Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager, Release 9.0(1)

First Published: April 09, 2014

Last Modified: August 22, 2014

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.

CONTENTS

PART I **Deployment Planning** 1

CHAPTER 1 **IM and Presence Service Features and Functions** 3

IM and Presence Service Components 4

Main Components 4

SIP Interface 4

AXL/SOAP Interface 5

LDAP Interface 5

XMPP Interface 6

CTI interface 6

Deployment models 6

IM-Only Deployment 6

High Availability Deployments 6

Multinode Deployment Models 7

Subclusters 7

Balanced User Assignment Redundant High Availability Deployment 7

Active/Standby User Assignment Redundant High Availability Deployment 8

Clustering Over WAN 9

User Assignment 10

End User Management 10

Availability and Instant Messaging 10

Chat 10

IM Forking 11

Offline IM 11

Broadcast IM 11

Chat Rooms on IM and Presence Service 11

Chat Room Limits 12

File Transfer 12

Important Notes About IM and Presence Service and Chat 12
IM Compliance 13
LDAP Integrations 13
Third-Party Integrations 13
Third-Party Client Integration 15
Supported Third-Party XMPP Clients 15
License Requirements for Third-Party Clients 15
XMPP Client Integration on Cisco Unified Communications Manager 15
LDAP Integration for XMPP Contact Search 15
Verify Domain Name for XMPP Clients 16
DNS Configuration for XMPP Clients 16
Security 16
Single Sign-On 16

CHAPTER 2 Multinode Scalability and WAN Deployments 17
Multinode Scalability Feature 17
Multinode Scalability Requirements 17
Scalability Options for Deployment 18
Cluster-Wide DNS SRV 19
Local Failover 19
Subcluster Failure Detection 19
Method Event Routing 20
External Database Recommendations 20
Clustering Over WAN for Intracluster and Intercluster Deployments 20
Intracluster Deployments Over WAN 20
Multinode Configuration for Deployment Over WAN 21
Intercluster Deployments 21
Intercluster Deployments Over WAN 21
Intercluster Peer Relationships 21
Intercluster Router to Router Connections 22
Node Name Value for Intercluster Deployments 22
Default Domain Value for Intercluster Deployments 23
Secure Intercluster Router to Router Connection 23

CHAPTER 3 IM and Presence Service Planning Requirements 25

Multinode Hardware Recommendations 25
Intercluster Hardware Recommendations 26
Supported End Points 26
LDAP Directory Servers Supported 27
WAN Bandwidth Requirements 27
WAN Bandwidth Considerations 27
Multinode Scalability and Performance 28
Multinode Scalability Requirements 28
Multinode Performance Recommendations 28
User License Requirements 29

CHAPTER 4 Workflows 31
Basic Deployment with High Availability Workflow 31
Basic Deployment with High Availability and IP Phone Presence Workflow 34
Federation Deployment Workflow 36
IM-Only Deployment Workflow 39

PART II System Configuration 41

CHAPTER 5 IM and Presence Service Multinode Deployment Configuration 43
Cisco Replication Watcher Service 43
Multinode Update Configuration After Deployment 44
Add New Node 44
Expand Cluster 45
Remove Node 45
Multinode Deployment Troubleshooting 46
Monitor Multinode System 46
Resolve Hardware Problem 47

CHAPTER 6 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 50
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
Verify Required Services Are Running on Cisco Unified Communications Manager 54

CHAPTER 7 IM and Presence Service Network Setup 55
Configuration changes and service restart notifications 55
Service Restart Notifications 55
Cisco XCP Router Restart 55
Restart Cisco XCP Router Service 56
Domain Value Configuration 56
Routing Information Configuration on IM and Presence Service 57
Routing Communication Recommendations 57
Configure MDNS Routing and Cluster ID 58
Configure Routing Communication 58
Configure Cluster ID 59
Configure Throttling Rate for Availability State Change Messages 60
Configure Proxy Server Settings 60
Services on IM and Presence Service 61
Configure Sync Agent Settings 61
Turn On Services for IM and Presence Service 61

CHAPTER 8 Cluster Topology Configuration of Subclusters, Nodes, and Users 63
Cluster Topology Configuration on IM and Presence Service 63
Subcluster, Node and User Management Recommendations 63
Node Creation and Movement Recommendations 63
Node Name Recommendations 64
User Assignment Mode Recommendations 65
Manual User Assignment Recommendations 65
User Redistribution 66
Create Subclusters in System Topology 67
Manage Nodes in System Topology 67
Configure User Assignment in System Topology 69

CHAPTER 9 High Availability Deployment Configuration 71
High Availability Deployments 71

High Availability Requirements 71
High Availability Subcluster 71
Failover Impact to Clients and Services 72
Automatic Failover Detection 72
Automatic Fallback 73
Cisco Server Recovery Manager (SRM) 74
Manual Failover and Fallback 74
High Availability and Intercluster Deployment Consideration 75
Turn On or Off High Availability for Subcluster 75
Configure Advanced Service Parameters for Server Recovery Manager 77
Perform Manual Failover to Backup Node 79
Perform Manual Fallback to Primary Node 80
Perform Manual Recovery of Subcluster 81

CHAPTER 10 IP Phone Presence Setup 83
Static Route Configuration on IM and Presence Service 83
Route Embed Templates 83
Configure Route Embed Templates on IM and Presence Service 84
Configure Static Routes on IM and Presence Service 85
Presence Gateway Configuration on IM and Presence Service 88
Presence Gateway Configuration Option 88
Configure Presence Gateway 88
Configure SIP Publish Trunk on IM and Presence Service 89
Configure Cluster-Wide DNS SRV Name for SIP Publish Trunk 89

CHAPTER 11 LDAP Directory Integration 91
LDAP Server Name, Address, and Profile Configuration 91
LDAP Directory Integration with Cisco Unified Communications Manager Task List 91
Secure Connection Between Cisco Unified Communications Manager and LDAP Directory 92
Configure LDAP Synchronization for User Provisioning 93
Upload LDAP Authentication Server Certificates 94
Configure LDAP Authentication 94
Configure Secure Connection Between IM and Presence Service and LDAP Directory 95
LDAP Directory Integration for Contact Searches on XMPP Clients 96

LDAP Account Lock Issue 97
Configure LDAP Server Names and Addresses for XMPP Clients 97
Configure LDAP Search Settings for XMPP Clients 98
Turn On Cisco XCP Directory Service 100

CHAPTER 12 Security Configuration on IM and Presence Service 101
Security Setup Task List 101
Create Login Banner 102
IM and Presence Service Certificate Types 103
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 105
Restart SIP Proxy Service 105
Download Certificate from IM and Presence Service 106
Upload IM and Presence Service Certificate to Cisco Unified Communications Manager 106
Restart Cisco Unified Communications Manager Service 106
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 107
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 109
Restart Cisco Tomcat Service 110
Verify Intercluster Syncing 110
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 112
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 118
SIP Security Settings Configuration on IM and Presence Service 119
Configure TLS Peer Subject 119
Configure TLS Context 119
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 121
Turn On IM and Presence Service Services to Support XMPP Clients 122

CHAPTER 13 **Intercluster Peer Configuration** 123
Prerequisites for Intercluster Deployment 123
Intercluster Peer Configuration 124
Configure Intercluster Peer 124
Turn On Intercluster Sync Agent 125
Verify Intercluster Peer Status 126
Update Intercluster Sync Agent Tomcat Trust Certificates 127

PART III **Feature Configuration** 129

CHAPTER 14 **Availability and Instant Messaging on IM and Presence Service Configuration** 131
Availability Setup on IM and Presence Service 131
Turn On or Off Availability Sharing for IM and Presence Service Cluster 131
Configure Ad-Hoc Presence Subscription Settings 132
Configure Maximum Contact List Size Per User 132
Configure Maximum Number of Watchers Per User 133
IM Setup On IM and Presence Service 134
Turn On or Off Instant Messaging for IM and Presence Service Cluster 134
Turn On or Off Offline Instant Messaging 134

Allow Clients to Log Instant Message History 135
Allow Cut and Paste in Instant Messages 136

CHAPTER 15 Single Sign-On Setup 137
Single Sign-On Setup Task List 138
Single Sign-On Setup Preparation 140
Third-Party Software and System Requirements for Single Sign-On 140
Important Information Before Single Sign-On Setup 141
Single Sign-On Setup and Management Tasks 142
Provision Active Directory for Single Sign-On 142
Client Browser Setup for Single Sign-On 143
Configure Internet Explorer for Single Sign-On 143
Configure Firefox for Single Sign-On 145
Configure Windows Registry for the Real-Time Monitoring Tool 145
Install Java 146
Import IM and Presence Certificates Into OpenAM 149
Install Tomcat 151
Deploy OpenAM War On Apache Tomcat 154
Set Up OpenAM Using GUI Configurator 155
Set Up Policies On OpenAM Server 156
Set Up SSO Module Instance 158
Set Up J2EE Agent Profile On OpenAM Server 159
Set OpenAM Session Timeout 161
Import OpenAM Certificate Into IM and Presence Service 162
Activate Single Sign-On 163
Configure Access Permissions Before Enable SSO 164
Enable Single Sign-On Using GUI 166
Deactivate Single Sign-On 167
Configure Access Permissions Before Disable SSO 167
Disable Single Sign-On 169
Uninstall OpenAM on Windows 169
Set Debug Level 170

PART IV Administration 171

CHAPTER 16 Chat Setup and Management 173

Chat Deployments 173

Chat Deployment Scenario 1 173

Chat Deployment Scenario 2 173

Chat Deployment Scenario 3 174

Chat Deployment Scenario 4 175

Chat Deployment Scenario 5 175

Chat Administration Settings 176

Change IM Gateway Settings 176

Enable File Transfer 177

Limit Number Of Sign-In Sessions 177

Chat Node Alias Management 178

Chat Node Aliases 178

Key Considerations 179

Turn On or Off System-Generated Chat Node Aliases 179

Manage Chat Node Aliases Manually 180

Turn on Cisco XCP Text Conference Manager 182

CHAPTER 17 End User Setup and Handling 183

End User Handling on IM and Presence Service 183

Authorization Policy Setup On IM and Presence Service 183

Automatic Authorization On IM and Presence Service 183

User Policy and Automatic Authorization 184

Configure Authorization Policy on IM and Presence Service 185

Bulk Export User Contact Lists 186

Bulk Import Of User Contact Lists 187

Check Maximum Contact List Size 189

Upload Input File Using BAT 189

Create New Bulk Administration Job 190

Check Results of Bulk Administration Job 190

CHAPTER 18 User Migration 193

User Migration Between IM and Presence Service Clusters 193

Unassign Users From Current Cluster 194

Export User Contact Lists 194
Disable Users for IM and Presence Service 195
Move Users to New Cluster 196
LDAP Sync Enabled on Cisco Unified Communications Manager 196
Move Users To New Organizational Unit 196
Synchronize Users To New Home Cluster 196
LDAP Sync Not Enabled On Cisco Unified Communications Manager 197
Enable Users For IM and Presence Service On New Cluster 197
Import Contact Lists On Home Cluster 197

