use the Command Line Interface for a complete listing. System alarms do not provide details about the affected users and the System Troubleshooter displays details for only up to 10 users. Use the Command Line Interface and validate users to gather information about which users caused an alarm. For more information, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

**Caution** Take the appropriate action to fix duplicate user IDs and duplicate or invalid Directory URIs to avoid communications disruptions for the affected users. To modify user contact information, see the *Cisco Unified Communications Manager Administration Guide*.

# User ID and Directory URI Error Conditions

The following table describes user ID and directory URI error conditions that can occur when a system check for duplicate user IDs and duplicate or invalid directory URIs is performed on an intercluster deployment. The alarms that are raised are listed, as well as suggested actions to take to correct the error.

***Table 29: User ID and Directory URI Error Conditions***

| Error Condition | Description | Suggested Action |
|---|---|---|
| Duplicate user IDs | Duplicate user IDs are assigned to one or more users on different clusters within the intercluster deployment. The affected users may be homed on an intercluster peer.<br>**Related alarms**:<br>`DuplicateUserid` | If the `DuplicateUserid` alert is raised, take immediate action to correct the issue. Each user within the intercluster deployment must have a unique user ID. |
| Duplicate directory URIs | Multiple users within the intercluster deployment are assigned the same directory URI value. The affected users may be homed on an intercluster peer.<br>**Related alarms**:<br>• `DuplicateUserid`<br>• `DuplicateDirectoryURIWarning` | If your system is configured to use the Directory URI IM address scheme and the `DuplicateDirectoryURI` alert is raised, take immediate action to correct the issue. Each user must be assigned a unique directory URI.<br>If your system is configured to use the *userID@Default_Domain* IM address scheme and duplicate directory URIs are detected, the `DuplicateDirectoryURIWarning` warning is raised and no immediate action is required; however, Cisco recommends that you resolve the issue. |

| Error Condition | Description | Suggested Action |
|---|---|---|
| Invalid directory URIs | One or more users within the deployment are assigned an invalid or empty directory URI value. A URI that is not in the user@domain format is an invalid Directory URI. The affected users may be homed on an intercluster peer.<br>**Related alarms**:<br>• `InvalidDirectoryURI`<br>• `InvalidDirectoryURIWarning` | If your system is configured to use the Directory URI IM address scheme and the following alert is raised, take immediate action to correct the issue:`InvalidDirectoryURI`.<br>If your system is configured to use the *userID@Default_Domain* IM address scheme and invalid directory URIs are detected, the `InvalidDirectoryURIWarning` warning is raised and no immediate action is required; however, Cisco recommends that you resolve the issue. |

# User ID and Directory URI Validation and Modification

Cisco recommends that you perform a check for duplicate user information rather than wait for alarms to be raised in the system, especially after adding new users or when migrating contact lists.

You can use the System Troubleshooter in the Cisco Unified CM IM and Presence Administration GUI to view a summary of user ID and Directory URI errors. For a more detailed and comprehensive report, use the CLI command to validate IM and Presence Service users.

If any users are identified as having duplicate or invalid information, you can modify the user records in Cisco Unified Communications Manager using the **End User Configuration** window, (**User Management** > **EndUser**). Ensure that all users have a valid user ID or Directory URI value as necessary. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

## User ID and Directory URI CLI Validation Examples

The CLI command to validate IM and Presence Service users to identify users that have duplicate user IDs and duplicate or invalid Directory URIs is **utils users validate { all | userid | uri }**.

For more information about using the CLI and command descriptions, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

### CLI Example Output Showing User ID Errors

```
Users with Duplicate User IDs
---------------------------------------------
 User ID: user3
  Node Name
  cucm-imp-1
  cucm-imp-2
```

### CLI Example Output Showing Directory URI Errors

```
Users with No Directory URI Configured
-----------------------------------------------------
 Node Name: cucm-imp-2
 User ID
 user4
```

```
Users with Invalid Directory URI Configured
-------------------------------------------------------
 Node Name: cucm-imp-2
 User ID   Directory URI
 user1     asdf@ASDF@asdf@ADSF@cisco

Users with Duplicate Directory URIs
-------------------------------------------------------
Directory URI: user1@cisco.com
 Node Name   User ID
 cucm-imp-1  user4
 cucm-imp-2  user3
```

## Set User Check Interval

Use Cisco Unified CM IM and Presence Administration to set the time interval for the Cisco IM and Presence Data Monitor service to check all nodes and clusters in your deployment for duplicate user IDs and directory URIs.

Enter the time interval in minutes using integers. The valid range is from 5 to 1440. The default is 30 minutes.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters**.

**Step 2** Choose **Cisco IM and Presence Data Monitor** in the **Service** field.

**Step 3** Enter an integer from 5 through 1440 as the **User Check Interval** and click **Save**.

## Validate User IDs and Directory URIs Using System Troubleshooter

Use the System Troubleshooter in the Cisco Unified CM IM and Presence Administration GUI to view the status of the system checks which identify duplicate user IDs and duplicate or invalid directory URIs across all nodes and clusters in the deployment.

For a more detailed and comprehensive report, use the CLI command to validate IM and Presence Service users. For more information about using the CLI and command details, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

### Procedure

**Step 1** Choose **Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter**.

**Step 2** Monitor the status of user IDs and Directory URIs in the **User Troubleshooter** area.

The **Problem** column is populated if the system check detects any issues.

- Verify all users have a unique User ID configured.
- Verify all users have a Directory URI configured.
- Verify all users have a unique Directory URI configured.
- Verify all users have a valid Directory URI configured.
- Verify all users have a unique Mail ID configured.

**Note** Duplicate mail IDs impact both Email Address for Federation and Exchange Calendar integration features.

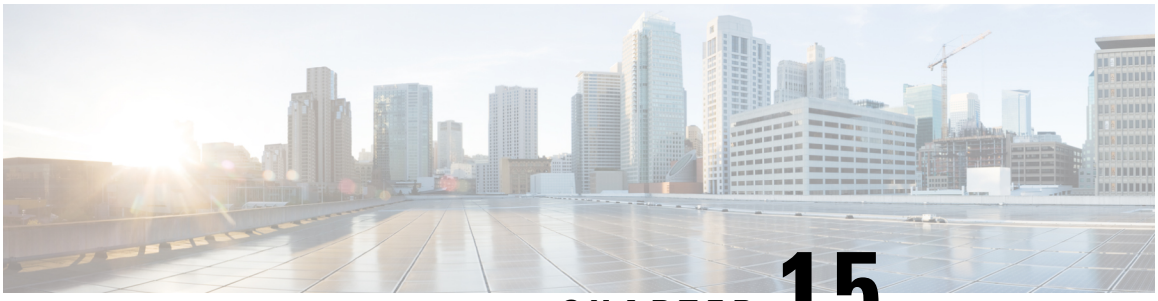
If duplicate or invalid user information is detected, perform the recommended solution. To troubleshoot UserID and directory URI errors, see topics related to troubleshooting.

**Tip** Clicking the **fix** link in the **Solution** column redirects you to the **End User Configuration** window in Cisco Unified Communications Manager Administration where you can locate and reconfigure user profiles. For detailed user validation information, use the CLI command to validate users.

**Note** The user ID and directory URI fields in the user profile may be mapped to the LDAP Directory. In that case, apply the fix in the LDAP Directory server.

### Related Topics

Received Duplicate UserID Error, on page 239
Received Duplicate or Invalid Directory URI Error, on page 240



CHAPTER 15

# User Migration


• User Migration Between IM and Presence Service Clusters, on page 213


# User Migration Between IM and Presence Service Clusters

This section describes how to migrate users between IM and Presence Service clusters. You must complete the following procedures in the order in which they are presented:

1. Unassign the migrating users from their current cluster.
2. Before migrating users, remove all stale rosters, group entries and non-presence contract records..
3. Export the contact lists of the migrating users from their current home cluster.
4. Disable the migrating users for IM and Presence Service and Cisco Jabber on their current home cluster from Cisco Unified Communications Manager.
5. If LDAP Sync is enabled on Cisco Unified Communications Manager:
   - move the users to the new Organization Unit, from which their new cluster synchronizes its information
   - synchronize the users to the new home Cisco Unified Communications Manager.
6. If LDAP Sync is not enabled on Cisco Unified Communications Manager, manually provision the migrating users on Cisco Unified Communications Manager.
7. Enable users for IM and Presence Service and Cisco Jabber.
8. Import contact lists to the new home cluster to restore contact list data for migrated users.

### Before You Begin

Complete the following tasks:

- Perform a full DRS of the current cluster and the new home cluster. See the *Disaster Recovery System Administration Guide* for more information.
- Ensure that the following services are running:
  - Cisco Intercluster Sync Agent
  - Cisco AXL Web Service

- Cisco Sync Agent

- Run the Troubleshooter and ensure that there are no Intercluster Sync Agent issues reported. All Intercluster Sync Agent issues reported on the Troubleshooter must be resolved before proceeding with this procedure.
- Cisco recommends that the **Allow users to view the availability of other users without being prompted for approval** setting is enabled. To enable this setting, choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Settings**. Any change to this setting requires a restart of the Cisco XCP Router.
- Cisco recommends that the following settings are set to **No Limit**:
  - Maximum Contact List Size (per user)
  - Maximum Watchers (per user)

  To configure these settings, choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Settings**.
- Ensure that the users to be migrated are licensed for Cisco Unified Presence or Cisco Jabber on their current (pre-migration) home cluster only. If these users are licensed on any other cluster, they need to be fully unlicensed before proceeding with the following procedures.

# Unassign Users From Current Cluster

Complete this procedure to unassign the migrating users from their current cluster.

### Procedure

**Step 1** Choose **Cisco Unified CM Administration** > **User Management** > **Assign Presence Users**.

**Step 2** Choose the users that you want to migrate to a remote IM and Presence cluster.

**Step 3** Click **Assign Selected Users** and in the next dialog box, click **Unassigned.**

**Step 4** Click **Save**.

### What to do next

Proceed to export your user contact lists.

# Remove Stale Entries

Before migrating users, remove stale rosters, group entries and non-presence contact records. This is to be done on the publisher IM&P node from which the users had presence disabled.

**Note** Repeat these steps as necessary in batches of 2000. If it is too time consuming to remove a large amount of stale entries via CLI, open a TAC case to leverage the stale roster script at the end of this section that requires root access.

**Procedure**

**Step 1** Start the CLI session. For details on how to start a CLI session, refer to the "Start CLI session" section of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

**Step 2** Check and remove stale roster entries. To do this, run the following queries:

a) Check for stale roster entries:

```
run sql select count(*) from rosters where user_id in (select xcp_user_id from enduser
where primarynodeid is NULL)
```

b) Remove stale roster entries:

```
run sql delete from rosters where pkid in (select * from (select first 2000 pkid from
rosters where user_id in (select xcp_user_id from enduser where primarynodeid is NULL)))
```

**Step 3** Check and remove stale group records. To do this, run the following queries:

a) Check for stale group records:

```
run sql select count(*) from groups where user_id in (select xcp_user_id from enduser
where primarynodeid is NULL)
```

b) Remove stale group records:

```
run sql delete from groups where pkid in (select * from (select first 2000 pkid from
groups where user_id in (select xcp_user_id from enduser where primarynodeid is NULL)))
```

**Step 4** Check and remove stale non-contact records (in order). To do this, run the following queries:

a) Check for stale non-contact records (in order):

```
run sql select count(*) from nonpresencecontacts where fkenduser in (select pkid from
enduser where primarynodeid is null)
```

b) Remove stale non-contact records (in order):

```
run sql delete from nonpresencecontacts where pkid in (select * from (select first 2000
 pkid from nonpresencecontacts where fkenduser in (select pkid from enduser where
primarynodeid is null)))
```

c) Use this query if you have root access:

```
run sql delete from epascontactaddinfo where pkid in (select * from (select first 2000
pkid from epascontactaddinfo where pkid not in (select fkepascontactaddinfo from
nonpresencecontacts)))
```

# Export User Contact Lists

Complete this procedure to export the contact lists of the migrating from their current cluster.

### Procedure

**Step 1** Export the contact lists of the migrating users from the current home cluster.

a) Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Contact List** > **Export**.
b) Choose **All unassigned users in the cluster** and click **Find.**
c) Review the results and use the **AND/OR** filter to filter the search results as required.
d) When the list is complete, click **Next.**
e) Choose a filename for the exported contact list data.
f) Optionally update the Job Description.
g) Click **Run Now** or schedule the job to run later.

**Step 2** Monitor the status of the contact list export job.

a) Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Job Scheduler**.
b) Click **Find** to list all BAT jobs.
c) Find your contact list export job and when it is reported as completed, choose the job.
d) Choose the CSV File Name link to view the contents of the contact list export file. Note that a timestamp is appended to the filename.
e) From the **Job Results** section, choose the log file to see a summary of what was uploaded. The job begin and end time is listed and a result summary for the job is presented.