CHAPTER 19 Multilingual Support Configuration For IM and Presence Service 199
Install Locale Installer on IM and Presence Service 199
Error Messages 201
Localized Applications 203

PART V Troubleshooting IM and Presence Service 207

CHAPTER 20 Troubleshooting High Availability 209
Node State Definitions 209
Node States, Causes and Recommended Actions 210

CHAPTER 21 Troubleshooting Single Sign-On 217
Security Trust Error Message 217
"Invalid Profile Credentials" Message 218
"Module Name Is Invalid" Message 218
"Invalid OpenAM Access Manager (Openam) Server URL" Message 218
Web Browser Indicates a 401 Error 219
Web Browser Indicates a 403 Error or Displays a Blank Screen 219
"User is not Authorized to Perform this Function" Error 219
Web Browser Indicates an HTTP 404 Error 219
Web Browser Indicates an HTTP 500 Error or Displays a Blank Screen 220
"Authentication Failed" Message 220
Web Browser Displays OpenAM Login Screen 221
Web Browser Displays IM and Presence Service Login Screen 221
Internet Explorer Prompts for Username and Password 221

"User has no profile on this organization" Message 222
Problems Enabling SSO 222
Certificate Failure 222

CHAPTER 22 Traces Used To Troubleshoot IM and Presence Service 225
Troubleshooting IM and Presence Service Using Trace 225
Common Traces and Log File Locations for IM and Presence Service Nodes 226
IM and Presence Service Login and Authentication Traces 227
Availability, IM, Contact List, and Group Chat Traces 227
Availability and IM Traces for Partitioned Intradomain Federation MOC Contact Issues 229
Availability and IM Traces for XMPP-Based Interdomain Federation Contact Issues 229
Availability and IM Traces for SIP-Based Interdomain Federation Contact Issues 230
Calendaring Traces 231
Intercluster Synchronization Traces and Inter-Clustering Troubleshooter 231
SIP Federation Traces 232
XMPP Federation Traces 232
High CPU and Low VM Alert Troubleshooting 232

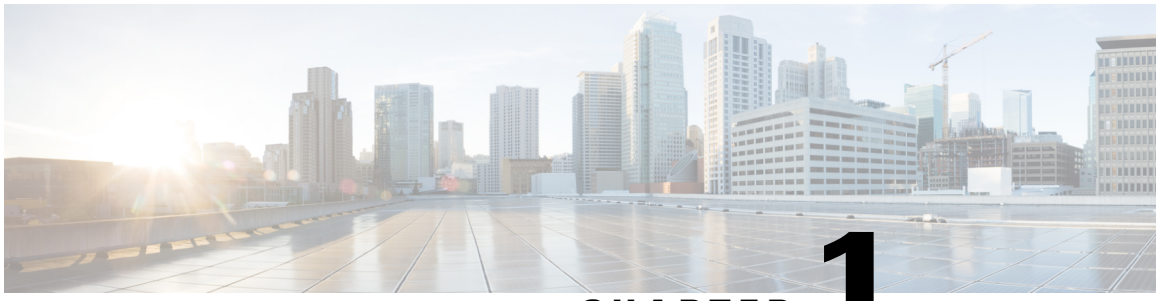
APPENDIX A High Availability Client Login Profiles 235
High Availability Login Profiles 235
Important Notes About High Availability Login Profiles 235
Use High Availability Login Profile Tables 236
Example High Availability Login Configurations 236
1000 Full UC Active/Standby 237
2 GB Active/Standby Profile 238
4 GB Active/Active Profile 238
4 GB Active/Standby Profile 239
6 GB Active/Active Profile 240
6 GB Active/Standby Profile 242

APPENDIX B XMPP Standards Compliance 245
XMPP Standards Compliance 245

PART I

Deployment Planning

- IM and Presence Service Features and Functions, page 3
- Multinode Scalability and WAN Deployments, page 17
- IM and Presence Service Planning Requirements, page 25
- Workflows, page 31



CHAPTER 1

IM and Presence Service Features and Functions

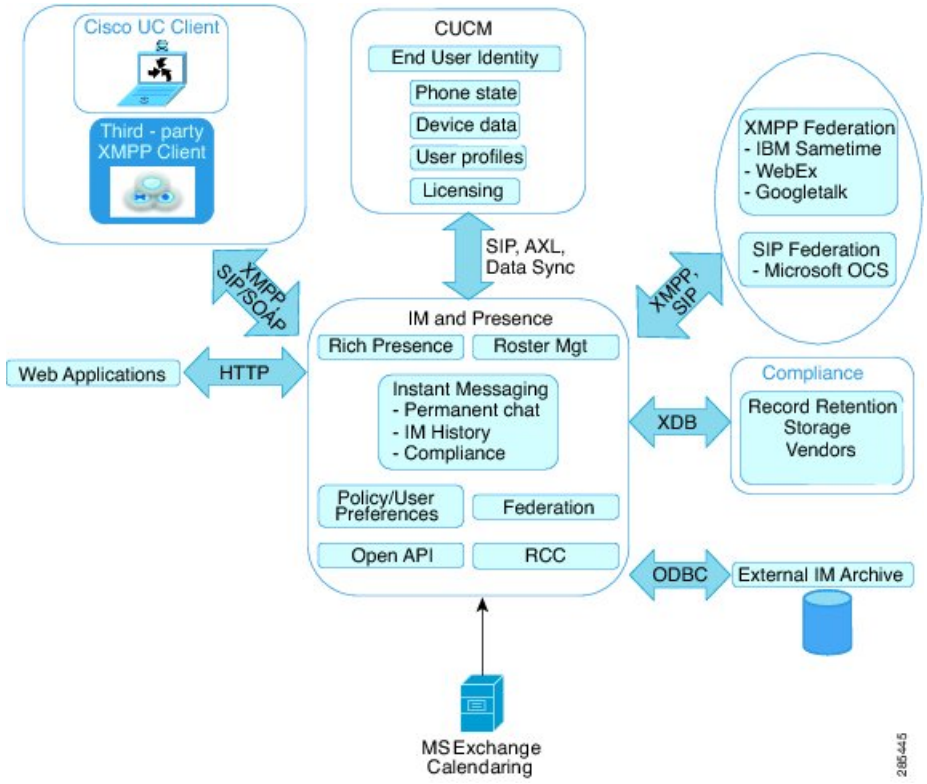
- IM and Presence Service Components, page 4
- Deployment models, page 6
- User Assignment, page 10
- End User Management, page 10
- Availability and Instant Messaging, page 10
- LDAP Integrations, page 13
- Third-Party Integrations, page 13
- Third-Party Client Integration, page 15
- Security, page 16
- Single Sign-On, page 16

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 and between IM and Presence Service and third-party products.

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 88

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
Configure Sync Agent Settings, on page 61

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 91
LDAP Server Name, Address, and Profile Configuration, on page 91
Secure Connection Between Cisco Unified Communications Manager and LDAP Directory, on page 92
Configure LDAP Server Names and Addresses for XMPP Clients, on page 97

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 121

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.

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 39

High Availability Deployments

The IM and Presence Service supports High Availability deployments.

Cisco recommends that you configure your IM and Presence Service deployments as High Availability deployments. Although mixed mode deployments are permitted, for example High Availability subclusters and non High Availability subclusters in a single deployment, this configuration is not recommended.

You must manually turn on High Availability in a subcluster. You can achieve a High Availability deployment by configuring the Balanced Mode (Redundant High Availability) or the Active/Standby Redundant High Availability deployment models, and turning on High Availability in your deployment.

Related Topics

Subclusters, on page 7

Multinode Deployment Models

You need to consider how you are going to deploy the multinode feature in your network. You configure your desired multinode deployment model in system topology management GUI in Cisco Unified CM IM and Presence Administration. Select **System** > **Cluster Topology** in Cisco Unified CM IM and Presence Administration to access system topology management GUI.

This module provides an overview of the deployment model options for the multinode feature, and provides examples of these deployments on system topology management GUI.

You only use system topology management GUI to configure your local IM and Presence Service cluster. See the intercluster peer module for information about configuring intercluster peer relationships with remote IM and Presence Service clusters.

Related Topics

User Assignment, on page 10

Subclusters

The multinode feature introduces the concept of a subcluster. A subcluster is a single IM and Presence Service node, or a pair of IM and Presence Service nodes, where each node has an independent database and set of users operating with a shared availability database that is able to support common users.

In a single-node deployment within a subcluster, there is no High Availability failover protection for users assigned to the node. In a dual-node deployment within a subcluster, if you turn on High Availability in the subcluster, users have failover protection; each node acts as a backup for the other node allowing clients to fail over in case of outages of components or nodes. When you turn on High Availability in a subcluster, all users in the subcluster have redundancy and full failover capabilities.

Related Topics

High Availability Deployments, on page 6
High Availability Deployments, on page 71
Create Subclusters in System Topology, on page 67

Balanced User Assignment Redundant High Availability Deployment

You can achieve a balanced mode High Availability deployment by evenly balancing users across all nodes in the subcluster, but only using up to 35% of the CPU of each IM and Presence Service node.