**Step 3** Download the contact list export file and store it for use later when the user migration is complete.

a) Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Upload/Download Files**.
b) Click **Find.**
c) Choose the contact list export file and click **Download Selected**.
d) Save the CSV file locally for upload later in the procedure.

### What to do next

Proceed to unlicense the users.

# Disable Users for IM and Presence Service

The following procedure describes how to disable a migrating user for IM and Presence Service and Cisco Jabber on their current home cluster.

For information about how to update users in bulk, see the *Cisco Unified Communications Manager Bulk Administration Guide*.

### Procedure

**Step 1** Choose **Cisco Unified CM Administration** > **User Management** > **End User**.

**Step 2** Use the filters to find the user that you want to disable for IM and Presence Service.

**Step 3** In the **End User Configuration** screen, uncheck **Enable User for Unified CM IM and Presence**.

**Step 4** Click **Save**.

# Move Users to New Cluster

The procedure to move the users to the new cluster differs depending on whether LDAP Sync is enabled on Cisco Unified Communications Manager.

## LDAP Sync Enabled on Cisco Unified Communications Manager

If LDAP Sync is enabled on Cisco Unified Communications Manager, you must move users to the new Organizational Unit and synchronize the users to the new home cluster.

### Move Users To New Organizational Unit

If LDAP Sync is enabled on Cisco Unified Communications Manager, you must move the users to the new Organizational Unit (OU) from which their new cluster synchronizes if the deployment uses a separate LDAP structure (OU divided) for each cluster, where users are only synchronized from LDAP to their home cluster.

**Note** You do not need to move the users if the deployment uses a flat LDAP structure, that is, all users are synchronized to all Cisco Unified Communications Manager and IM and Presence Service clusters where users are licensed to only one cluster.

For more information about how to move the migrating users to the relevant OU of the new home cluster, see the LDAP Administration documentation.

After you move the users, you must delete the LDAP entries from the old LDAP cluster.

#### What to do next

Proceed to synchronize the users to the new home cluster.

### Synchronize Users To New Home Cluster

If LDAP is enabled on Cisco Unified Communications Manager, you must synchronize the users to the new home Cisco Unified Communications Manager cluster. You can do this manually on Cisco Unified Communications Manager or you can wait for a scheduled synchronization on Cisco Unified Communications Manager.

To manually force the synchronization on Cisco Unified Communications Manager, complete the following procedure.

#### Procedure

**Step 1** From Cisco Unified CM Administration, choose **System** > **LDAP** > **LDAP Directory**.

**Step 2** Click **Perform Full Sync Now**.

### What to do next

Proceed to enable users for IM and Presence Service and license users on the new cluster.

### Related Topics

Enable Users For IM and Presence Service On New Cluster, on page 218

## LDAP Sync Not Enabled On Cisco Unified Communications Manager

If LDAP Sync is not enabled on Cisco Unified Communications Manager, you must manually provision the users on the new Cisco Unified Communications Manager cluster. See the *Cisco Unified Communications Manager Administration Guide* for more information.

# Enable Users For IM and Presence Service On New Cluster

When the users have been synchronized, or manually provisioned, on the new home cluster, you must enable the users for IM and Presence Service and Cisco Jabber.

### Procedure

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

**Step 2** Use the filters to find the user that you want to enable for IM and Presence Service.

**Step 3** In the **End User Configuration** screen, check **Enable User for Unified CM IM and Presence**.

**Step 4** Click **Save**.

**Step 5** Provision the users on Cisco Unified Communications Manager for Phone and CSF. See the *Cisco Unified Communications Manager Administration Guide* for more information.

For information about how to update users in bulk, see the *Cisco Unified Communications Manager Bulk Administration Guide*.

### What to do next

Proceed to import contact lists on the new home cluster.

# Import Contact Lists On Home Cluster

You must import the contact lists to restore contact data for the migrated users.

### Procedure

**Step 1** Upload the previously exported contact list CSV file.

a) Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Upload/Download Files**.

b) Click **Add New**.

c) Click **Browse** to locate and choose the contact list CSV file.

d) Choose **Contact Lists** as the Target.

e) Choose **Import Users' Contacts - Custom File** as the Transaction Type,
f) Optionally check **Overwrite File if it exists**.
g) Click **Save** to upload the file.

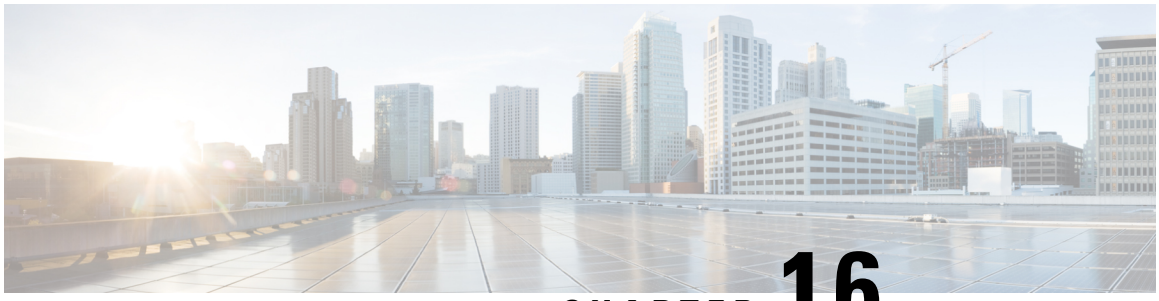
**Step 2** Run the import contact list job.

a) Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Contact List** > **Update**.
b) Choose the CSV file you uploaded in Step 1.
c) Optionally update the Job Description.
d) To run the job now, click **Run Immediately**. Click **Run Later** to schedule the update for a later time.
e) Click **Submit.**

**Step 3** Monitor the contact list import status.

a) Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Job Scheduler**.
b) Click **Find** to list all BAT jobs.
c) Choose the job ID of the contact list import job when its status is reported as complete.
d) To view the contents of the contact list file, choose the file listed at **CSV File Name**.
e) Click the **Log File Name** link to open the log.

The begin and end time of the job is listed and a result summary is also displayed.



CHAPTER 16

# Multilingual Support Configuration For IM and Presence Service


- Locale Installation, on page 221
- Install Locale Installer on IM and Presence Service, on page 223
- Error Messages, on page 224
- Localized Applications, on page 226


## Locale Installation

You can configure Cisco Unified Communications Manager and IM and Presence Service to support multiple languages. There is no limit to the number of supported languages you can install.

Cisco provides locale-specific versions of the Cisco Unified Communications Manager Locale Installer and the IM and Presence Service Locale Installer on www.cisco.com. Installed by the system administrator, the locale installer allows the user to view/receive the chosen translated text or tones, if applicable, when a user works with supported interfaces.

After you upgrade Cisco Unified Communications Manager or the IM & Presence Service, you must reinstall all the locales. Install the latest version of the locales that match the major.minor version number of your Cisco Unified Communications Manager node or IM and Presence Service node.

Install locales after you have installed Cisco Unified Communications Manager on every node in the cluster and have set up the database. If you want to install specific locales on IM and Presence Service nodes, you must first install the Cisco Unified Communications Manager locale file for the same country on the Cisco Unified Communications Manager cluster.

Use the information in the following sections to install locales on Cisco Unified Communications Manager nodes and on IM and Presence Service nodes after you complete the software upgrade.

### User Locales

User locale files contain language information for a specific language and country. They provide translated text and voice prompts, if available, for phone displays, user applications, and user web pages in the locale that the user chooses. These files use the following naming convention:.

- cm-locale-language-country-version.cop (Cisco Unified Communications Manager)
- ps-locale-language_country-version.cop (IM and Presence Service)

If your system requires user locales only, install them after you have installed the CUCM locale.

### Network Locales

Network locale files provide country-specific files for various network items, including phone tones, annunciators, and gateway tones. The combined network locale file uses the following naming convention:

- cm-locale-combinednetworklocale-version.cop (Cisco Unified Communications Manager)

Cisco may combine multiple network locales in a single locale installer.

**Note** Virtualized deployments of Cisco Unified Communications Manager on Cisco-approved, customer-provided servers can support multiple locales. Installing multiple locale installers ensures that the user can choose from a multitude of locales.

You can install locale files from either a local or a remote source by using the same process for installing software upgrades. You can install more than one locale file on each node in the cluster. Changes do not take effect until you reboot every node in the cluster. Cisco strongly recommends that you do not reboot the nodes until you have installed all locales on all nodes in the cluster. Minimize call-processing interruptions by rebooting the nodes after regular business hours.

## Locale Installation Considerations

Install locales after you have installed Cisco Unified Communications Manager on every node in the cluster and have set up the database. If you want to install specific locales on IM and Presence Service nodes, you must first install the Cisco Unified Communications Manager locale file for the same country on the Cisco Unified Communications Manager cluster.

You can install more than one locale file on each node in the cluster. To activate the new locale, you must restart each node in the cluster after installation.

You can install locale files from either a local or a remote source by using the same process for installing software upgrades. See the *Upgrade Guide for Cisco Unified Communications Manager* for more information about upgrading from a local or a remote source.

## Locale Files

Install locales after you have installed Cisco Unified Communications Manager on every node in the cluster and have set up the database. If you want to install specific locales on IM and Presence Service nodes, you must first install the Cisco Unified Communications Manager locale file for the same country on the Cisco Unified Communications Manager cluster.

You can install more than one locale file on each node in the cluster. To activate the new locale, you must restart each node in the cluster after installation.

When you install locales on a node, install the following files:

- User Locale files - These files contain language information for a specific language and country and use the following convention:

  `cm-locale-language-country-version.cop` (Cisco Unified Communications Manager)

ps-locale-language_country-version.cop (IM and Presence Service)

- Combined Network Locale file - Contains country-specific files for all countries for various network items, including phone tones, annunciators, and gateway tones. The combined network locale file uses the following naming convention:

  `cm-locale-combinednetworklocale-version.cop` (Cisco Unified Communications Manager)

# Install Locale Installer on IM and Presence Service

### Before you begin

- Install the Locale Installer on Cisco Unified Communications Manager. If you want to use a locale other than English, you must install the appropriate language installers on both Cisco Unified Communications Manager and on IM and Presence Service.
- If your IM and Presence Service cluster has more than one node, make sure that the locale installer is installed on every node in the cluster (install on the IM and Presence database publisher node before the subscriber nodes).
- User locales should not be set until all appropriate locale installers are loaded on both systems. Users may experience problems if they inadvertently set their user locale after the locale installer is loaded on Cisco Unified Communications Manager but before the locale installer is loaded on IM and Presence Service. If issues are reported, we recommend that you notify each user to sign into the Cisco Unified Communications Self Care Portal and change their locale from the current setting to English and then back again to the appropriate language. You can also use the BAT tool to synchronize user locales to the appropriate language.
- You must restart the server for the changes to take effect. After you complete all locale installation procedures, restart each server in the cluster. Updates do not occur in the system until you restart all servers in the cluster; services restart after the server reboots.

### Procedure

**Step 1** Navigate to `cisco.com` and choose the locale installer for your version of IM and Presence Service.

http://software.cisco.com/download/navigator.html?mdfid=285971059

**Step 2** Click the version of the IM and Presence Locale Installer that is appropriate for your working environment.

**Step 3** After downloading the file, save the file to the hard drive and note the location of the saved file.

**Step 4** Copy this file to a server that supports SFTP.

**Step 5** Sign into Cisco Unified IM and Presence Operating System Administration using the administrator account and password.

**Step 6** Choose **Software Upgrades** > **Install/Upgrade**.

**Step 7** Choose Remote File System as the software location source.

**Step 8** Enter the file location, for example `/tmp`, in the Directory field.

**Step 9** Enter the IM and Presence Service server name in the Server field.

**Step 10** Enter your username and password credentials in the User Name and User Password fields.

**Step 11** Choose SFTP for the Transfer Protocol.

**Step 12** Click **Next**.

**Step 13** Choose the IM and Presence Service locale installer from the list of search results.

**Step 14** Click **Next** to load the installer file and validate it.

**Step 15** After you complete the locale installation, restart each server in the cluster.

**Step 16** The default setting for installed locales is "English, United States". While your IM and Presence Service node is restarting, change the language of your browser, if necessary, to match the locale of the installer that you have downloaded.

**Step 17** Verify that your users can choose the locales for supported products.

**Tip** Make sure that you install the same components on every server in the cluster.

# Error Messages

See the following table for a description of the messages that can occur during Locale Installer activation. If an error occurs, you can view the messages in the installation log.