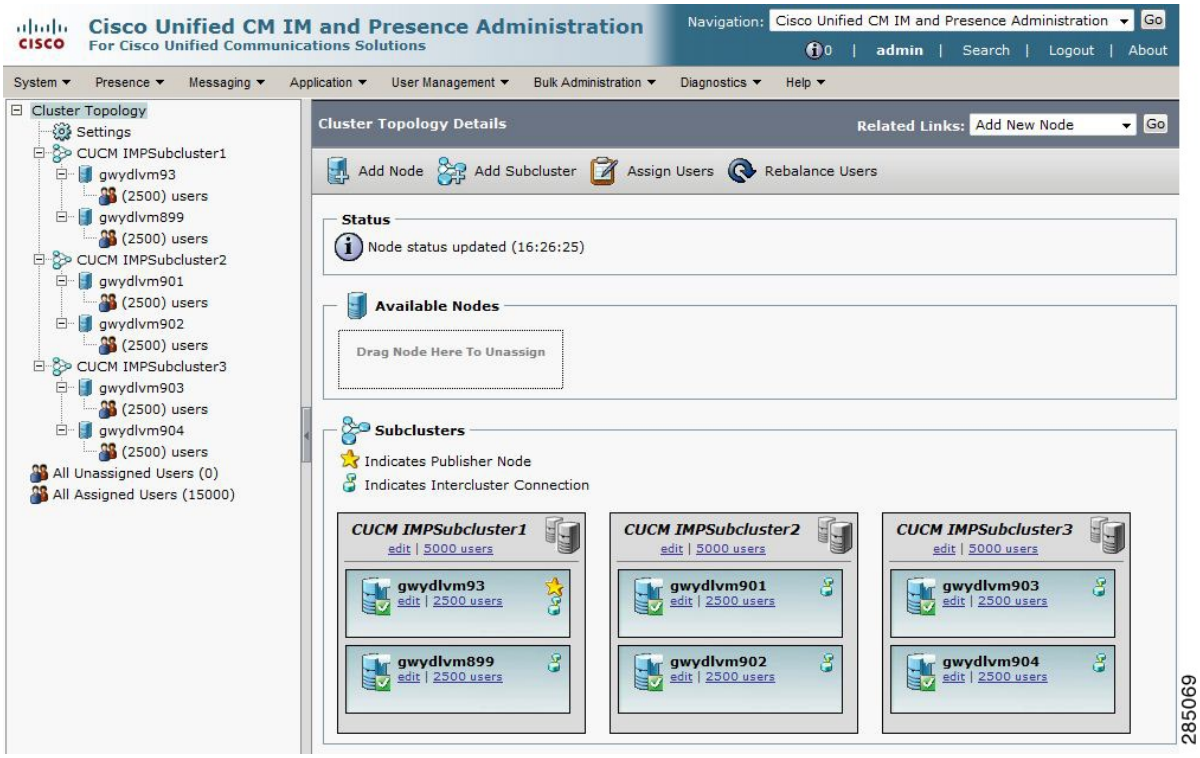
The balanced mode High Availability deployment option in a redundant mode supports up to 45,000 users per cluster. For example, if you have six IM and Presence Service nodes in your deployment, and 15,000 users, you assign 2,500 users to each IM and Presence Service node.

When you use the balanced mode High Availability deployment option in a redundant mode, as compared to a non-redundant mode, only half the number of users are assigned to each node. However, if one node fails,

the other node will handle the full load of the additional 50% of users in the subcluster, even at peak traffic. In order to support this failover protection, you must turn on High Availability in each of the subclusters in your deployment.

See the following figure for an example of this deployment model on system topology management GUI. In this example, there are 15,000 users in total, so 2,500 users are evenly balanced across the six nodes.

Figure 2: Balanced User Assignment Non-Redundant High Availability Deployment



Related Topics

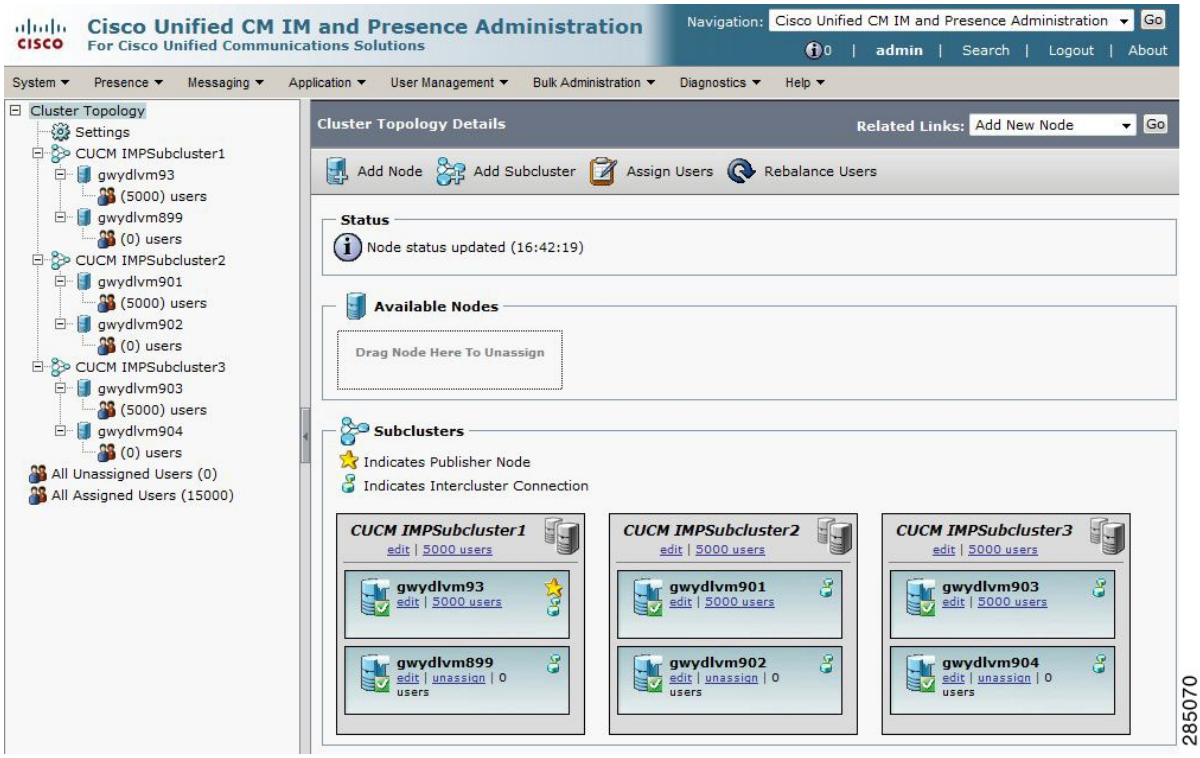
Cluster Topology Configuration on IM and Presence Service, on page 63
User Assignment Mode Recommendations, on page 65
Scalability Options for Deployment, on page 18
High Availability Deployments, on page 71
http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-device-support-tables-list.html
High Availability Deployments, on page 6

Active/Standby User Assignment Redundant High Availability Deployment

For this deployment model, assign all your users to the primary IM and Presence Service node, and none to the backup node. When you turn on High Availability in the subcluster, the backup node can handle all traffic from the primary node if the primary node fails.

See the following figure for an example configuration for this deployment model on system topology management GUI. In this example, there are 15,000 users in total, so 5000 users are assigned to the first node of each subcluster.

Figure 3: Active/Standby User Assignment High Availability Deployment



Related Topics

Cluster Topology Configuration on IM and Presence Service, on page 63
User Redistribution, on page 66
User Assignment Mode Recommendations, on page 65
Scalability Options for Deployment, on page 18
High Availability Deployments, on page 71
http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-device-support-tables-list.html
High Availability Deployments, on page 6

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 20

User Assignment

To allow users to avail of the availability and Instant Messaging (IM) services, you must assign users to nodes, and subclusters, in your IM and Presence Service deployment. You can manually or automatically assign users. You manage user assignment using the User Assignment Mode parameter on the Sync Agent on IM and Presence Service.

Balanced mode (default) assigns users equally to each node in the subcluster and attempts to balance the total number of users equally across each node. **Active-Standby** mode assigns all users to the first node of the subcluster, leaving the secondary server as a backup. **None** mode results in no assignment of the users to the nodes in the cluster by the sync agent. The default mode is Balanced.

If you choose manual user assignment, you must manually assign your users to nodes, and subclusters, using the System Topology interface in the **Cisco Unified CM IM and Presence Administration** GUI.

Related Topics

Multinode Deployment Models, on page 7
User Assignment Mode Recommendations, on page 65

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 134
Turn On or Off Availability Sharing for IM and Presence Service Cluster, on page 131

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 134

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 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.

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.

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 1: 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 This is the max number of messages that are returned when a user queries the room history.	100 messages
Messages in chat history displayed by default 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 177

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

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 91

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 2003, 2007 and 2010 • 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 • Configuring Microsoft Active Directory for this integration • Load-balancing MOC requests in a dual node IM and Presence Service deployment over TCP • Load-balancing MOC requests in a dual node IM and Presence Service deployment over TLS
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 • Configuring Microsoft OCS for Partitioned Intradomain Federation • Configuring Microsoft LCS for Partitioned Intradomain Federation • User Migration
Remote Call Control with Microsoft Lync Server 2010 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 • Configuring Microsoft Active Directory • Configuring normalization rules • 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/

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 29
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 96

Verify Domain Name for XMPP Clients

To verify the domain name value for XMPP clients on IM and Presence Service, select **Cisco Unified CM IM and Presence Administration** > **System** > **Cluster Topology**, select **Settings** in the right pane, and verify the Domain Name value.

The domain name on the XMPP client, specifically the XMPP connection attempt domain name, must match the domain on IM and Presence Service.

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.

Security

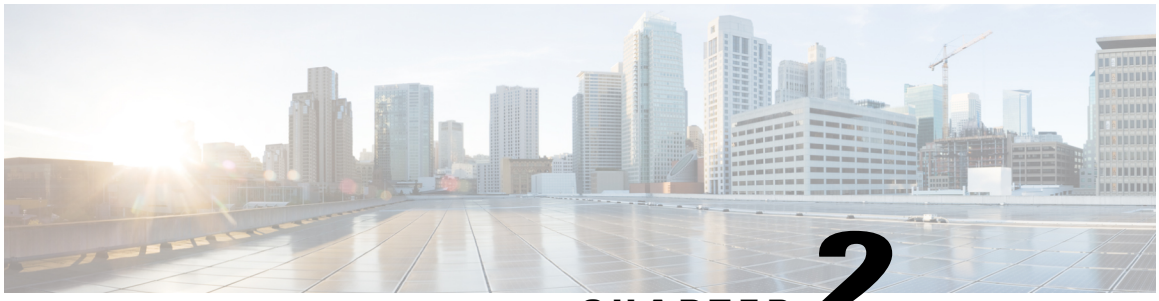
You can configure a secure connection between IM and Presence Service and Cisco Unified Communications Manager, XMPP clients, and SIP clients by exchanging certificates. Certificates can be self-signed or generated by a Certificate Authority (CA).