***Table 30: Locale Installer Messages and Descriptions***

| Message | Description |
|---|---|
| [LOCALE] File not found: <language>_<country>_user_locale.csv, the user locale has not been added to the database. | This error occurs when the system cannot locate the CSV file, which contains user locale information to add to the database, which indicates an error with the build process. |
| [LOCALE] File not found: <country>_network_locale.csv, the network locale has not been added to the database. | This error occurs when the system cannot locate the CSV file, which contains network locale information to add to the database This indicates an error with the build process. |
| [LOCALE] CSV file installer installdb is not present or not executable | You must ensure that an application called *installdb* is present. It reads information that a CSV file contains and applies it correctly to the target database. If this application is not found, it did not get installed with the Cisco Unified Communications application (very unlikely), has been deleted (more likely), or the node does not have a Cisco Unified Communications application, such as Cisco Unified Communications Manager or IM and Presence Service, installed (most likely). Installation of the locale will terminate because locales will not work without the correct records in the database. |

| Message | Description |
|---|---|
| [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maDialogs_<ll>_<CC>.properties.Checksum.<br><br>[LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maMessages_<ll>_<CC>.properties.Checksum.<br><br>[LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maGlobalUI_<ll>_<CC>.properties.Checksum.<br><br>[LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt.Checksum. | These errors could occur when the system fails to create a checksum file, which an absent Java executable, `/usr/local/thirdparty/java/j2sdk/jre/bin/java`, `an absent or damaged Java archive file, /usr/local/cm/jar/cmutil.jar`, or an absent or damaged Java class, `com.cisco.ccm.util.Zipper`, causes. Even if these errors occur, the locale will continue to work correctly, with the exception of Cisco Unified Communications Manager Assistant, which can not detect a change in localized Cisco Unified Communications Manager Assistant files. |
| [LOCALE] Could not find /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt in order to update Unified CM Assistant locale information. | This error occurs when the system does not find the file in the correct location, which is most likely due to an error in the build process. |
| [LOCALE] Addition of <locale-installer-file-name> to the database has failed! | This error occurs because the collective result of any failure that occurs when a locale is being installed causes it; it indicates a terminal condition. |
| [LOCALE] Could not locate <locale-installer-file-name> | The system will not migrate this locale during an upgrade.<br><br>The downloaded locale installer file no longer resides in the download location. The platform may have moved or deleted it. This is noncritical error indicates that after the Cisco Unified Communications application has been upgraded, you need to either reapply the locale installer or download and apply a new locale installer. |
| [LOCALE] Could not copy <locale-installer-file-name> to migratory path. This locale will not be migrated during an upgrade! | You cannot copy the downloaded locale installer file to the migration path. This noncritical error indicates that after the Cisco Unified Communications application has been upgraded, you need to either reapply the locale installer or download and apply a new locale installer. |
| [LOCALE] DRS unregistration failed | The locale installer could not deregister from the Disaster Recovery System. A backup or restore record will not include the locale installer. Record the installation log and contact Cisco TAC. |

| Message | Description |
|---|---|
| [LOCALE] Backup failed! | The Disaster Recovery System could not create a tarball from the downloaded locale installer files. Re-apply the local installer before attempting to back up.<br>**Note** Manually reinstalling locales after a system restore achieves the same goal. |
| [LOCALE] No COP files found in restored tarball! | Corruption of backup files may prevent successful extraction of locale installer files.<br>**Note** Manual reapplication of the locale installer will restore the locale fully. |
| [LOCALE] Failed to successfully reinstall COP files! | Corruption of backup files may damage locale installer files.<br>**Note** Manual reapplication of the locale installer will restore the locale fully. |
| [LOCALE] Failed to build script to reinstall COP files! | The platform could not dynamically create the script used to reinstall locales.<br>**Note** Manual reapplication of the locale installer will restore the locale fully. Record the installation log and contact TAC. |

# Localized Applications

IM and Presence Service applications support a variety of different languages. See the following table for a list of localized applications and the available languages.

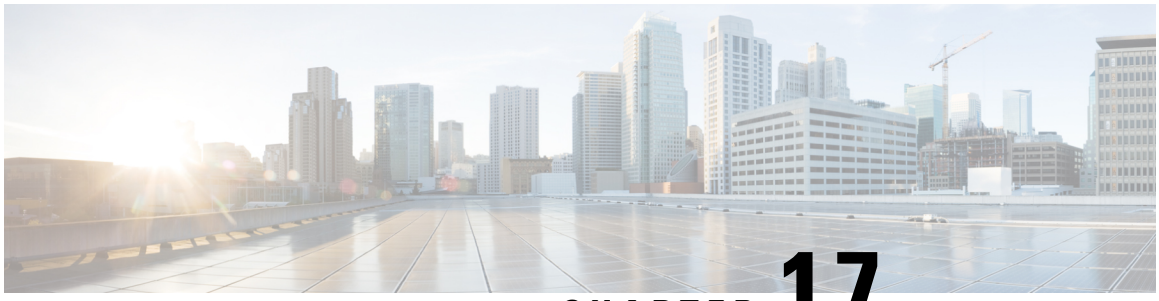
***Table 31: List of Localized Applications and Supported Languages***

| Interface | Supported Languages |
|---|---|
| **Administrative Applications** | |
| Cisco Unified CM IM and Presence Administration | Chinese (China), English, Japanese (Japan), Korean (Korean Republic) |
| Cisco Unified IM and Presence Operating System | Chinese (China), English, Japanese (Japan), Korean (Korean Republic) |

PART V

# Troubleshooting IM and Presence Service


- Troubleshooting High Availability, on page 229
- Troubleshooting UserID and Directory URI Errors, on page 239
- Troubleshooting Single Sign-On, on page 243
- Traces Used To Troubleshoot IM and Presence Service, on page 249



CHAPTER 17

# Troubleshooting High Availability


- Manual Failover, Fallback, and Recovery, on page 229
- View Presence Redundancy Group Node Status, on page 231
- Node State Definitions, on page 232
- Node States, Causes, and Recommended Actions, on page 233


# Manual Failover, Fallback, and Recovery

Use Cisco Unified Communications Manager Administration to initiate a manual failover, fallback, and recovery for IM and Presence Service nodes in a presence redundancy group. You can also initiate these actions from Cisco Unified Communications Manager or IM and Presence Service using the CLI. See the *Command Line Interface Guide for Cisco Unified Communications Solutions* for details.

- Manual failover: When you initiate a manual failover, the Cisco Server Recovery Manager stops the critical services on the failed node. All users from the failed node are disconnected and must re-login to the backup node.

**Note** After a manual failover occurs, critical services will not be started unless we invoke manual fallback.

- Manual fallback: When you initiate a manual fallback, the Cisco Server Recovery Manager restarts critical services on the primary node and disconnects all users that had been failed over. Those users must then re-login to their assigned node.
- Manual recovery: When both nodes in the presence redundancy group are in a failed state and you initiate a manual recovery, the IM and Presence Service restarts the Cisco Server Recovery Manager service on both nodes in the presence redundancy group.

## Initiate Manual Failover

You can manually initiate a failover of IM and Presence Service nodes in a presence redundancy group using Cisco Unified Communications Manager Administration.

### Procedure

**Step 1** Select **System** > **Presence Redundancy Groups**.

The **Find and List Presence Redundancy Groups** window displays.

**Step 2** Select the presence redundancy group search parameters, and then click **Find**.

Matching records appear.

**Step 3** Select the presence redundancy group that is listed in the **Find and List Presence Redundancy Group** window.

The **Presence Redundancy Group Configuration** window appears.

**Step 4** Click **Failover** in the ServerAction field.

**Note** This button appears only when the server and presence redundancy group are in the correct states.

# Initiate Manual Fallback

Use Cisco Unified Communications Manager Administration to manually initiate the fallback of an IM and Presence Service node in a presence redundancy group that has failed over. For more information about presence redundancy group node status, see topics related to node state, state change causes, and recommended actions.

### Procedure

**Step 1** Select **System** > **Presence Redundancy Groups**.

The **Find and List Presence Redundancy Groups** window displays.

**Step 2** Select the presence redundancy group search parameters, and then click **Find**.

Matching records appear.

**Step 3** Select the presence redundancy group that is listed in the **Find and List Presence Redundancy Group** window.

The **Presence Redundancy Group Configuration** window appears.

**Step 4** Click **Fallback** in the ServerAction field.

**Note** This button appears only when the server and presence redundancy group are in the correct states.

# Initiate Manual Recovery

A manual recovery is necessary when both nodes in the presence redundancy group are in the failed state. Use Cisco Unified Communications Manager Administration to manually initiate the recovery of IM and Presence Service nodes in a presence redundancy group that is in the failed state.

For more information about presence redundancy group node status, see topics related to node state, state change causes, and recommended actions.

### Before you begin

A manual recovery is necessary when both nodes in the presence redundancy group are in the failed state. Use Cisco Unified Communications Manager Administration to manually initiate the recovery of IM and Presence Service nodes in a presence redundancy group that is in the failed state.

### Procedure

**Step 1** Select **System** > **Presence Redundancy Groups**.

The **Find and List Presence Redundancy Groups** window displays.

**Step 2** Select the presence redundancy group search parameters, and then click **Find**.

Matching records appear.

**Step 3** Select the presence redundancy group that is listed in the **Find and List Presence Redundancy Group** window.

The **Presence Redundancy Group Configuration** window appears.

**Step 4** Click **Recover**.

**Note** This button appears only when the server and presence redundancy group are in the correct states.

# View Presence Redundancy Group Node Status

Use the **Cisco Unified CM Administration** user interface to view the status of IM and Presence Service nodes that are members of a presence redundancy group.

### Procedure

**Step 1** Choose **System** > **Presence Redundancy Groups**.

The **Find and List Presence Redundancy Groups** window displays.

**Step 2** Choose the presence redundancy group search parameters, and then click **Find**.

Matching records appear.

**Step 3** Choose a presence redundancy group that is listed in the search results.

The **Presence Redundancy Group Configuration** window appears. If two nodes are configured in that group and high availability is enabled, then the status of the nodes within that group are displayed in the High Availability area.

# Node State Definitions

*Table 32: Presence Redundancy Group Node State Definitions*

| State | Description |
|---|---|
| Initializing | This is the initial (transition) state when the Cisco Server Recovery Manager service starts; it is a temporary state. |
| Idle | IM and Presence Service is in Idle state when failover occurs and services are stopped. In Idle state, the IM and Presence Service node does not provide any availability or Instant Messaging services. In Idle state, you can manually initiate a fallback to this node using the **Cisco Unified CM Administration** user interface. |
| Normal | This is a stable state. The IM and Presence Service node is operating normally. In this state, you can manually initiate a failover to this node using the **Cisco Unified CM Administration** user interface. |
| Running in Backup Mode | This is a stable state. The IM and Presence Service node is acting as the backup for its peer node. Users have moved to this (backup) node. |
| Taking Over | This is a transition state. The IM and Presence Service node is taking over for its peer node. |
| Failing Over | This is a transition state. The IM and Presence Service node is being taken over by its peer node. |
| Failed Over | This is a steady state. The IM and Presence Service node has failed over, but no critical services are down. In this state, you can manually initiate a fallback to this node using the **Cisco Unified CM Administration** user interface. |
| Failed Over with Critical Services Not Running | This is a steady state. Some of the critical services on the IM and Presence Service node have either stopped or failed. |
| Falling Back | This is a transition state. The system is falling back to this IM and Presence Service node from the node that is running in backup mode. |
| Taking Back | This is a transition state. The failed IM and Presence Service node is taking back over from its peer. |
| Running in Failed Mode | An error occurs during the transition states or Running in Backup Mode state. |
| Unknown | Node state is unknown.<br>A possible cause is that high availability was not enabled properly on the IM and Presence Service node. Restart the Server Recovery Manager service on both nodes in the presence redundancy group. |

# Node States, Causes, and Recommended Actions

You can view the status of nodes in a presence redundancy group on the **Presence Redundancy Group Configuration** window when you choose a group using the **Cisco Unified CM Administration** user interface.