For more information, see topics related to security configuration.

Single Sign-On

The Single Sign-On (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 Service User Options
- 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



CHAPTER 2

Multinode Scalability and WAN Deployments

- Multinode Scalability Feature, page 17
- Cluster-Wide DNS SRV, page 19
- Local Failover, page 19
- Subcluster Failure Detection, page 19
- Method Event Routing, page 20
- External Database Recommendations, page 20
- Clustering Over WAN for Intracluster and Intercluster Deployments, page 20

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 subcluster, 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 2: Multinode Scalability Options

Deployment Mode	Scalability Option	
	Add a New Node to an Existing Subcluster	**Add a New Node to a New Subcluster**
Balanced Non-Redundant High Availability Deployment	If you add a new node to an existing subcluster, the new node can support the same number of users as the existing node; the subcluster 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 subcluster.	If you add a new node to a new subcluster, you can support more users in your deployment. This does not provide balanced High Availability for the users in the subcluster. To provide balanced High Availability, you must add a second node to the subcluster.
Balanced Redundant High Availability Deployment	If you add a new node to an existing subcluster, 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 subcluster. **Note** You may have to reassign your users within the subcluster, depending how many users were on the existing node.	If you add a new node to a new subcluster, you can support more users in your deployment. This does not provide balanced High Availability for the users in the subcluster. To provide balanced High Availability, you must add a second node to the subcluster.
Active/Standby Redundant High Availability Deployment	If you add a new node to an existing subcluster, you provide High Availability for the users in the existing node in the subcluster. 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 subcluster, you can support more users in your deployment. This does not provide High Availability for the users in the subcluster. To provide High Availability, you must add a second node to the subcluster.

Related Topics

Multinode Deployment Models, on page 7
Expand Cluster, on page 45

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.

Related Topics

Configure Cluster-Wide DNS SRV Name for SIP Publish Trunk, on page 89

Local Failover

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

Subcluster Failure Detection

The IM and Presence Service supports a failure detection mechanism for a subcluster. Each node in the subcluster monitors the status, or heartbeat, of the peer node. You can configure the heartbeat connection and heartbeat intervals on IM and Presence by selecting **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters** > **Cisco Config Agent (service)**. In the section General Cisco Config Agent Parameters (Clusterwide), configure the following parameters:

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

Note We 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.

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 subcluster geographically split over WAN, where one node in the subcluster is in one geographic site and the second node in the subcluster 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 subclusters 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 subcluster, 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 subcluster-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 20
IM and Presence Service Multinode Deployment Configuration, on page 43
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/uc7_0.html

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 27

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 23

Node Name Value for Intercluster Deployments

Note This topic is only applicable if you are not using DNS in your network.

If you configure an intercluster deployment, and you do not use DNS in your network, you must configure the node name value as the IP address of the node.

During installation IM and Presence Service only permits you to specify the hostname as the node name value. Therefore, once you complete the installation, you must change the node name value to the IP address of the node.

Perform this configuration on all nodes in both the local and remote clusters.

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
Manage Nodes in System Topology, on page 67

Default Domain Value for Intercluster Deployments

Note This topic is only applicable if you are not using DNS in your network.

If you configure an intercluster deployment, and you do not use DNS in your network, note the following:

- The default domain value on the local IM and Presence Service node must match the default domain value on the remote node.
- IM and Presence automatically defaults to the domain value DOMAIN.NOT.SET. On both the local and remote cluster, you must replace this default value with a valid domain value, otherwise the intercluster functionality will not work correctly.

To configure the default domain value for the IM and Presence Service node, follow the procedures described in Domain Value Configuration.

Related Topic

Node Name Value for Intercluster Deployments, on page 22

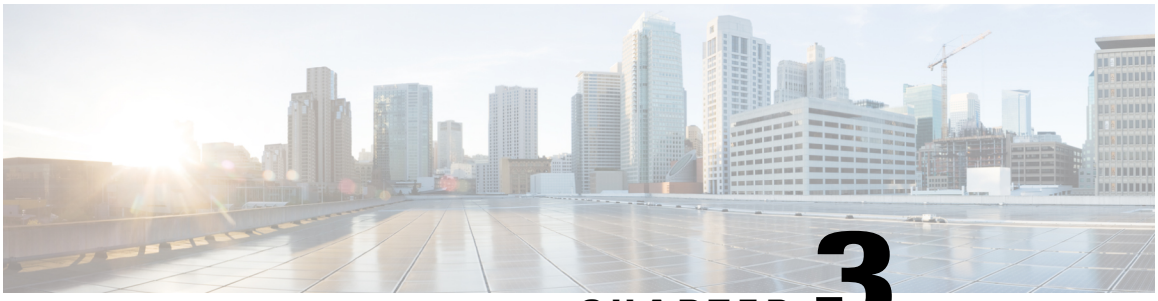
Secure Intercluster Router to Router Connection

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 22



CHAPTER 3

IM and Presence Service Planning Requirements

- Multinode Hardware Recommendations, page 25
- Intercluster Hardware Recommendations, page 26
- Supported End Points, page 26
- LDAP Directory Servers Supported, page 27
- WAN Bandwidth Requirements, page 27
- Multinode Scalability and Performance, page 28
- User License Requirements, page 29

Multinode Hardware Recommendations

When configuring the multinode feature, consider the following:

- Cisco recommends turning on High Availability in your deployment.
- Minimize your hardware, for example, instead of using six MCS 7825 servers that support a total of six thousand users, choose two MCS 7835 servers 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 subcluster and put fewer users on this subcluster than on the more powerful subclusters. Note that we do not recommend this deployment practice.

Warning 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.

- Use the following disk drives for the multinode feature:
  - MCS 7816: minimum one 160GB drive (a 250GB drive can also be used)

- MCS 7825: minimum two 160GB drives (two 250GB drives can also be used, upgrade required from smaller 80GB drives)
- MCS 7835: minimum two 146GB drives (upgrade required from smaller 72GB drives)
- MCS 7845: minimum four 72GB drives (upgrade recommended to four 146GB drives)

Note The MCS 7845 with four 72GB drives can run the scalability feature, but this hardware with four 146GB drives is preferred.

- If you have older-generation hardware, follow the disk drive upgrade recommendations above. You must meet the minimal disk capacity on each server in the cluster in order to achieve scale.

Note Upgrading drives will allow you to use older hardware in a multinode cluster. However, Cisco recommends that you use the latest hardware available for the multinode feature because this hardware has more powerful CPU, more memory and faster input/output processing.

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 hardware is used on all IM and Presence Service clusters in the Enterprise to allow for syncing of all user data between clusters. For example, if an MCS 7845 is deployed in Cluster A with 15,000 users, then an MCS 7845 should be deployed in Cluster B even if only needed for 500 users.

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 Client (Microsoft Office Communicator client)

LDAP Directory Servers Supported

IM and Presence Service integrates with these LDAP directory servers:

- Microsoft Active Directory 2000, 2003 and 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 subcluster, 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 subcluster 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 subcluster, 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 hardware classes results in nodes that are under-powered, therefore resulting in poor performance.
- You deploy 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 subclusters. The IM and Presence Service defaults to Balanced Mode user assignment to achieve optimum performance.

Related Topics

Multinode Hardware Recommendations, on page 25
Balanced User Assignment Redundant High Availability Deployment, on page 7

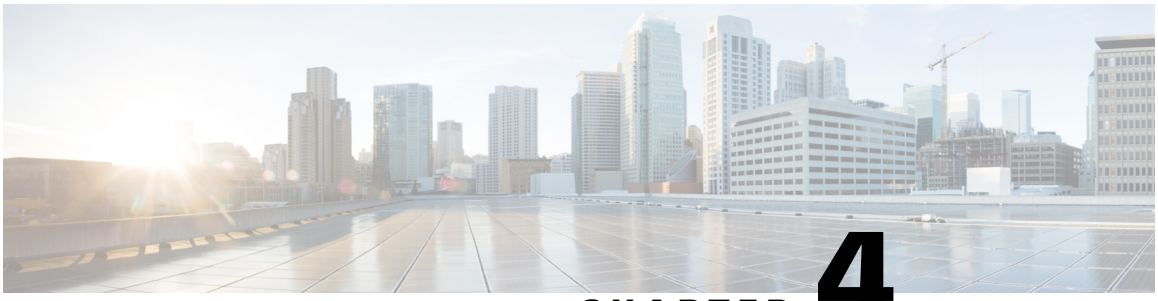
User License Requirements

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.



CHAPTER 4

Workflows

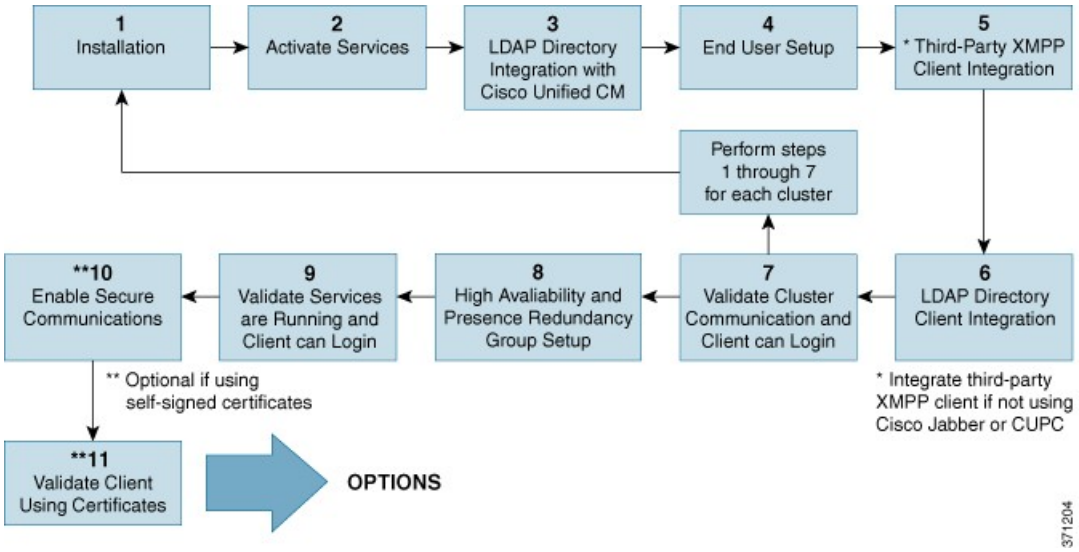
- Basic Deployment with High Availability Workflow, page 31
- Basic Deployment with High Availability and IP Phone Presence Workflow, page 34
- Federation Deployment Workflow, page 36
- IM-Only Deployment Workflow, page 39

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 4: 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 3: 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*. **Tip** Network services start automatically after you install the node.

	Task	Description
3	LDAP Directory Integration with Cisco Unified Communications Manager	Set up LDAP directory integration on the IM and Presence Service node: • Secure the Cisco Unified Communications Manager and LDAP directory connection. • Secure the connection between IM and Presence Service and the LDAP server. **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 subclusters in yourIM and Presence Service deployment. You can manually or automatically assign users to the nodes in your IM and Presence Service deployment. **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: • Configure LDAP synchronization for user provisioning. • Upload LDAP server certificates. • Configure LDAP user authentication. **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	High Availability and Subcluster Setup	For instructions to set up high availability and subclusters, see the *System Configuration* section.
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.

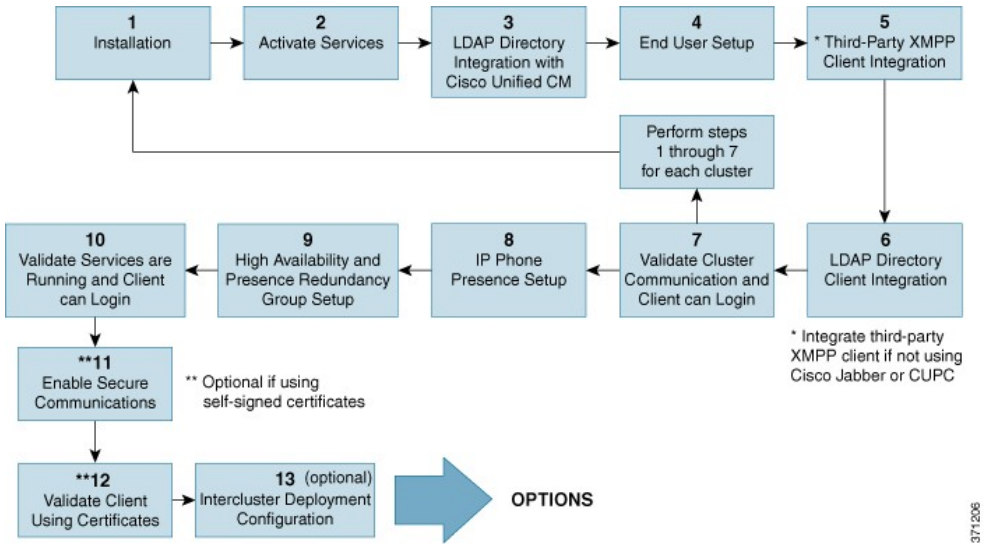
	Task	Description
10	Enable Secure Communications	Perform the following tasks to enable secure communications on the IM and Presence Service node: • Configure certificate exchange between IM and Presence Service and Cisco Unified Communications Manager. • Upload CA signed certificates to IM and Presence Service. • Configure SIP security settings on IM and Presence Service for the TLS peer subject. • (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 5: Basic IM and Presence Service Workflow with High Availability and IP Phone Presence



The following table describes each task in the workflow.

Table 4: 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*. **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: • Secure the Cisco Unified Communications Manager and LDAP directory connection. • Secure the connection between IM and Presence Service and the LDAP server. **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 subclusters in yourIM and Presence Service deployment. You can manually or automatically assign users to the nodes in your IM and Presence Service deployment. **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: • Configure LDAP synchronization for user provisioning. • Upload LDAP server certificates. • Configure LDAP user authentication. **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.

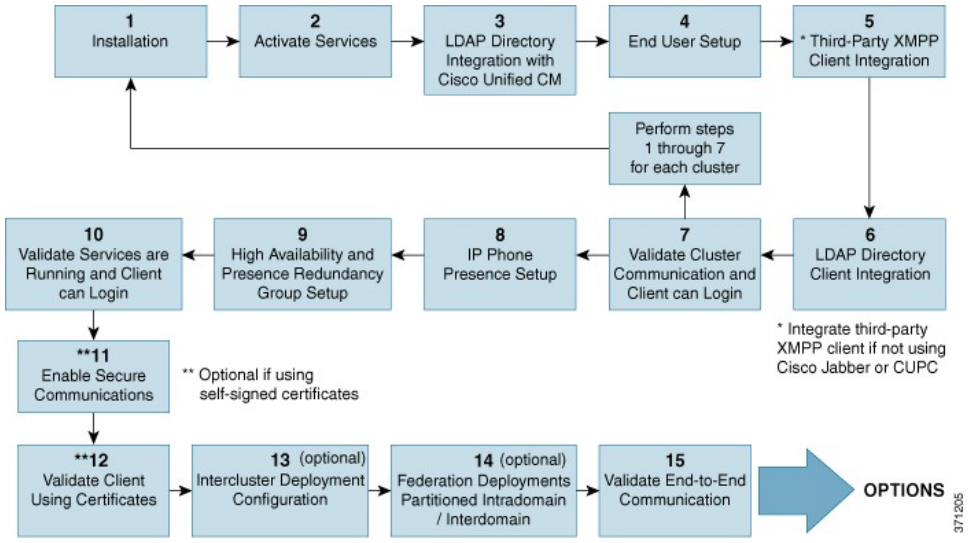
	Task	Description
8	IP Phone Presence Setup	Set up the following on IM and Presence Service node: • Static routes • Presence Gateway • SIP publish trunk • Cluster-wide DNS SRV name for SIP publish trunk
9	High Availability and Subcluster Setup	For instructions to set up high availability and subclusters, see the *System Configuration* section.
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.
11	Enable Secure Communications	Perform the following tasks to enable secure communications on the IM and Presence Service node: • Configure certificate exchange between IM and Presence Service and Cisco Unified Communications Manager. • Upload CA signed certificates to IM and Presence Service. • Configure SIP security settings on IM and Presence Service for the TLS peer subject. • (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 6: IM and Presence Service Workflow for Federation Deployment



The following table describes each task in the workflow.

Table 5: 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*. **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: • Secure the Cisco Unified Communications Manager and LDAP directory connection. • Secure the connection between IM and Presence Service and the LDAP server. **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 subclusters in yourIM and Presence Service deployment. You can manually or automatically assign users to the nodes in your IM and Presence Service deployment. **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: • Configure LDAP synchronization for user provisioning. • Upload LDAP server certificates. • Configure LDAP user authentication. **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: • Static routes • Presence Gateway • SIP publish trunk • Cluster-wide DNS SRV name for SIP publish trunk
9	High Availability and Subcluster Setup	For instructions to set up high availability and subclusters, see the *System Configuration* section.
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: • Configure certificate exchange between IM and Presence Service and Cisco Unified Communications Manager. • Upload CA signed certificates to IM and Presence Service. • Configure SIP security settings on IM and Presence Service for the TLS peer subject. • (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.

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

Table 6: 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: http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

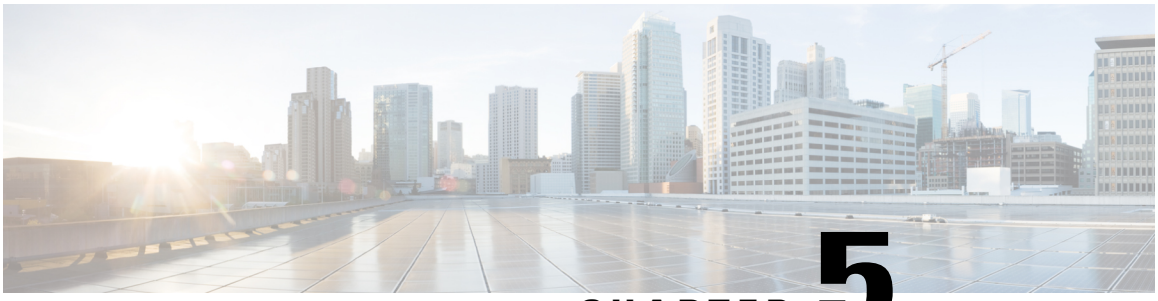
Task	Description
Integrate the LDAP server for Cisco Jabber	Configure the LDAP settings on IM and Presence Service to allow Cisco Jabber users to search for contacts from the LDAP directory. **Note** You should create an LDAP profile and verify LDAP attribute mappings, even if your Cisco Jabber client 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

- IM and Presence Service Multinode Deployment Configuration, page 43
- Cisco Unified Communications Manager configuration for integration with IM and Presence Service, page 49
- IM and Presence Service Network Setup, page 55
- Cluster Topology Configuration of Subclusters, Nodes, and Users, page 63
- High Availability Deployment Configuration, page 71
- IP Phone Presence Setup , page 83
- LDAP Directory Integration, page 91
- Security Configuration on IM and Presence Service, page 101
- Intercluster Peer Configuration, page 123



CHAPTER 5

IM and Presence Service Multinode Deployment Configuration

- Cisco Replication Watcher Service, page 43
- Multinode Update Configuration After Deployment, page 44
- Multinode Deployment Troubleshooting, page 46

Cisco Replication Watcher Service

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

On the subscriber nodes, the Cisco Replication Watcher service delays the startup of feature services until IDS replication is successfully established. The Cisco Replication Watcher service 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 Replication Watcher service allows feature services to start on node1 and node2, but delays feature service startup on node3.

The Cisco Replication Watcher service 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 Replication Watcher service 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 Replication Watcher service 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 Service 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.

Multinode Update Configuration After Deployment

Add New Node

Follow this procedure if you need to add new nodes after a multinode deployment is running.

You can create the new node in your topology before you install the node, specifically before you install the IM and Presence Service software on the new node. However, you cannot assign the new node to a subcluster before you install IM and Presence Service software on the new node.

Restrictions

Your hardware must comply with the multinode hardware recommendations.

Procedure

Step 1 Create a new subcluster in system topology management GUI (if required).

Step 2 Create a new node in system topology management GUI.