*Table 33: Presence Redundancy Group Node High-Availability States, Causes, and Recommended Actions*

| Node 1 | | Node 2 | | |
|---|---|---|---|---|
| **State** | **Reason** | **State** | **Reason** | **Cause/Recommended Actions** |
| Normal | Normal | Normal | Normal | Normal |
| Failing Over | On Admin Request | Taking Over | On Admin Request | The administrator initiated a manual failover from node 1 to node 2. The manual failover is in progress. |
| Idle | On Admin Request | Running in Backup Mode | On Admin Request | The manual failover from node 1 to node 2 that the administrator initiated is complete. |
| Taking Back | On Admin Request | Falling Back | On Admin Request | The administrator initiated a manual fallback from node 2 to node 1. The manual fallback is in progress. |
| Idle | Initialization | Running in Backup Mode | On Admin Request | The administrator restarts the SRM service on node 1 while node 1 is in “Idle” state. |
| Idle | Initialization | Running in Backup Mode | Initialization | The administrator either restarts both nodes in the presence redundancy group, or restarts the SRM service on both nodes while the presence redundancy group was in manual failover mode. |
| Idle | On Admin Request | Running in Backup Mode | Initialization | The administrator restarts the SRM service on node 2 while node 2 is running in backup mode, but before the heartbeat on node 1 times out. |
| Failing Over | On Admin Request | Taking Over | Initialization | The administrator restarts the SRM service on node 2 while node 2 is taking over, but before the heartbeat on node1 times out. |
| Taking Back | Initialization | Falling Back | On Admin Request | The administrator restarts the SRM service on node 1 while taking back, but before the heartbeat on node 2 times out. After the taking back process is complete, both nodes are in Normal state. |
| Taking Back | Automatic Fallback | Falling Back | Automatic Fallback | Automatic Fallback has been initiated from node 2 to node 1 and is currently in progress. |

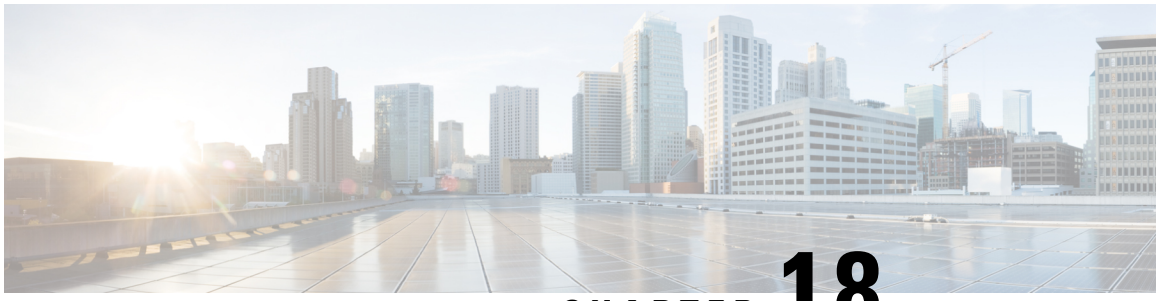
| Node 1 | | Node 2 | | |
|---|---|---|---|---|
| **State** | **Reason** | **State** | **Reason** | **Cause/Recommended Actions** |
| Failed Over | Initialization or Critical Services Down | Running in Backup Mode | Critical Service Down | Node 1 transitions to Failed Over state when either of the following conditions occur:<br>• Critical services come back up due to a reboot of node 1.<br>• The administrator starts critical services on node 1 while node 1 is in Failed Over with Critical Services Not Running state.<br>When node 1 transitions to Failed Over state the node is ready for the administrator to perform a manual fallback to restore the nodes in the presence redundancy group to Normal state. |
| Failed Over with Critical Services not Running | Critical Service Down | Running in Backup Mode | Critical Service Down | A critical service is down on node 1. IM and Presence Service performs an automatic failover to node 2.<br>**Recommended Actions:**<br>**1.** Check node 1 for any critical services that are down and try to manually start those services.<br>**2.** If the critical services on node 1 do not start, then reboot node 1.<br>**3.** When all the critical services are up and running after the reboot, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state. |
| Failed Over with Critical Services not Running | Database Failure | Running in Backup Mode | Database Failure | A database service is down on node 1. IM and Presence Service performs an automatic failover to node 2.<br>**Recommended Actions:**<br>**1.** Reboot node 1.<br>**2.** When all the critical services are up and running after the reboot, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state. |

| Node 1 | | Node 2 | | |
|---|---|---|---|---|
| **State** | **Reason** | **State** | **Reason** | **Cause/Recommended Actions** |
| Running in Failed Mode | Start of Critical Services Failed | Running in Failed Mode | Start of Critical Services Failed | Critical services fail to start while a node in the presence redundancy group is taking back from the other node.<br>**Recommended Actions.** On the node that is taking back, perform the following actions:<br>**1.** Check the node for critical services that are down. To manually start these services, click **Recovery** in the **Presence Redundancy Group Configuration** window.<br>**2.** If the critical services do not start, reboot the node.<br>**3.** When all the critical services are up and running after the reboot, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state. |
| Running in Failed Mode | Critical Service Down | Running in Failed Mode | Critical Service Down | Critical services go down on the backup node. Both nodes enter the failed state.<br>**Recommended Actions:**<br>**1.** Check the backup node for critical services that are down. To start these services manually, click **Recovery** in the **Presence Redundancy Group Configuration** window.<br>**2.** If the critical services do not start, reboot the node. |

| Node 1 | | Node 2 | | |
|---|---|---|---|---|
| **State** | **Reason** | **State** | **Reason** | **Cause/Recommended Actions** |
| Node 1 is down due to loss of network connectivity or the SRM service is not running. | | Running in Backup Mode | Peer Down | Node 2 has lost the heartbeat from node 1. IM and Presence Service performs an automatic failover to node 2.<br>**Recommended Action.** If node 1 is up, perform the following actions:<br>**1.** Check and repair the network connectivity between nodes in the presence redundancy group. When you reestablish the network connection between the nodes, the node may go into a failed state. Click **Recovery** in the **Presence Redundancy Group Configuration** window to restore the nodes to the Normal state.<br>**2.** Start the SRM service and perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state.<br>**3.** (If the node is down) Repair and power up node 1.<br>**4.** When the node is up and all critical services are running, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state. |
| Node 1 is down (due to possible power down, hardware failure, shutdown, reboot) | | Running in Backup Mode | Peer Reboot | IM and Presence Service performs an automatic failover to node 2 due to the following possible conditions on node 1:<br>• hardware failure<br>• power down<br>• restart<br>• shutdown<br>**Recommended Actions:**<br>**1.** Repair and power up node 1.<br>**2.** When the node is up and all critical services are running, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state. |

| Node 1 | | Node 2 | | |
|---|---|---|---|---|
| **State** | **Reason** | **State** | **Reason** | **Cause/Recommended Actions** |
| Failed Over with Critical Services not Running OR Failed Over | Initialization | Backup Mode | Peer Down During Initialization | Node 2 does not see node 1 during startup.<br>**Recommended Action:**<br>When node1 is up and all critical services are running, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state. |
| Running in Failed Mode | Cisco Server Recovery Manager Take Over Users Failed | Running in Failed Mode | Cisco Server Recovery Manager Take Over Users Failed | User move fails during the taking over process.<br>**Recommended Action:**<br>Possible database error. Click **Recovery** in the **Presence Redundancy Group Configuration** window. If the problem persists, then reboot the nodes. |
| Running in Failed Mode | Cisco Server Recovery Manager Take Back Users Failed | Running in Failed Mode | Cisco Server Recovery Manager Take Back Users Failed | User move fails during falling back process.<br>**Recommended Action:**<br>Possible database error. Click **Recovery** in the **Presence Redundancy Group Configuration** window. If the problem persists, then reboot the nodes. |
| Running in Failed Mode | Unknown | Running in Failed Mode | Unknown | The SRM on a node restarts while the SRM on the other node is in a failed state, or an internal system error occurs.<br>**Recommended Action:**<br>Click **Recovery** in the **Presence Redundancy Group Configuration** window. If the problem persists, then reboot the nodes. |
| Backup Activated | Auto Recover Database Failure | Failover Affected Services | Auto Recovery Database Failure. | The database goes down on the backup node. The peer node is in failover mode and can take over for all users in the presence redundancy group. Auto-recovery operation automatically occurs and all users are moved over to the primary node. |
| Backup Activated | Auto Recover Database Failure | Failover Affected Services | Auto Recover Critical Service Down | A critical service goes down on the backup node. The peer node is in failover mode and can take over for all users in the presence redundancy group. Auto-recovery operation automatically occurs and all users are moved over to the peer node. |

| Node 1 | | Node 2 | | |
|---|---|---|---|---|
| **State** | **Reason** | **State** | **Reason** | **Cause/Recommended Actions** |
| Unknown | | Unknown | | Node state is unknown.<br>A possible cause is that high availability was not enabled properly on the IM and Presence Service node.<br>**Recommended Action:**<br>Restart the Server Recovery Manager service on both nodes in the presence redundancy group. |



CHAPTER 18

# Troubleshooting UserID and Directory URI Errors


- Received Duplicate UserID Error, on page 239
- Received Duplicate or Invalid Directory URI Error, on page 240


## Received Duplicate UserID Error

**Problem** I received an alarm indicating that there are duplicate user IDs and I have to modify the contact information for those users.

**Solution** Perform the following steps.

1. Use the **utils users validate { all | userid | uri }** CLI command to generate a list of all users. For more information about using the CLI, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

   The UserID is entered in the result set and is followed by the list of servers where the duplicate UserIDs are homed. The following sample CLI output shows UserID errors during output:

   ```
   Users with Duplicate User IDs
   ---------------------------------------------
    User ID: user3
     Node Name
     cucm-imp-1
     cucm-imp-2
   ```

2. If the same user is assigned to two different clusters, then unassign the user from one of the clusters.
3. If different users on different clusters have the same User ID assigned to them, then rename the UserID value for one of the users to ensure there is no longer any duplication.
4. If the user information is invalid or empty, proceed to correct the user ID information for that user using the Cisco Unified Communications Manager Administration GUI.
5. You can modify the user records in Cisco Unified Communications Manager using the **End User Configuration** window, (**User Management** > **EndUser**) to ensure that all users have a valid user ID or Directory URI value as necessary. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

**Note** The user ID and directory URI fields in the user profile may be mapped to the LDAP Directory. In that case, apply the fix in the LDAP Directory server.

6. Run the CLI command to validate users again to ensure that there are no more duplicate user ID errors.

# Received Duplicate or Invalid Directory URI Error

**Problem** I received an alarm indicating that there are duplicate or invalid user Directory URIs and I have to modify the contact information for those users.

**Solution** Perform the following steps.

1. Use the **utils users validate { all | userid | uri }** CLI command to generate a list of all users. For more information about using the CLI, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

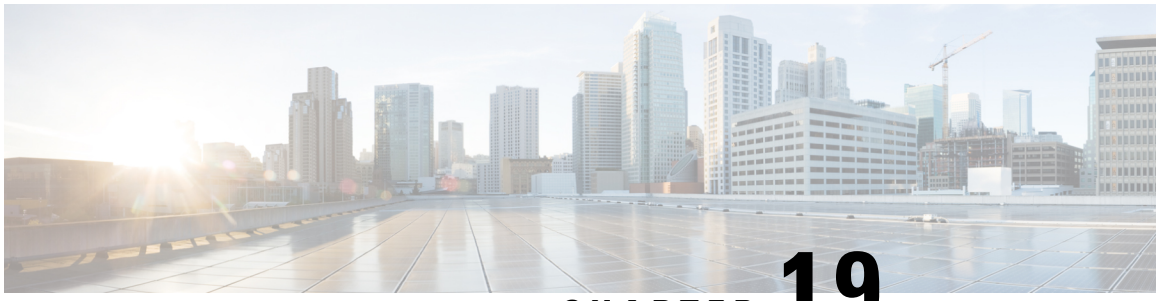
   The Directory URI value is entered in the result set and is followed by the list of servers where the duplicate or invalid Directory URIs are homed. The following sample CLI output shows Directory URI errors detected during a validation check:

```
Users with No Directory URI Configured
--------------------------------------------------
 Node Name: cucm-imp-2
 User ID
 user4

Users with Invalid Directory URI Configured
--------------------------------------------------
 Node Name: cucm-imp-2
 User ID   Directory URI
 user1     asdf@ASDF@asdf@ADSF@cisco

Users with Duplicate Directory URIs
--------------------------------------------------
Directory URI: user1@cisco.com
 Node Name   User ID
 cucm-imp-1  user4
 cucm-imp-2  user3
```

2. If the same user is assigned to two different clusters, then unassign the user from one of the clusters.
3. If different users on different clusters have the same Directory URI value assigned to them, then rename the Directory URI value for one of the users to ensure there is no longer any duplication.
4. If the user information is invalid or empty, proceed to correct the user's Directory URI information.
5. You can modify the user records in Cisco Unified Communications Manager using the **End User Configuration** window, (**User Management** > **EndUser**) to ensure that all users have a valid user ID or Directory URI value as necessary. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

**Note** The user ID and directory URI fields in the user profile may be mapped to the LDAP Directory. In that case, apply the fix in the LDAP Directory server.

6. Run the CLI command to validate users again to ensure that there are no more duplicate or invalid Directory URI errors.



CHAPTER 19

# Troubleshooting Single Sign-On


- Security Trust Error Message, on page 243
- "Invalid Profile Credentials" Message, on page 244
- "Module Name Is Invalid" Message, on page 244
- "Invalid OpenAM Access Manager (Openam) Server URL" Message, on page 244
- Web Browser Indicates a 401 Error, on page 244
- Web Browser Indicates a 403 Error or Displays a Blank Screen , on page 245
- "User is not Authorized to Perform this Function" Error, on page 245
- Web Browser Indicates an HTTP 404 Error , on page 245
- Web Browser Indicates an HTTP 500 Error or Displays a Blank Screen, on page 245
- "Authentication Failed" Message, on page 246
- Web Browser Displays OpenAM Login Screen, on page 246
- Web Browser Displays IM and Presence Service Login Screen, on page 246
- Internet Explorer Prompts for Username and Password, on page 247
- "User has no profile on this organization" Message, on page 247
- Problems Enabling SSO, on page 247
- Certificate Failure, on page 248


## Security Trust Error Message

**Problem** When enabling the Single Sign-On feature, a 'Security trust error' message displays.

**Possible Cause** There may be a security certificate issue causing the IM and Presence Service node to not trust the OpenAM node.