Step 3 Install the IM and Presence Service software on the new node.
See the *Installing Cisco Unified Communications Manager, Release 9.0(1)* for the installation procedure.

Step 4 Assign the node to the subcluster (if required).

Note Before you assign or move a node to a subcluster, check the following

- From System troubleshooter page, verify that the Cisco Replication Watcher service is running on all nodes.
- On the **Network services** screen in Cisco Unified IM and Presence Serviceability (on the subscriber node), verify that all IM and Presence Service services are running.

IM and Presence assigns the node to the cluster, but the node will not receive traffic until you assign users to it.

Step 5 Turn on High Availability in the subclusters as required.

Step 6 Assign users from other nodes to the new node as required.

Related Topics

Multinode Hardware Recommendations, on page 25
Create Subclusters in System Topology, on page 67
Manage Nodes in System Topology, on page 67
Configure User Assignment in System Topology, on page 69
High Availability Deployments, on page 71

Expand Cluster

Restrictions

- Your hardware must comply with the multinode hardware recommendations.
- Cisco recommends that you perform any node movements that involve you unassigning or moving a large numbers of users at off peak times. Such large operations can adversely impact performance.

Procedure

Step 1 Create the new subcluster(s) in system topology management GUI (if required).

Step 2 Create the new nodes in system topology management GUI.

Step 3 Install each new node.

Step 4 Assign the nodes to the (new) subclusters.

Note Before you assign or move a node to a subcluster, check the following

- From System troubleshooter page, verify that the Cisco Replication Watcher service is running on all nodes.
- On the **Network services** screen in Cisco Unified IM and Presence Serviceability (on the subscriber node), verify that all IM and Presence Service services are running.

Step 5 Turn on High Availability in the subclusters as required.

Step 6 Once all the nodes are online, assign users to the new nodes using the following user assignment options:

a) Using the Find User Assignment feature, unassign selected users from each node, and use the User Assignment Mode parameter to reassign new users to new subcluster(s) and nodes.

b) Using the Find User Assignment feature, manually move users to new nodes.

c) Unassign all users, and then reassign the users to the cluster using the appropriate User Assignment Mode parameter setting for the whole cluster.

Tip You must turn off High Availability in a subcluster before you move or unassign a node in that subcluster.

Related Topics

Multinode Hardware Recommendations, on page 25
Create Subclusters in System Topology, on page 67
Manage Nodes in System Topology, on page 67
Configure User Assignment in System Topology, on page 69
High Availability Deployments, on page 71

Remove Node

Follow this procedure if you need to safely remove an IM and Presence Service node from a subcluster.

Note This procedure removes subscriber nodes only. Publisher nodes cannot be removed.

Caution Removing a node will cause a service interruption to users on the remaining node(s) in the subcluster. This procedure should only be performed during a maintenance window.

Procedure

Step 1 Select **Cisco Unified CM IM and Presence Administration > System > Cluster Topology**.

Step 2 Turn off High Availability if it is enabled.

Step 3 Unassign or move all users from the node that you want to remove.

Step 4 To remove the node from its subcluster, drag the node icon to the Available Nodes pane. Select **OK** when a warning dialog box indicates that services in the subcluster will be restarted as a result of removing the node.

Step 5 Delete the node you have unassigned from the Cluster Topology page. Select **OK** when a warning dialog box indicates this action can only be undone by performing a fresh installation.

Step 6 Shut down the host VM or server for the node you have unassigned.

Step 7 Remove the Application Server entry on Cisco Unified Communications Manager for the node you have unassigned.

Multinode Deployment Troubleshooting

Monitor Multinode System

Restriction

If you need to add hardware to your multinode deployment, the hardware must comply with the multinode hardware recommendations.

Procedure

Step 1 Use the IM and Presence Real-Time Monitoring Tool (RTMT) tool to monitor the CPU and memory usage of each IM and Presence Service node in the cluster.

Step 2 Use these guidelines to determine if you need additional hardware:

Deployment Model	Recommendation
No High Availability or Balanced Non-Redundant High Availability	If the CPU reaches more than 70% capacity for a sustained period on any IM and Presence Service node, we recommend that you add hardware resources to your deployment.

Deployment Model	Recommendation
Balanced Redundant High Availability	If the CPU reaches more than 35% capacity over a sustained period on either IM and Presence Service node in the subcluster, we recommend that you add hardware resources to your deployment.
Active/Standby High Availability	If the CPU reaches more than 70% capacity for a sustained period of time on the active IM and Presence Service node, we recommend that you add hardware resources to your deployment.

Related Topics

Multinode Hardware Recommendations, on page 25
Multinode Deployment Models, on page 7

Resolve Hardware Problem

Follow this procedure if there is a problematic node, or some general hardware failure.

Restrictions

If you need to add hardware to your multinode deployment, the hardware must comply with the multinode hardware recommendations.

Procedure

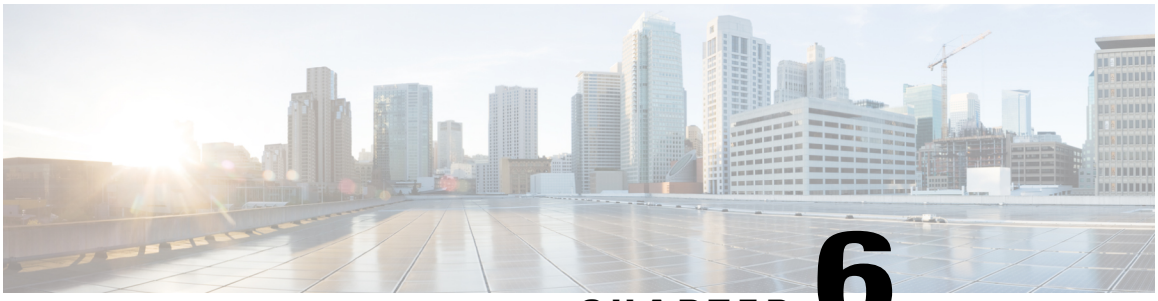
Step 1 Create a new node in system topology management GUI.
Step 2 Perform a fresh installation on this node.
Step 3 Unassign the users from the problematic node.
Step 4 Stop all services on the problematic node.
Step 5 Unassign the problematic node.
Step 6 Assign the new node to the subcluster, replacing the problematic node.
Step 7 Reassign the unassigned users to the new node.
Step 8 Delete the problematic node.
Step 9 Activate all services on the new node.
Troubleshooting Tip

You must turn off High Availability in a subcluster before you move or unassign a node in that subcluster.

Related Topics

Multinode Hardware Recommendations, on page 25

Manage Nodes in System Topology, on page 67
Configure User Assignment in System Topology, on page 69



CHAPTER 6

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, page 49
- Configure Inter-Presence Group Subscription Parameter, page 50
- SIP Trunk Configuration on Cisco Unified Communications Manager, page 51
- Verify Required Services Are Running on Cisco Unified Communications Manager, page 54

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 7: 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. 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. 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. **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. **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. **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. **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. **Cisco Unified CM Administration** > **User Management** > **User Group**

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 91

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:

- When you add or remove a node on the system topology management GUI, the node is automatically added to or removed from the Application Server list on Cisco Unified Communications Manager.
- When you configure the Cisco Unified Communications Manager publisher on IM and Presence Service from **Cisco Unified CM IM and Presence Administration** > **System** > **CUCM Publisher**, the IM and Presence Service node is automatically added to the Application Server list 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*.

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 89
Configure SIP Trunk Security Profile for IM and Presence Service, on page 52
Configure SIP Publish Trunk on IM and Presence Service, on page 89
Presence Gateway Configuration Option, on page 88

Verify Required Services Are Running on Cisco Unified Communications Manager

Procedure

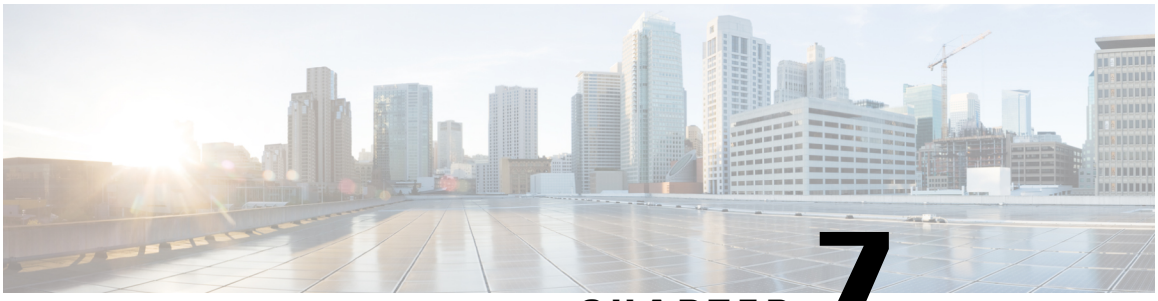
Step 1 On Cisco Unified Communications Manager, choose **Cisco Unified Serviceability** > **Tools** > **Control Center - Feature Services**.

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 7

IM and Presence Service Network Setup

- Configuration changes and service restart notifications, page 55
- Domain Value Configuration, page 56
- Routing Information Configuration on IM and Presence Service, page 57
- Configure Proxy Server Settings, page 60
- Services on IM and Presence Service, page 61

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.

Domain Value Configuration

Note

- Cisco Unified Presence automatically defaults the presence domain for the cluster to the DNS domain specified during Cisco Unified Presence installation.
- It is highly recommended that you use a DNS deployment . If however you are not using DNS in your network and you did not set a DNS domain at install, the presence domain is set to "DOMAIN.NOT.SET" by default. You must replace this default value with the enterprise-wide presence domain.
- In order to be considered valid, the presence domain value must match the DNS domain name. Using a valid domain name ensures that the SRM initializes correctly in a High Availability deployment.

Follow this procedure if you want to change the domain value (from one valid domain value to another valid IP proxy domain value).

This procedure is applicable if you have a DNS or non-DNS deployment.

Procedure

Step 1 Stop the Cisco SIP Proxy, Presence Engine and XCP Router services on IM and Presence on all nodes in your cluster.

Step 2 On the publisher node, perform the following steps to configure the new domain value:

a) Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Cluster Topology**.

b) In the right pane, click **Settings**.

c) Configure the Domain Name value with the new domain.
d) Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters**, and select the **Cisco SIP Proxy** service.
e) Configure the Federation Routing IM and Presence FQDN with the new domain.
f) You will be prompted to confirm these configuration changes. Click **OK** for both prompts, and then select **Save**.

Step 3 On all nodes in the cluster, use this CLI command to set the new domain:
set network domain <new_domain>
This CLI command invokes a reboot of the servers

Step 4 On all nodes in the cluster, manually start the Cisco Presence Engine and Cisco XCP Router services after the reboot is complete (if required).

Step 5 Manually regenerate all certificates on each node in the cluster.

Note When you regenerate the Tomcat certificate, you must restart Tomcat. You can restart Tomcat after you regenerate all of the certificates on the local server. Use this CLI command to restart Tomcat: utils service restart Cisco Tomcat

Step 6 If you use DNS in your network, update the DNS configuration for the new domain. Update any host records and any DNS SRV records that you require for the new domain

Step 7 Configure any XMPP clients with the new domain.

Routing Information Configuration on IM and Presence Service

Routing Communication Recommendations

MDNS is the default mechanism for establishing the XCP route fabric on IM and Presence Service; the network automatically establishes router-to-router connections between all IM and Presence Service nodes in a cluster. A requirement for MDNS routing is that all nodes in the cluster are in the same multicast domain. We recommend MDNS routing because it 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.

Alternatively, you can choose router-to-router communication for your deployment. In this case, IM and Presence Service dynamically configures all router-to-router connections between nodes in a cluster. Choose this routing configuration type if all the nodes in your cluster are not in the same multicast domain. Note that when you choose router-to-router communication:

- Your deployment will incur 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.

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** > **System** > **Cluster Topology** > **Settings** 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 173

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** > **Cluster 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** > **Cluster Topology**.

Step 2 In the right pane, choose **Settings**.

Step 3 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 4 Click **Save**.

Step 5 Restart the Cisco XCP Router service on all nodes in your deployment.

Related Topics

Restart Cisco XCP Router Service, on page 56

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** > **System** > **Cluster Topology**.

Step 2 In the right pane, choose **Settings**.

Step 3 View or edit the Cluster ID value.

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

Step 4 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 173

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**.

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

Configure Sync Agent Settings

Before You Begin

- Configure the topology for your deployment before starting the Sync Agent.
- If you deploy the Cisco Jabber client with IM and Presence Service, and you configure system-wide default application profiles, configure and enable the default profiles before you activate the Sync Agent.

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 Sync Agent** from the **Service** menu.

Step 4 Choose a value for the **User Assignment Mode** as follows:

a) If set to **Balanced**, the Sync Agent synchronizes user information to IM and Presence Service, and then assigns the users to each node in an attempt to balance the user assignment evenly across all nodes.

- If set to **Active/Standby**, the Sync Agent synchronizes user information to IM and Presence Service, and assigns the total number of users to the first node of a subcluster only. If there is only a single node in the subcluster, the Sync Agent uses this node for assignment regardless of the location of the node within the subcluster.

b) If set to **None**, the Sync Agent synchronizes user information to IM and Presence Service but does not assign any users. You must manually assign your users to nodes using the system topology interface

Step 5 Choose **Save**.

Related Topics

Cluster Topology Configuration on IM and Presence Service, on page 63
Turn On Services for IM and Presence Service, on page 61

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.

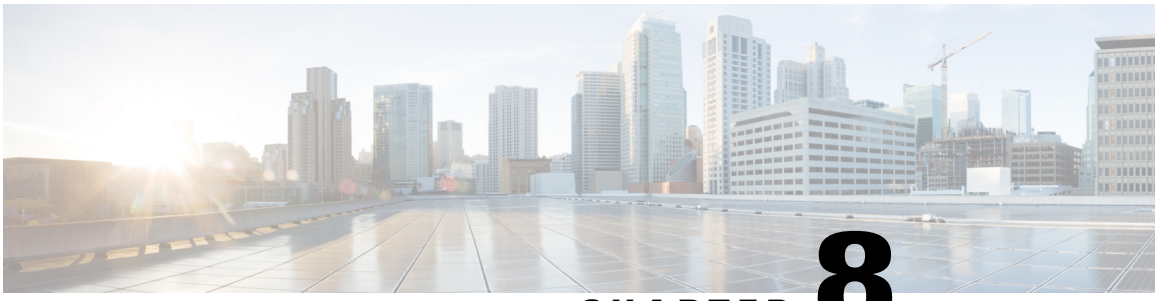
Step 3 For a basic IM and Presence Service deployment, turn on the following services:

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

Step 4 Click **Save**.

Related Topics

Configure Sync Agent Settings, on page 61



CHAPTER 8

Cluster Topology Configuration of Subclusters, Nodes, and Users

- Cluster Topology Configuration on IM and Presence Service, page 63
- Subcluster, Node and User Management Recommendations, page 63
- Create Subclusters in System Topology, page 67
- Manage Nodes in System Topology, page 67
- Configure User Assignment in System Topology, page 69

Cluster Topology Configuration on IM and Presence Service

When you configure the multinode feature using Cluster Topology, note the following:

- Perform the system topology configuration on the IM and Presence publisher node.
- Before configuring the system topology, read the multinode planning and deployment information for best practice information about configuring this type of deployment.

Perform these procedures only if you are deploying IM and Presence Service in a multinode configuration.

Caution Only use the system topology interface to configure your local IM and Presence Service cluster. See the intercluster peer module for information about configuring intercluster peer relationships with remote IM and Presence clusters.

Subcluster, Node and User Management Recommendations

Node Creation and Movement Recommendations

When you create nodes in the system topology management GUI you can:

- Assign the nodes to a subcluster in IM and Presence Service, or allow the nodes to remain unassigned. These states are interchangeable.
- Assign IM and Presence Service users to the nodes, or allow the nodes to remain without any user assignments.
- Turn on or off High Availability on a subcluster. See the section about configuring High Availability deployments later in this chapter.
- Move a node from one subcluster to another if the node is assigned, has no users and high- availability is turned off in the subcluster.
- Move a node from one subcluster to another if the node is assigned and has no users.
- Configure real pingable nodes, or logical nodes which can be installed later and which remain inaccessible until that time.

To move nodes with users assigned, perform one of the following actions:

- Unassign the users, move the node, and then reassign the users to the node. Note that when you unassign the users, they will lose service.
- Create a logical node and move the users to the logical node. Move the node, reassign the users to the node, and remove the logical node.
- Remove all users from a node before you unassign or move it.
- Turn off High Availability in the subcluster before you unassign or move a node in that subcluster.
- We strongly recommend that you perform any node movements that involve unassigning or moving a large numbers of users at off peak times. Such large operations can adversely impact performance.

Related Topics

Manage Nodes in System Topology, on page 67

Node Name Recommendations

By default, the name for a node is the hostname that you configure during IM and Presence Service installation. For example, if the hostname of your IM and Presence Service node is called “cup1”, the node name is “cup1”. You can change the node name to the dotted IP address or the FQDN, for example, “192.168.0.1” or “cup1.acme.com”. If you change the default name for the node, note the following:

- You must be able to resolve the hostname or the FQDN from the IM and Presence Service node, and Cisco Jabber clients.
- If either IM and Presence Service node or the Cisco Jabber client cannot resolve the hostname or the FQDN, configure the IP address for the node name value.
- To test the name resolution from the IM and Presence Service node, use the command `utils network ping <node_name>`
- To test the name resolution from the Cisco Jabber client, use the command `ping <node_name>`
- If your network uses DNS that can map to IPv4 addresses, you can enter the IM and Presence Service hostname. Otherwise, you must enter the full IPv4 address of the IM and Presence Service node.

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.

Related Topics

Manage Nodes in System Topology, on page 67

User Assignment Mode Recommendations

You can manually or automatically assign users in an IM and Presence Service deployment. Use the User Assignment Mode parameter on the Sync Agent to manage user assignment on IM and Presence Service:

- If set to **Balanced**, IM and Presence Service divides all users equally across all nodes in all subclusters. Use this user assignment mode for the Balanced Mode Non-Redundant High Availability and the Balanced Mode Redundant High Availability deployment options.
- If set to **Active/Standby**, IM and Presence Service assigns all users only to the first node of a subcluster. If there is only a single node in the subcluster, IM and Presence Service uses this node for assignment regardless of the location of the node within the subcluster.
- If set to **None**, you must manually assign your users to nodes in system topology management GUI.
- If all the hardware in your cluster is of the same generation and has the same capacity, set the User Assignment Mode to **Balanced**.
- If you have hardware of mixed generations and capacities in a node, set the User Assignment Mode to **None**. Manually assign your users making sure that each server is not loaded beyond capacity.

Related Topics

Configure Sync Agent Settings, on page 61

Manual User Assignment Recommendations

If you choose to manually assign users in system topology management GUI, note the following:

- You can manually unassign, assign or reassign users. You can assign users to a single node, and you can also distribute groups of users across the node, or nodes, in a cluster, or a given subcluster.
- If you assign a user to one of the nodes in a subcluster, the other node in the subcluster can become the backup (redundant) node for the user if you turn on High Availability for the subcluster. If you do not configure a backup node in the subcluster, and you do not turn on High Availability for the subcluster, the user does not have High Availability failover protection.
- Users who are assigned may be reassigned, that is, moved to another subcluster, or to a specific node. You can move users individually or in bulk.
- Users can remain unassigned. Unassigned users do not receive availability information.

Note We recommend that you only reassign a user (assign a user that was previously unassigned) if the Cisco Presence Engine is running on all nodes in your cluster, otherwise IM and Presence Service will not reestablish the presence subscriptions to and from this user.

When you are assigning users, note the following:

- You can only assign users if they are licensed.
- Unassigning or reassigning users results in termination of active sessions. In such instances, clients must reconnect to the new location.
- You can export users in bulk using the Bulk Administration Tool (BAT). You can also use BAT to perform bulk user reassignment from one node to another.

Generally we recommend that you take the Cisco Presence Engine and Cisco SIP Proxy services offline when performing bulk operations. Note that taking these services offline will adversely impact performance.

Related Topics

Configure User Assignment in System Topology, on page 69
Turn On or Off High Availability for Subcluster, on page 75

User Redistribution

Note

- If you turn on High Availability in a subcluster, be aware that IM and Presence Service does not redistribute users to nodes that are in a failover states; the valid node states that support user redistribution are Normal and Running in Backup Mode.
- If you **rebalance** your users, you must reconfigure the upper and lower client re-login limit values based on the HA login profile tables, see topics related to High Availability client login profiles.