**Solution** Ensure that the following certificates have been uploaded to the IM and Presence Service node and that the Tomcat service on the IM and Presence Service node has been restarted: OpenAM self-signed certificate if that was the chosen approach when Java was installed and Root certificate and any intermediate certificate that signed the OpenAM certificate if that was the chosen approach when Java was installed. You must also ensure that the correct OpenAM URL is specified on the GUI when enabling SSO. The OpenAM URL must be the Fully Qualified Domain Name with the port number. For example, `https://openam-01.corp28.com:8443/opensso`.

### Related Topics

Install Java, on page 150

# "Invalid Profile Credentials" Message

**Problem** When enabling SSO, an 'Invalid Profile Credentials' message displays.

**Possible Cause** You may be specifying the incorrect name and password for the IM and Presence Service node J2EE Agent.

**Solution** Confirm the name and password values that are set for the J2EE agent profile on the OpenAM server. These are the values that you must specify when enabling SSO.

**Related Topics**

Set Up J2EE Agent Profile On OpenAM Server, on page 164

# "Module Name Is Invalid" Message

**Problem** When enabling Single Sign-On, a 'Module Name is Invalid' message displays.

**Possible Cause** You may be specifying the incorrect name for the SSO Module Instance.

**Solution** Review the instructions to set up the SSO module instance.

**Related Topics**

Set Up SSO Module Instance, on page 163

# "Invalid OpenAM Access Manager (Openam) Server URL" Message

**Problem** When enabling Single Sign-On, an 'Invalid OpenAM Access Manager (Openam) Server URL' message displays.

**Possible Cause** The OpenAM URL specified on the GUI or CLI when enabled SSO may not be correct.

**Solution** Ensure that the correct OpenAM URL is specified on the GUI when you enable SSO. The OpenAM URL must be the Fully Qualified Domain Name with the port number. For example, `https://server1.cisco.com:8443/opensso`. You must also ensure that the OpenAM server is up and running and that the OpenAM administration GUI is accessible.

# Web Browser Indicates a 401 Error

**Problem** When accessing an SSO-enabled web application for an IM and Presence node, the web browser indicates an HTTP 401 error code.

**Possible Cause** There may be a problem with the user's browser settings.

**Solution** Review the instructions to set up the client browser for Single Sign-On.

**Related Topics**

Client Browser Setup for Single Sign-On, on page 148

# Web Browser Indicates a 403 Error or Displays a Blank Screen

**Problem** When accessing an SSO-enabled web application for an IM and Presence Service node, the web browser indicates an HTTP 403 error code or I get a blank screen.

**Possible Cause** There may be a problem with OpenAM policy configuration for this IM and Presence Service node.

**Solution** Ensure that you added all six policy rules for this IM and Presence Service node and that all policy rules have been enabled with GET/POST actions and are set to Allow. You must also ensure that the Subject has been added to the policy.

**Related Topics**

Set Up Policies On OpenAM Server, on page 161

# "User is not Authorized to Perform this Function" Error

**Problem** After accessing the web application and trying to access a page, the following message displays: "User is not authorized to perform this function".

**Possible Cause** There may be a problem with the user's assigned permissions for IM and Presence Service.

**Solution** If access to IM and Presence Service web applications is failing, ensure that the user is a member of the *Standard CCM Super Users* group or a group with the equivalent roles on this IM and Presence Service node.

# Web Browser Indicates an HTTP 404 Error

**Problem** When accessing an SSO-enabled web application for an IM and Presence Service node, the web browser indicates an HTTP 404 error code.

**Possible Cause** There may be a problem with one of the following configurations for this IM and Presence Service node: OpenAM policy configuration or OpenAM J2EE Agent configuration.

**Solution** Ensure you are not attempting to access this IM and Presence Service node using a URL that contains the hostname only; this is not supported when SSO is enabled for a web application. Review the policy rules for this IM and Presence Service node. Also ensure that you have added the Login Processing URIs to this IM and Presence Service J2EE agent configuration on the OpenAM server.

**Related Topics**

Set Up Policies On OpenAM Server, on page 161
Set Up J2EE Agent Profile On OpenAM Server, on page 164

# Web Browser Indicates an HTTP 500 Error or Displays a Blank Screen

**Problem** When accessing an SSO-enabled web application for an IM and Presence Service node, the web browser indicates an HTTP 500 error code or a blank screen displays.

**Possible Cause** There may be a problem with OpenAM J2EE Agent configuration for this IM and Presence Service node.

**Solution** Ensure that you have, 1) added the Login Processing URLs for the J2EE Agent for this node and, 2) that you have added the Login Processing URL on the OpenAM Services tab and removed all other Login URLs.

### Related Topics

Set Up J2EE Agent Profile On OpenAM Server, on page 164

# "Authentication Failed" Message

**Problem** When accessing an SSO-enabled web application for an IM and Presence Service node, the web browser displays an OpenAM login screen with an "Authentication failed" message.

**Possible Cause** There may be a problem with the WindowsDesktopSSO login module.

**Solution** Ensure that, 1) all the SSO Module Instance settings are correct, 2) the keytab file exists at the specified directory, and 3) the clocks are synchronized for the following devices:

- **Solution** User's Windows-based computer
- **Solution** Active Directory
- **Solution** OpenAM Server
- **Solution** IM and Presence Service node

### Related Topics

Set Up SSO Module Instance, on page 163

# Web Browser Displays OpenAM Login Screen

**Problem** When accessing an SSO-enabled web application for an IM and Presence Service node, the web browser displays an OpenAM login screen.

**Possible Cause** There may be a problem with OpenAM J2EE Agent configuration for this IM and Presence Service node.

**Solution** Ensure you have added the Login URL on the **OpenAM Services** tab and removed all other Login URLs.

### Related Topics

Set Up J2EE Agent Profile On OpenAM Server, on page 164

# Web Browser Displays IM and Presence Service Login Screen

**Problem** When accessing an SSO-enabled web application for an IM and Presence Service node, the web browser displays the web application login screen.

**Possible Cause** There may be a problem with OpenAM J2EE Agent configuration for this IM and Presence Service node.

**Solution** Ensure you have added the Login Processing URLs for this IM and Presence Service node J2EE Agent.

**Related Topics**

Set Up J2EE Agent Profile On OpenAM Server, on page 164

# Internet Explorer Prompts for Username and Password

**Problem** When accessing an SSO-enabled web application for an IM and Presence Service node, the Internet Explorer web browser prompts you for a username and password.

**Possible Cause** There may be a problem with the user's browser settings.

**Solution** Review the instructions to set up the client browser for Single Sign-On.

**Related Topics**

Client Browser Setup for Single Sign-On, on page 148

# "User has no profile on this organization" Message

**Problem** When accessing an SSO-enabled web application for an IM and Presence Service node, the web browser displays an OpenAM screen with a "User has no profile on this organization" message.

**Possible Cause** The OpenAM User Profile may not be set to **ignored**.

**Solution** See the instructions to set up OpenAM using the GUI Configurator.

**Related Topics**

Set Up OpenAM Using GUI Configurator, on page 159

# Problems Enabling SSO

**Problem** You are unable to enable the SSO feature.

**Possible Cause** If the Tomcat instance on which the OpenAM server is deployed becomes unresponsive or shuts down unexpectedly, you may not be able to enable the SSO feature on IM and Presence Service. In order to enable SSO successfully on IM and Presence Service, OpenAM must be operational. IM and Presence does not monitor the OpenAM Tomcat instance. As a result, no IM and Presence Service alarm or notification generated for this occurrence.

**Solution** If you experience difficulty when enabling SSO from either the Cisco Unified IM and Presence Operating System Administration GUI, verify that Tomcat is running on the OpenAM server. If you continue to experience difficulty after verifying that Tomcat is running on the OpenAM server, restart Tomcat on the OpenAM server and try enabling SSO again.

**Solution** When Tomcat crashes on the OpenAM server, OpenAM becomes unresponsive; IM and Presence Service may not be notified.

# Certificate Failure

**Problem** When using the Certificate Import Tool to validate the communication between OpenAM and IM and Presence Service, you may encounter an error with the "Verify SSL connectivity to the specified certificate server" test. This test may fail with the following error: "The Troubleshooter has encountered an internal error".

**Possible Cause** This error may be the result of the way the OpenAM/Tomcat instance has configured its HTTP Connector.

**Solution** Perform the following steps to resolve the certificate failure.

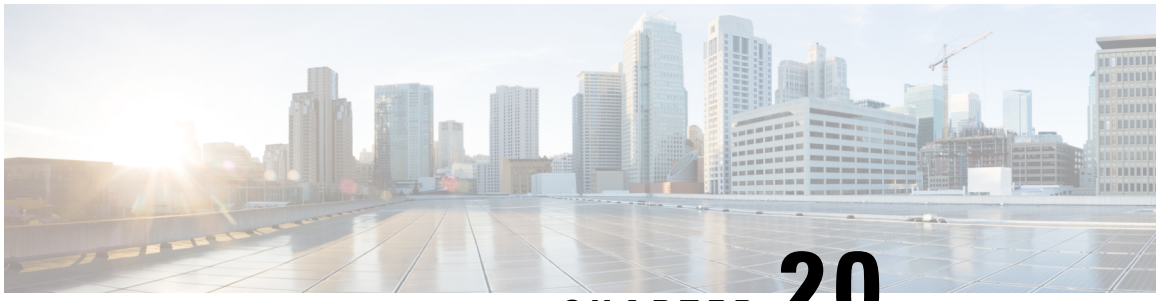
1. Locate the server.xml configuration file on the OpenAM/Tomcat server. This file is typically located here:

   ```
   C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf\server.xml
   ```

2. Check the value set for the **clientAuth** attribute of the **Connector** with a port value of 8443. If this attribute is set to True, this can cause the **Certificate Import Tool** to fail.
3. Change the **clientAuth** attribute to **want** or **false**.
4. Restart the Tomcat service on the OpenAM server.
5. Re-run the **Certificate Import Tool** and import the OpenAM certificate into IM and Presence Service.
6. Change the **clientAuth** attribute back to its original value.
7. Restart the Tomcat service on the OpenAM server.

### Related Topics

Import OpenAM Certificate Into IM and Presence Service, on page 166



CHAPTER 20

# Traces Used To Troubleshoot IM and Presence Service


- Troubleshooting IM and Presence Service Using Trace, on page 249
- Common Traces and Log File Locations for IM and Presence Service Nodes, on page 250
- IM and Presence Service Login and Authentication Traces, on page 251
- Availability, IM, Contact List, and Group Chat Traces, on page 251
- Availability and IM Traces for Partitioned Intradomain Federation MOC Contact Issues, on page 252
- Availability and IM Traces for XMPP-Based Interdomain Federation Contact Issues, on page 253
- Availability and IM Traces for SIP-Based Interdomain Federation Contact Issues, on page 254
- Calendaring Traces, on page 254
- Intercluster Synchronization Traces and Inter-Clustering Troubleshooter, on page 255
- SIP Federation Traces, on page 255
- XMPP Federation Traces, on page 256
- High CPU and Low VM Alert Troubleshooting, on page 256


## Troubleshooting IM and Presence Service Using Trace

You can initiate traces using Cisco Unified IM and Presence Serviceability to help you troubleshoot issues with your IM and Presence Service deployment. After the traces are enabled, you can use either the Real-Time Monitoring Tool (RTMT) or the command line interface (CLI) to access the trace log files.

For instructions on using Serviceability traces for IM and Presence Service, see the *Cisco Unified Serviceability Administration Guide*. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands such as **file list** and **file get** to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

**Tip** Use only SFTP servers for file transfers using CLI commands such as **file get**.

# Common Traces and Log File Locations for IM and Presence Service Nodes

The following table lists common traces that you can perform on your IM and Presence Service node and the resulting log files. You can view the trace log files using the Real-Time Monitoring Tool (RTMT) or using command line interface (CLI) commands such as **file list** and **file get**. Use only SFTP servers for file transfers using CLI commands such as **file get**. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

***Table 34: Common Traces and Trace Log Files for IM and Presence Service Nodes***

| Service | Trace Log Filename |
|---|---|
| Cisco AXL Web Service | `/tomcat/logs/axl/log4j/axl.log` |
| Cisco Intercluster Sync Agent | `/epas/trace/epassa/log4j/icSyncAgent.log` |
| Cisco Presence Engine | `/epas/trace/epe/sdi/epe.txt` |
| Cisco SIP Proxy | `/epas/trace/esp/sdi/esp.txt` |
| Cisco Syslog Agent | `/cm/trace/syslogmib/sdi/syslogmib.txt` |
| Cisco Tomcat Security Log | `/tomcat/logs/security/log4/security*.log` |
| Cisco XCP Authentication Service | `/epas/trace/xcp/log/auth-svc-1*.log` |
| Cisco XCP Client Connection Manager | `/epas/trace/xcp/log/client-cm-1*.log` |
| Cisco XCP Config Manager | `/epas/trace/xcpconfigmgr/log4j/xcpconfigmgr.log` |
| Cisco XCP Connection Manager | `/epas/trace/xcp/log/xmpp-cm-4*.log` |
| Cisco XCP Router | `/epas/trace/xcp/log/rtr-jsm-1*.log` |
| Cisco XCP SIP Federation Connection Manager | `/epas/trace/xcp/log/sip-cm-3*.log` |
| Cisco XCP Text Conferencing Manager | `/epas/trace/xcp/log/txt-conf-1*.log` |
| Cisco XCP XMPP Federation Connection Manager | `/epas/trace/xcp/log/xmpp-cm-4*.log` |
| Cluster Manager | `/platform/log/clustermgr*` |
| Client Profile Agent (CPA) | `/tomcat/logs/epassoap/log4j/EPASSoap*.log` |

| Service | Trace Log Filename |
|---|---|
| dbmon | /cm/trace/dbl/sdi/dbmon*.txt |

# IM and Presence Service Login and Authentication Traces

If IM and Presence Service users experience issues signing into their client software, you can run traces on the IM and Presence Service node on which the user is provisioned. The following table lists the services to trace. You can view the trace log files using the Real-Time Monitoring Tool (RTMT) or using command line interface (CLI) commands such as **file list** and **file get**. Use only SFTP servers for file transfers using CLI commands such as **file get**. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

***Table 35: Traces Used to Investigate Login and Authentication Issues***

| Service | Trace Log Filename |
|---|---|
| Cisco Client Profile Agent (CPA) | /tomcat/logs/epassoap/log4j/EPASSoap*.log |
| Cisco XCP Connection Manager | /epas/trace/xcp/log/client-cm-1*.log |
| Cisco XCP Router | /epas/trace/xcp/log/rtr-jsm-1*.log |
| Cisco XCP Authentication Service | /epas/trace/xcp/logs/auth-svc-1*.log |
| Cisco Tomcat Security Logs | /tomcat/logs/security/log4/security*.log |

# Availability, IM, Contact List, and Group Chat Traces

You can run traces to troubleshoot Availability, IM, contact list, and group chat issues for your IM and Presence Service deployment.

The following table lists the recommended services to trace for commonly encountered issues.

***Table 36: Recommended Traces for Availability, IM, Contact List, and Group Chat Issues***

| Issue/Solution | Services |
|---|---|
| End user has no availability status displayed or incorrect availability status for some or all of their contacts.<br>Perform traces for the listed services on the IM and Presence Service node on which the end users and contacts are provisioned. | • Cisco XCP Connection Manager<br>• Cisco XCP Router<br>• Cisco Presence Engine |
| End user has issues with their self availability status, including on-the-phone or meeting status.<br>Perform traces for the listed services on the IM and Presence Service node on which the end user is provisioned. | • Cisco XCP Connection Manager<br>• Cisco XCP Router<br>• Cisco Presence Engine |

| Issue/Solution | Services |
|---|---|
| End user has issues sending or receiving instant messages.<br>Perform traces for the listed services on the IM and Presence Service nodes on which the sender and recipient are provisioned. | • Cisco XCP Connection Manager<br>• Cisco XCP Router |
| End user is experiencing any of the following issues:<br>• Difficulty creating or joining a chat room.<br>• Chat room messages are not being delivered to all members.<br>• Any other issues with the chat room.<br>Perform traces for the listed services on the IM and Presence Service node on which the chat room members are provisioned. | • Cisco XCP Connection Manager<br>• Cisco XCP Router<br>• Cisco XCP Text Conferencing Manager |
| The node on which the chat room that is experiencing difficulties is hosted and the node on which the creator is provisioned are not the same.<br>Perform an initial trace analysis to determine which node hosted the chat room. Then perform traces for the following services on the IM and Presence Service node that hosted the chat room. | • Cisco XCP Text Conferencing Manager<br>• Cisco XCP Router |

After the traces are complete, you can view the trace log files using the Real-Time Monitoring Tool (RTMT) or using command line interface (CLI) commands such as **file list** and **file get**. Use only SFTP servers for file transfers using CLI commands such as **file get**. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

- Cisco Presence Engine: `/epas/trace/epe/sdi/epe*.txt`
- Cisco XCP Connection Manager: `/epas/trace/xcp/log/client-cm-1*.log.gz`
- Cisco XCP Router: `/epas/trace/xcp/log/rtr-jsm-1*.log`
- Cisco XCP Text Conferencing Manager: `/epas/trace/xcp/log/txt-conf-1*.log`

# Availability and IM Traces for Partitioned Intradomain Federation MOC Contact Issues

If the local IM and Presence Service user is unable to exchange availability or instant messages with an intradomain Microsoft Office Communicator (MOC) contact, you can run traces on the IM and Presence Service node on which the local user is provisioned. The following table lists the services to trace. You can view the trace log files using the Real-Time Monitoring Tool (RTMT) or using command line interface (CLI) commands such as **file list** and **file get**. Use only SFTP servers for file transfers using CLI commands such as **file get**. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

*Table 37: Traces Used to Investigate Availability and IM Issues with Partitioned Intradomain Federation MOC Contacts*

| Services | Trace Log Filename |
|---|---|
| Cisco XCP Router | `/epas/trace/xcp/log/rtr-jsm-1*.log` |
| Cisco XCP SIP Federation Connection Manager | `/epas/trace/xcp/log/sip-cm-3*.log` |
| Cisco SIP Proxy | `/epas/trace/esp/sdi/esp.txt` |
| Cisco Presence Engine | `/epas/trace/epe/sdi/epe.txt` |

**Note** Cisco SIP Proxy debug logging is required to see the sip message exchange.

# Availability and IM Traces for XMPP-Based Interdomain Federation Contact Issues

If the local IM and Presence Service user is unable to exchange availability status or instant messages with an interdomain federation contact, you can run traces on the IM and Presence Service node on which the local user is provisioned. The following table lists the services to trace. You can view the trace log files using the Real-Time Monitoring Tool (RTMT) or using command line interface (CLI) commands such as **file list** and **file get**. Use only SFTP servers for file transfers using CLI commands such as **file get**. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

*Table 38: Traces Used to Investigate Availability and IM Issues for XMPP-based Interdomain Federation Contacts*

| Services | Trace Log Filename |
|---|---|
| Cisco XCP Connection Manager | `/epas/trace/xcp/log/client-cm-1*.log` |
| Cisco XCP Router | `/epas/trace/xcp/log/rtr-jsm-1*.log` |
| Cisco Presence Engine | `/epas/trace/epe/sdi/epe*.txt` |
| Cisco XCP XMPP Federation Connection Manager<br><br>Perform this trace on each IM and Presence Service node on which XMPP federation is enabled. | `/epas/trace/xcp/log/xmpp-cm-4*.log` |

# Availability and IM Traces for SIP-Based Interdomain Federation Contact Issues

If the local IM and Presence Service user is unable to exchange availability status or instant messages with an interdomain federation contact, you can run traces on the IM and Presence Service node on which the local user is provisioned. The following table lists the services to trace. You can view the trace log files using the Real-Time Monitoring Tool (RTMT) or using command line interface (CLI) commands such as **file list** and **file get**. Use only SFTP servers for file transfers using CLI commands such as **file get**. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

***Table 39: Traces Used to Investigate Availability and IM Issues for XMPP-based Interdomain Federation Contacts***

| Services | Trace Log Filename |
|---|---|
| Cisco XCP Connection Manager | `/epas/trace/xcp/log/xmpp-cm-4*.log` |
| Cisco XCP Router | `/epas/trace/xcp/log/rtr-jsm-1*.log` |
| Cisco Presence Engine | `/epas/trace/epe/sdi/epe.txt` |
| Cisco SIP Proxy | `/epas/trace/esp/sdi/esp.txt` |
| Cisco XCP SIP Federation Connection Manager | `/epas/trace/xcp/log/sip-cm-3*.log` |

# Calendaring Traces

You can run traces to troubleshoot calendaring issues for your IM and Presence Service deployment. The following table lists the service to trace.

After the trace is complete, you can view the resulting log file using the Real-Time Monitoring Tool (RTMT) and filter your search in the resulting Cisco Presence Engine log file. Look for instances of ".owa." and "".ews.". You can also use command line interface (CLI) commands such as **file list** and **file get** to view the log file results. Use only SFTP servers for file transfers using CLI commands such as **file get**. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*

***Table 40: Trace Used to Investigate Calendaring Issues***

| Service | Trace Log Filename |
|---|---|
| Cisco Presence Engine | `/epas/trace/epe/sdi/epe*.txt` |

# Intercluster Synchronization Traces and Inter-Clustering Troubleshooter

If an IM and Presence Service node generates alerts that indicate there are intercluster synchronization issues with another node in your deployment, you can run traces on the nodes that are not synchronizing to diagnose the issue. After the traces are complete, you can view the resulting log files using the Real-Time Monitoring Tool (RTMT) or using command line interface (CLI) commands such as **file list** and **file get**. Use only SFTP servers for file transfers using CLI commands such as **file get**. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

You can also check for synchronization errors using the Cisco Unified CM IM and Presence Administration GUI when you select **Diagnostics** > **System Troubleshooter** and navigate to **Inter-Clustering Troubleshooter**. You can capture a screen snap of the page.

The following table lists the services to trace for intercluster synchronization issues. Perform traces for the listed services on each IM and Presence Service node that is experiencing intercluster synchronization issues.

***Table 41: Traces Used to Investigate Intercluster Sycnronization Issues Between Nodes***

| Service | Trace Log Filename |
|---|---|
| Cisco Intercluster Sync Agent | `/epas/trace/epassa/log4j/icSyncAgent*.log` |
| Cisco AXL Web Service | `/tomcat/logs/axl/log4j/axl*.log` |
| Cisco Tomcat Security Log | `/tomcat/logs/security/log4j/security*.log` |
| Cisco Syslog Agent | `/cm/trace/syslogmib/sdi/syslogmib*.txt` |

# SIP Federation Traces

You can run traces to troubleshoot SIP federation issues for your IM and Presence Service deployment. The following table lists the services to trace.

After the traces are complete, you can view the resulting log files using the Real-Time Monitoring Tool (RTMT) or using command line interface (CLI) commands such as **file list** and **file get**. Use only SFTP servers for file transfers using CLI commands such as **file get**. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

***Table 42: Traces Used to Investigate Login and Authentication Issues***

| Service | Trace Log Filename |
|---|---|
| Cisco SIP Proxy | `/epas/trace/esp/sdi/esp*.txt` |
| Cisco XCP Router | `/epas/trace/xcp/log/rtr-jsm-1*.log` |

| Service | Trace Log Filename |
|---|---|
| Cisco XCP SIP Federation Connection Manager | /epas/trace/xcp/log/sip-cm-3*.log |

# XMPP Federation Traces

You can run traces to troubleshoot XMPP federation issues on your IM and Presence Service deployment. The following table lists the services to trace.

After the traces are complete, you can view the resulting log files using the Real-Time Monitoring Tool (RTMT) or using command line interface (CLI) commands such as **file list** and **file get**. Use only SFTP servers for file transfers using CLI commands such as **file get**. For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands to access trace log files, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

***Table 43: Traces Used to Investigate XMPP Federation Issues***

| Service | Trace Log Filename |
|---|---|
| Cisco XCP Router | /epas/trace/xcp/log/rtr-jsm-1*.log |
| Cisco XCP XMPP Federation Connection Manager | /epas/trace/xcp/log/xmpp-cm-4*.log |

# High CPU and Low VM Alert Troubleshooting

If an IM and Presence Service node is generating high CPU or low VM availability alerts, you can collect information from the node using the Command Line Interface (CLI) to help troubleshoot the cause. You can also run traces on related services on the node, and then view the resulting log files using the Real-Time Monitoring Tool (RTMT). For more information about installing and using the RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. For information about using CLI commands, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

You can also setup Cisco Unified IM and Presence Serviceability alarms to provide information about runtime status and the state of the system to local system logs. IM and Presence Service writes system errors in the Application Logs that you view using the SysLog Viewer in RTMT. For more information about setting up syslog alarms for a service, see the *Cisco Unified Serviceability Administration Guide*. For information about viewing alarm information using the SysLog Viewer, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

***Table 44: CLI Commands Used to Investigate High CPU and Low VM Alerts***

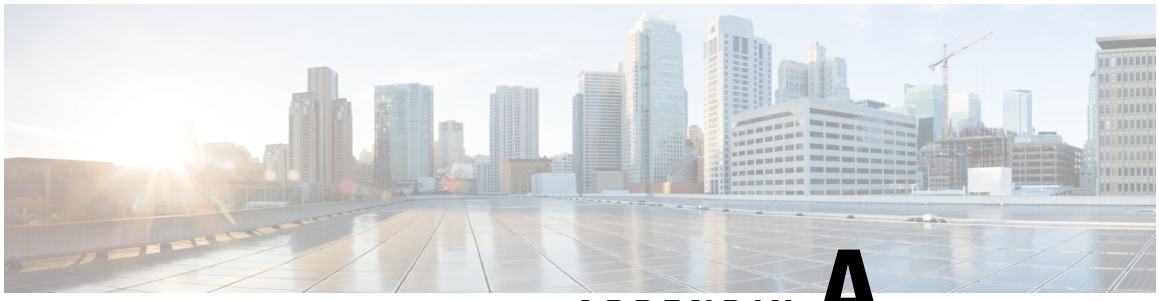
| Solution | CLI Command |
|---|---|
| Use the CLI to run the following commands on the node. | show process using-most cpu<br>show process using-most memory<br>utils dbreplication runtimestate<br>utils service list |

| Solution | CLI Command |
|---|---|
| Use the CLI to collect all RIS (Real-time Information Service) performance logs for the node. Use only SFTP servers for file transfers using **file get**. | `file get activelog cm/log/ris/csv` |

The following table lists the services to select when you run traces on the IM and Presence Service node to investigate high CPU and low VM alerts. Perform traces for the listed services on the IM and Presence Service node that is generating high CPU or low VM alerts.

***Table 45: Traces Used to Investigate High CPU and Low VM Alerts***

| Services | Trace Log Filename |
|---|---|
| Cisco XCP Router | `/epas/trace/xcp/log/rtr-jsm-1*.log` |
| Cisco XCP SIP Federation Connection Manager | `/epas/trace/xcp/log/sip-cm-3*.log` |
| Cisco SIP Proxy | `/epas/trace/esp/sdi/esp*.txt` |
| Cisco Presence Engine | `/epas/trace/epe/sdi/epe*.txt` |
| Cisco Tomcat Security Log | `/tomcat/logs/security/log4/security*.log` |
| Cisco Syslog Agent | `/cm/trace/syslogmib/sdi/syslogmib*.txt` |



APPENDIX A

# High Availability Client Login Profiles


- High Availability Login Profiles, on page 259
- Single Cluster Configuration, on page 261


# High Availability Login Profiles

## Important Notes About High Availability Login Profiles

- You can use the High Availability login profile tables in this section to configure the upper and lower client re-login values for your presence redundancy group. You configure the upper and lower client login values by choosing **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters**, and choosing **Cisco Server Recovery Manager** from the Service menu.
- By configuring the upper and lower client re-login limits on your presence redundancy group based on the tables we provide here, you can avoid performance issues and high CPU spikes in your deployment.
- We provide a High Availability login profile for each IM and Presence Service node memory size, and for each High Availability deployment type, active/active or active/standby.
- The High Availability login profile tables are calculated based on the following inputs:
    - The lower client re-login limit is based on the Server Recovery Manager service parameter "Critical Service Down Delay", for which the default is 90 seconds. If the Critical Service Down Delay is changed then the lower limit must also change.
    - The total number of users in the presence redundancy group for Active/Standby deployments, or the node with highest number of users for Active/Active deployments.
- You must configure the upper and lower client re-login limit values on both nodes in a presence redundancy group. You must manually configure all these values on both nodes in the presence redundancy group.
- The upper and lower client re-login limit values must be the same on each node in the presence redundancy group.
- If you **rebalance** your users, you must reconfigure the upper and lower client re-login limit values based on the High Availability login profile tables.

# Use High Availability Login Profile Tables

Use the High Availability login profile tables to retrieve the following values:

- **Client Re-Login Lower Limit** service parameter value
- **Client Re-Login Upper Limit** service parameter value.

### Procedure

**Step 1** Choose a profile table based on your virtual hardware configuration, and your High Availability deployment type.

**Step 2** In the profile table, choose the number of users in your deployment (round up to the nearest value). If you have an active/standby deployment, use the node with the highest number of users.

**Step 3** Based on the Number of Users value for your presence redundancy group, retrieve the corresponding lower and upper retry limits in the profile table.

**Step 4** Configure the lower and upper retry limits on IM and Presence Service by choosing **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters**, and choosing **Cisco Server Recovery Manager** from the Service menu.

**Step 5** Check the Critical Service Down Delay value by choosing **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters** and choosing **Cisco Server Recovery Manager** from the **Service** Menu. The default value is 90 seconds. The lower retry limit should be set to this value.

# Example High Availability Login Configurations

### Example 1: 15000 Users Full UC Profile - active/active deployment

You have 3000 users in your presence redundancy group, with 2000 users on one node, and 1000 users on the second node. For an unbalanced active/active deployment, Cisco recommends you use the node with the highest number of users, in this case the node with 2000 users. Using the 15000 users full US (4 vCPU 8GB) active/active profile, you retrieve these lower and upper retry values:

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| 2000 | 120 | 253 |

**Note** The upper retry limit is the approximate time (seconds) it takes for all clients to login to their backup node after a failover occurs.

**Note** The lower limit of 120 assumes the **Critical Service Down Delay** service parameter is set to 120.

#### Example 2: 5000 Users Full UC Profile - active/active deployment

You have 4700 users on each node in your presence redundancy group  in an IM-only deployment. Cisco recommends that you round up to the nearest value, so using the 5000 users full US (4 vCPU 8GB) active/active profile you retrieve the lower and upper retry value based on a number of users value of 5000:

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| 5000 | 120 | 953 |

# Single Cluster Configuration

## 500 Users Full UC (1vCPU 700MHz 2GB) Active/Active Profile

*Table 46: User Login Retry Limits for Standard Deployment (500 Users Full UC Active/Active)*

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| **Full UC** | | |
| 100 | 120 | 187 |
| 250 (default) | 120 | 287 |
| **IM only** | | |
| 500 | 120 | 453 |

## 500 Users Full UC (1vCPU 700MHz 2GB) Active/Standby Profile

*Table 47: User Login Retry Limits for Standard Deployment (500 Users Full UC Active/Standby)*

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| **Full UC** | | |
| 100 | 120 | 187 |
| 250 (default) | 120 | 287 |
| 500 | 120 | 453 |
| **IM only** | | |
| 750 | 120 | 620 |
| 1000 | 120 | 787 |

# 1000 Users Full UC (1vCPU 1500MHz 2GB) Active/Active Profile

*Table 48: User Login Retry Limits for Standard Deployment (1000 Users Full UC Active/Active)*

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| **Full UC** | | |
| 100 | 120 | 153 |
| 250 | 120 | 203 |
| 500 (default) | 120 | 287 |
| **IM only** | | |
| 750 | 120 | 370 |
| 1000 | 120 | 453 |

# 1000 Users Full UC (1vCPU 1500MHz 2GB) Active/Standby Profile

*Table 49: User Login Retry Limits for Standard Deployment (1000 Users Full UC Active/Standby)*

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| **Full UC** | | |
| 100 | 120 | 153 |
| 250 | 120 | 203 |
| 500 (default) | 120 | 287 |
| 750 | 120 | 370 |
| 1000 | 120 | 453 |
| **IM only** | | |
| 1250 | 120 | 537 |
| 1500 | 120 | 620 |
| 1750 | 120 | 703 |
| 2000 | 120 | 787 |

# 2000 Users Full UC (1vCPU 1500Mhz 4GB) Active/Active Profile

*Table 50: User Login Retry Limits for Standard Deployment (2000 Users Full UC Active/Active)*

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| **Full UC** | | |
| 100 | 120 | 153 |
| 500 (default) | 120 | 287 |
| 1000 | 120 | 453 |

# 2000 Users Full UC (1vCPU 1500Mhz 4GB) Active/Standby Profile

*Table 51: User Login Retry Limits for Standard Deployment (2000 Users Full UC Active/Standby)*

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| **Full UC** | | |
| 100 | 120 | 153 |
| 250 | 120 | 203 |
| 500 (default) | 120 | 287 |
| 750 | 120 | 370 |
| 1000 | 120 | 453 |
| 1250 | 120 | 537 |
| 1500 | 120 | 620 |
| 1750 | 120 | 703 |
| 2000 | 120 | 787 |

# 5000 Users Full UC (4 GB 2vCPU) Active/Active Profile

*Table 52: User Login Retry Limits for Standard Deployment (5000 Users Full UC Active/Active)*

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| **Full UC** | | |
| 100 | 120 | 137 |
| 500 | 120 | 203 |
| 1000 | 120 | 287 |

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| 1500 | 120 | 370 |
| 2000 | 120 | 453 |
| 2500 (default) | 120 | 537 |
| **IM only** | | |
| 3000 | 120 | 620 |
| 3500 | 120 | 703 |
| 4000 | 120 | 787 |
| 4500 | 120 | 870 |
| 5000 | 120 | 953 |
| 6000 | 120 | 1120 |
| 6250 | 120 | 1162 |

# 5000 Users Full UC (4 GB 2vCPU) Active/Standby Profile

*Table 53: User Login Retry Limits for Standard Deployment (5000 Users Full UC Active/Standby)*

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| **Full UC** | | |
| 100 | 120 | 137 |
| 500 | 120 | 203 |
| 1000 | 120 | 287 |
| 1500 | 120 | 370 |
| 2000 | 120 | 453 |
| 2500 (default) | 120 | 537 |
| 3000 | 120 | 620 |
| 3500 | 120 | 703 |
| 4000 | 120 | 787 |
| 4500 | 120 | 870 |
| 5000 | 120 | 953 |
| **IM only** | | |

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| 6000 | 120 | 1120 |
| 7000 | 120 | 1287 |
| 8000 | 120 | 1453 |
| 9000 | 120 | 1620 |
| 10000 | 120 | 1787 |
| 11000 | 120 | 1953 |
| 12000 | 120 | 2120 |
| 12500 | 120 | 2203 |

# 15000 Users Full UC (4 vCPU 8GB) Active/Active Profile

**Attention** To achieve maximum client login throughput on a 15000 user system, Cisco recommends a minimum of 2.5GHz CPU clock speed.

*Table 54: User Login Retry Limits for Standard Deployment (15000 Users Full UC Active/Active)*

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| **Full UC** | | |
| 100 | 120 | 127 |
| 500 | 120 | 153 |
| 1000 | 120 | 187 |
| 1500 | 120 | 220 |
| 2000 | 120 | 253 |
| 2500 | 120 | 287 |
| 3000 | 120 | 320 |
| 3500 | 120 | 353 |
| 4000 | 120 | 387 |
| 4500 | 120 | 420 |
| 5000 (default) | 120 | 453 |
| 6000 | 120 | 520 |
| 7000 | 120 | 587 |

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| 7500 | 120 | 620 |
| **IM only** | | |
| 8000 | 120 | 653 |
| 9000 | 120 | 720 |
| 10000 | 120 | 787 |
| 11000 | 120 | 853 |
| 12000 | 120 | 920 |
| 12500 | 120 | 953 |

# 15000 Users Full UC (4 vCPU 8GB) Active/Standby Profile

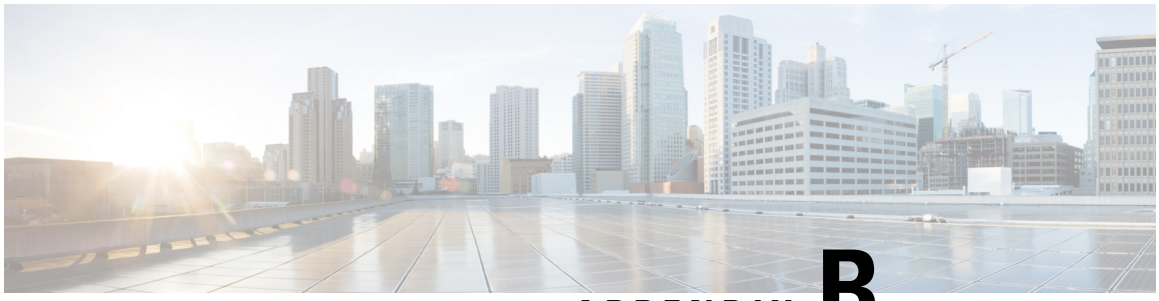
**Attention** To achieve maximum client login throughput on a 15000 user system, Cisco recommends a minimum of 2.5GHz CPU clock speed.

*Table 55: User Login Retry Limits for Standard Deployment (15000 Users Full UC Active/Standby)*

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| **Full UC** | | |
| 100 | 120 | 127 |
| 500 | 120 | 153 |
| 1000 | 120 | 187 |
| 1500 | 120 | 220 |
| 2000 | 120 | 253 |
| 2500 | 120 | 287 |
| 3000 | 120 | 320 |
| 3500 | 120 | 353 |
| 4000 | 120 | 387 |
| 4500 | 120 | 420 |
| 5000 (default) | 120 | 453 |
| 6000 | 120 | 520 |
| 7000 | 120 | 587 |

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| 8000 | 120 | 653 |
| 9000 | 120 | 720 |
| 10000 | 120 | 787 |
| 11000 | 120 | 853 |
| 12000 | 120 | 920 |
| 13000 | 120 | 987 |
| 14000 | 120 | 1053 |
| 15000 | 120 | 1120 |
| **IM only** | | |
| 16000 | 120 | 1187 |
| 17000 | 120 | 1253 |
| 18000 | 120 | 1320 |
| 19000 | 120 | 1387 |
| 20000 | 120 | 1453 |
| 21000 | 120 | 1520 |
| 22000 | 120 | 1587 |
| 23000 | 120 | 1653 |
| 24000 | 120 | 1720 |
| 25000 | 120 | 1787 |

High Availability Client Login Profiles



APPENDIX B

# Additional Requirements


- High Availability Login Profiles, on page 269
- Single Cluster Configuration, on page 271
- XMPP Standards Compliance, on page 277


# High Availability Login Profiles

## Important Notes About High Availability Login Profiles

- You can use the High Availability login profile tables in this section to configure the upper and lower client re-login values for your presence redundancy group. You configure the upper and lower client login values by choosing **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters**, and choosing **Cisco Server Recovery Manager** from the Service menu.
- By configuring the upper and lower client re-login limits on your presence redundancy group based on the tables we provide here, you can avoid performance issues and high CPU spikes in your deployment.
- We provide a High Availability login profile for each IM and Presence Service node memory size, and for each High Availability deployment type, active/active or active/standby.
- The High Availability login profile tables are calculated based on the following inputs:
  - The lower client re-login limit is based on the Server Recovery Manager service parameter "Critical Service Down Delay", for which the default is 90 seconds. If the Critical Service Down Delay is changed then the lower limit must also change.
  - The total number of users in the presence redundancy group for Active/Standby deployments, or the node with highest number of users for Active/Active deployments.
- You must configure the upper and lower client re-login limit values on both nodes in a presence redundancy group. You must manually configure all these values on both nodes in the presence redundancy group.
- The upper and lower client re-login limit values must be the same on each node in the presence redundancy group.
- If you **rebalance** your users, you must reconfigure the upper and lower client re-login limit values based on the High Availability login profile tables.

# Use High Availability Login Profile Tables

Use the High Availability login profile tables to retrieve the following values:

- **Client Re-Login Lower Limit** service parameter value
- **Client Re-Login Upper Limit** service parameter value.

### Procedure

**Step 1** Choose a profile table based on your virtual hardware configuration, and your High Availability deployment type.

**Step 2** In the profile table, choose the number of users in your deployment (round up to the nearest value). If you have an active/standby deployment, use the node with the highest number of users.

**Step 3** Based on the Number of Users value for your presence redundancy group, retrieve the corresponding lower and upper retry limits in the profile table.

**Step 4** Configure the lower and upper retry limits on IM and Presence Service by choosing **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters**, and choosing **Cisco Server Recovery Manager** from the Service menu.

**Step 5** Check the Critical Service Down Delay value by choosing **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters** and choosing **Cisco Server Recovery Manager** from the **Service** Menu. The default value is 90 seconds. The lower retry limit should be set to this value.

# Example High Availability Login Configurations

### Example 1: 15000 Users Full UC Profile - active/active deployment

You have 3000 users in your presence redundancy group, with 2000 users on one node, and 1000 users on the second node. For an unbalanced active/active deployment, Cisco recommends you use the node with the highest number of users, in this case the node with 2000 users. Using the 15000 users full US (4 vCPU 8GB) active/active profile, you retrieve these lower and upper retry values:

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| 2000 | 120 | 253 |

**Note** The upper retry limit is the approximate time (seconds) it takes for all clients to login to their backup node after a failover occurs.

**Note** The lower limit of 120 assumes the **Critical Service Down Delay** service parameter is set to 120.

#### Example 2: 5000 Users Full UC Profile - active/active deployment

You have 4700 users on each node in your presence redundancy group  in an IM-only deployment. Cisco recommends that you round up to the nearest value, so using the 5000 users full US (4 vCPU 8GB) active/active profile you retrieve the lower and upper retry value based on a number of users value of 5000:

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| 5000 | 120 | 953 |

# Single Cluster Configuration

## 500 Users Full UC (1vCPU 700MHz 2GB) Active/Active Profile

*Table 56: User Login Retry Limits for Standard Deployment (500 Users Full UC Active/Active)*

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| **Full UC** | | |
| 100 | 120 | 187 |
| 250 (default) | 120 | 287 |
| **IM only** | | |
| 500 | 120 | 453 |

## 500 Users Full UC (1vCPU 700MHz 2GB) Active/Standby Profile

*Table 57: User Login Retry Limits for Standard Deployment (500 Users Full UC Active/Standby)*

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| **Full UC** | | |
| 100 | 120 | 187 |
| 250 (default) | 120 | 287 |
| 500 | 120 | 453 |
| **IM only** | | |
| 750 | 120 | 620 |
| 1000 | 120 | 787 |

# 1000 Users Full UC (1vCPU 1500MHz 2GB) Active/Active Profile

*Table 58: User Login Retry Limits for Standard Deployment (1000 Users Full UC Active/Active)*

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| **Full UC** | | |
| 100 | 120 | 153 |
| 250 | 120 | 203 |
| 500 (default) | 120 | 287 |
| **IM only** | | |
| 750 | 120 | 370 |
| 1000 | 120 | 453 |

# 1000 Users Full UC (1vCPU 1500MHz 2GB) Active/Standby Profile

*Table 59: User Login Retry Limits for Standard Deployment (1000 Users Full UC Active/Standby)*

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| **Full UC** | | |
| 100 | 120 | 153 |
| 250 | 120 | 203 |
| 500 (default) | 120 | 287 |
| 750 | 120 | 370 |
| 1000 | 120 | 453 |
| **IM only** | | |
| 1250 | 120 | 537 |
| 1500 | 120 | 620 |
| 1750 | 120 | 703 |
| 2000 | 120 | 787 |

# 2000 Users Full UC (1vCPU 1500Mhz 4GB) Active/Active Profile

*Table 60: User Login Retry Limits for Standard Deployment (2000 Users Full UC Active/Active)*

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| **Full UC** | | |
| 100 | 120 | 153 |
| 500 (default) | 120 | 287 |
| 1000 | 120 | 453 |

# 2000 Users Full UC (1vCPU 1500Mhz 4GB) Active/Standby Profile

*Table 61: User Login Retry Limits for Standard Deployment (2000 Users Full UC Active/Standby)*

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| **Full UC** | | |
| 100 | 120 | 153 |
| 250 | 120 | 203 |
| 500 (default) | 120 | 287 |
| 750 | 120 | 370 |
| 1000 | 120 | 453 |
| 1250 | 120 | 537 |
| 1500 | 120 | 620 |
| 1750 | 120 | 703 |
| 2000 | 120 | 787 |

# 5000 Users Full UC (4 GB 2vCPU) Active/Active Profile

*Table 62: User Login Retry Limits for Standard Deployment (5000 Users Full UC Active/Active)*

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| **Full UC** | | |
| 100 | 120 | 137 |
| 500 | 120 | 203 |
| 1000 | 120 | 287 |

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| 1500 | 120 | 370 |
| 2000 | 120 | 453 |
| 2500 (default) | 120 | 537 |
| **IM only** | | |
| 3000 | 120 | 620 |
| 3500 | 120 | 703 |
| 4000 | 120 | 787 |
| 4500 | 120 | 870 |
| 5000 | 120 | 953 |
| 6000 | 120 | 1120 |
| 6250 | 120 | 1162 |

# 5000 Users Full UC (4 GB 2vCPU) Active/Standby Profile

*Table 63: User Login Retry Limits for Standard Deployment (5000 Users Full UC Active/Standby)*

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| **Full UC** | | |
| 100 | 120 | 137 |
| 500 | 120 | 203 |
| 1000 | 120 | 287 |
| 1500 | 120 | 370 |
| 2000 | 120 | 453 |
| 2500 (default) | 120 | 537 |
| 3000 | 120 | 620 |
| 3500 | 120 | 703 |
| 4000 | 120 | 787 |
| 4500 | 120 | 870 |
| 5000 | 120 | 953 |
| **IM only** | | |

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| 6000 | 120 | 1120 |
| 7000 | 120 | 1287 |
| 8000 | 120 | 1453 |
| 9000 | 120 | 1620 |
| 10000 | 120 | 1787 |
| 11000 | 120 | 1953 |
| 12000 | 120 | 2120 |
| 12500 | 120 | 2203 |

# 15000 Users Full UC (4 vCPU 8GB) Active/Active Profile

**Attention** To achieve maximum client login throughput on a 15000 user system, Cisco recommends a minimum of 2.5GHz CPU clock speed.

*Table 64: User Login Retry Limits for Standard Deployment (15000 Users Full UC Active/Active)*

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| **Full UC** | | |
| 100 | 120 | 127 |
| 500 | 120 | 153 |
| 1000 | 120 | 187 |
| 1500 | 120 | 220 |
| 2000 | 120 | 253 |
| 2500 | 120 | 287 |
| 3000 | 120 | 320 |
| 3500 | 120 | 353 |
| 4000 | 120 | 387 |
| 4500 | 120 | 420 |
| 5000 (default) | 120 | 453 |
| 6000 | 120 | 520 |
| 7000 | 120 | 587 |

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| 7500 | 120 | 620 |
| **IM only** | | |
| 8000 | 120 | 653 |
| 9000 | 120 | 720 |
| 10000 | 120 | 787 |
| 11000 | 120 | 853 |
| 12000 | 120 | 920 |
| 12500 | 120 | 953 |

# 15000 Users Full UC (4 vCPU 8GB) Active/Standby Profile

**Attention** To achieve maximum client login throughput on a 15000 user system, Cisco recommends a minimum of 2.5GHz CPU clock speed.

*Table 65: User Login Retry Limits for Standard Deployment (15000 Users Full UC Active/Standby)*

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| **Full UC** | | |
| 100 | 120 | 127 |
| 500 | 120 | 153 |
| 1000 | 120 | 187 |
| 1500 | 120 | 220 |
| 2000 | 120 | 253 |
| 2500 | 120 | 287 |
| 3000 | 120 | 320 |
| 3500 | 120 | 353 |
| 4000 | 120 | 387 |
| 4500 | 120 | 420 |
| 5000 (default) | 120 | 453 |
| 6000 | 120 | 520 |
| 7000 | 120 | 587 |

| Expected Number of Active Users | Lower Retry Limit | Upper Retry Limit |
|---|---|---|
| 8000 | 120 | 653 |
| 9000 | 120 | 720 |
| 10000 | 120 | 787 |
| 11000 | 120 | 853 |
| 12000 | 120 | 920 |
| 13000 | 120 | 987 |
| 14000 | 120 | 1053 |
| 15000 | 120 | 1120 |
| **IM only** | | |
| 16000 | 120 | 1187 |
| 17000 | 120 | 1253 |
| 18000 | 120 | 1320 |
| 19000 | 120 | 1387 |
| 20000 | 120 | 1453 |
| 21000 | 120 | 1520 |
| 22000 | 120 | 1587 |
| 23000 | 120 | 1653 |
| 24000 | 120 | 1720 |
| 25000 | 120 | 1787 |

# XMPP Standards Compliance

The IM and Presence Service is compliant with the following XMPP standards:

- RFC 3920 Extensible Messaging and Presence Protocol (XMPP): Core RFC 3921 Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence
  - XEP-0004 Data Forms
  - XEP-0012 Last Activity
  - XEP-0013 Flexible Offline Message Retrieval
  - XEP-0016 Privacy Lists
  - XEP-0030 Service Discovery

- XEP-0045 Multi-User Chat
- XEP-0054 Vcard-temp
- XEP-0055 Jabber Search
- XEP-0060 Publish-Subscribe
- XEP-0065 SOCKS5 Bystreams
- XEP-0066 Out of Band Data Archive OOB requests
- XEP-0068 Field Standardization for Data Forms
- XEP-0071 XHTML-IM
- XEP-0082 XMPP Date and Time Profiles
- XEP-0092 Software Version
- XEP-0106 JID Escaping
- XEP-0114 Jabber Component Protocol
- XEP-0115 Entity Capabilities
- XEP-0124 Bidirectional Streams over Synchronous HTTP (BOSH)
- XEP-0126 Invisibility
- XEP-0128 Service Discovery Extensions
- XEP-0160 Best Practices for Handling Offline Messages
- XEP-0163 Personal Eventing Via PubSub
- XEP-0170 Recommended Order of Stream Feature Negotiation
- XEP-0178 Best Practices for Use of SASL EXTERNAL
- XEP-0220 Server Dialback
- XEP-0273 SIFT (Stanza Interception and Filtering Technology)