After adding or removing nodes, you can redistribute users using the **Rebalance Users** parameter in system topology management GUI. This parameter redistributes users based on the configured User Assignment mode. These are examples of how you can use the Rebalance Users parameter with the User Assignment mode to manage user assignment:

- Scenario A: The customer has a subcluster with two nodes, and each node contains 5000 users. The User Assignment mode is set to Balanced. The customer then adds a second subcluster with two nodes, and sets the Rebalance Users parameter. IM and Presence Service distributes the users evenly to the four nodes so that each node now has 2500 users.
- Scenario B: The customer has a subcluster with two nodes, and each node contains 2500 users. The User Assignment mode is set to Balanced. The customer wants to add a second subcluster with two nodes, but also wants to change the User Assignment mode to Active/Standby. The customer changes the mode to Active/Standby, whereby all 5000 users are redistributed to the first node in the subcluster. The customer then adds a second subcluster with two nodes, and sets the Rebalance Users parameter. IM and Presence Service evenly distributes the users across both first nodes in each subcluster. Each first node now has 2500 users.

We strongly recommend that you perform any node movements that involve unassigning or moving a large numbers of users at off peak times. Such large operations can adversely impact performance.

Related Topics

High Availability Login Profiles, on page 235
Node Creation and Movement Recommendations, on page 63
Configure User Assignment in System Topology, on page 69

Create Subclusters in System Topology

The system automatically assigns the first IM and Presence Service node that you install as the publisher node. After you install the publisher node, create the required subclusters and subsequent nodes in your IM and Presence Service cluster in system topology management GUI.

Repeat this procedure for each subcluster that you require for your deployment.

Note Perform this procedure on the publisher IM and Presence Service node.

Before You Begin

Plan your multinode deployment model.

Procedure

Step 1 Select **Cisco Unified CM IM and Presence Administration** > **System** > **Cluster Topology**.

Step 2 Select **Add New Subcluster**.

Step 3 Define a unique name for the subcluster.

Step 4 Select **Save**.

Troubleshooting Tip

To update a subcluster, or view the status of a subcluster, select the **edit** link on the subcluster.

What to Do Next

Proceed to manage nodes using System Topology.

Manage Nodes in System Topology

Create the required subsequent nodes for your deployment. By creating the subsequent nodes in the topology view of the publisher node, IM and Presence Service associates the subsequent nodes with the publisher node.

Before You Begin

Note

- Perform this procedure on the publisher IM and Presence Service node.
- Perform this procedure before you install any of the subsequent IM and Presence Service nodes. If you assign a subsequent IM and Presence Service node to a subcluster prior to installing it, users in remote clusters will not receive availability information. An availability outage will occur until the node is installed.

Depending on how you plan to configure your node name, obtain the required value for your nodes (for example FQDN, hostname or dotted IP address). Note the following restrictions:

- If you wish to change the default node name, there are certain node name restrictions. Read the node name recommendations topic.
- You can only move a node from one subcluster to another if the node is assigned and has no users.
- You must turn off High Availability in a subcluster before you move or unassign a node in that subcluster.

Procedure

Step 1 Create the required subclusters for your deployment.

Step 2 Select **Cisco Unified CM IM and Presence Administration** > **System** > **Cluster Topology**.

Step 3 Create the required subsequent nodes for your deployment:

a) Select **Add New Node**.
b) Define a unique name for the node.
c) Select **Save**.

Step 4 Perform one of the following actions:

- To assign a node to a subcluster, drag the node into the empty slot in the subcluster.
  - Do not assign the subsequent node to a subcluster until after you install it, and you have checked the status of the node.
  - Before you assign a node to a subcluster, check the following
    - From System troubleshooter page, verify that the Cisco Replication Watcher service is running on all nodes.
    - On the Network services screen in Cisco Unified IM and Presence Serviceability (on the subscriber node), verify that all IM and Presence services are running on the assigned node.
- To move a previously assigned node, drag the node from the subcluster and drop it into the empty slot of the peer subcluster.
  - Turn off high-availability in the subcluster before you move the node.
  - Unassign all users from the node before you move it.

Step 5 Select **Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter** to verify the status of your topology configuration.

Tip To update a node, or view the status of a node, select the **edit** link on the node to view the Node Detail screen. From the edit window, you can:

- ◦ View the total users assigned to the node.
  ◦ Verify the status of the node.
- If you turn on High Availability in the subcluster, the critical services that IM and Presence Service monitors on the node for failover are marked in the "Monitored" column.
- If you turn on High Availability, you can also view the High Availability state of the node, and the reason for this state.

What to Do Next

Proceed to configure user assignments in System Topology.

Related Topics

Restart Cisco XCP Router Service, on page 56
Node Name Recommendations, on page 64
Node Creation and Movement Recommendations, on page 63
High Availability Deployments, on page 71
Intercluster Deployments, on page 21
Intercluster Peer Configuration, on page 123

Configure User Assignment in System Topology

Note This topic is only applicable if you have chosen to manually assign your users.

In system topology management GUI, you can manually unassign, assign or reassign users. You can assign users to a single node, and you can also distribute groups of users across the node, or nodes, in a cluster, or a given subcluster.

Before You Begin

- Read the user assignment recommendations topic.
- You may want to export users in bulk. Use the Bulk Administration Tool (BAT) to perform this procedure. Restriction
- You can only assign licensed users.
- If you turn on High Availability in a subcluster, note that you can only assign or move users to nodes in that subcluster that are not in a failover state. Valid node states are Normal and Running in Backup Mode.

Procedure

Step 1 Select **Cisco Unified CM IM and Presence Administration** > **System** > **Topology**.

Step 2 Perform one of the following actions:

- To assign users, choose **Assign Users**.
- To unassign or reassign users, choose **All Assigned Users** in the left pane of the system topology interface.

Step 3 Use the **Find User Assignment** window to find and display users.

Step 4 Perform one of the following actions:

a) Check the users that you wish to assign, and select **Assign Selected Users**.
b) Select all users, and select **Assign All Users**.

Step 5 Using the list boxes in the Change Assignment frame, specify your user assignment:

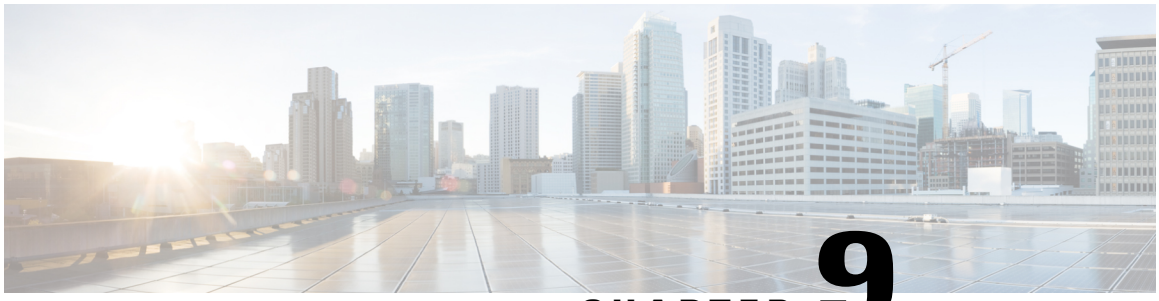
a) to a named node
b) to a named subcluster (auto-assigned)
c) to all subclusters (auto-assigned)
d) to nothing (unassigned)

Step 6 Select **Save**.

Tip Select **Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter** to verify the status of your topology configuration.

Related Topics

User Assignment, on page 10
User Assignment Mode Recommendations, on page 65
Turn On or Off High Availability for Subcluster, on page 75
Multinode Scalability and WAN Deployments, on page 17



CHAPTER 9

High Availability Deployment Configuration

- High Availability Deployments, page 71
- Turn On or Off High Availability for Subcluster, page 75
- Configure Advanced Service Parameters for Server Recovery Manager, page 77
- Perform Manual Failover to Backup Node, page 79
- Perform Manual Fallback to Primary Node, page 80
- Perform Manual Recovery of Subcluster, page 81

High Availability Deployments

High Availability Requirements

The IM and Presence Service supports High Availability at a subcluster level. Both nodes in the subcluster must be running the same version of IM and Presence Service software for High Availability to work.

High Availability Subcluster

IM and Presence Service supports High Availability in a subcluster meaning if a node in the subcluster fails, the Instant Message and Availability services from that node can failover to the second node in the subcluster.

You must manually turn on High Availability in a subcluster on the Cluster Topology interface on IM and Presence Service Administration interface. On the main Cluster Topology interface, the subcluster icon indicates that you have turned on High Availability on the subcluster.

A green tick beside the High Availability icon indicates that High Availability in the subcluster is running normally. A red “x” beside the High Availability icon indicates that the subcluster is in a failed state.

IM and Presence Service automatically detects failover in a subcluster by monitoring the heartbeat and monitoring the critical services on the peer node. When IM and Presence Service detects failover, it automatically moves all users to the backup node and supports automatic fallback to the primary node. From the Cisco Unified CM IM and Presence Administration interface, you can initiate a manual fallback to the primary node.

Note IM and Presence Service performs an automatic fallback when the backup activated node fails due to a critical service failure and the peer node is in the "Failed Over" state and supports the automatic recovery fallback.

To monitor and troubleshoot the status of the High Availability functionality on a subcluster, view the High Availability states that IM and Presence Service assigns to each node. If a failover occurs, on the node detail screen, IM and Presence Service marks the users that have failed over to the backup node.

Related Topics

Node States, Causes and Recommended Actions, on page 210

Failover Impact to Clients and Services

During failover to the backup node, availability and instant messaging services are temporarily unavailable on client applications. After failover is complete, the availability and instant messaging services become available on the client again when the client signs back in. Similarly, if fallback occurs, availability and instant messaging services are temporarily unavailable on client applications until fallback completes and the client signs back in. Cisco Jabber signs users back in automatically.

The impact of failover on temporary ad hoc chat messages depends on the particular client application. On Cisco Jabber, any ad hoc chat windows that were open before failover should display again after the failover is complete. However, if all of the users in a chat room automatically exit the chat room as part of a failover or fallback process, or if the ad hoc chat room is hosted on a failed node, the ad hoc chat windows will not display again after failover and a message is displayed explaining that the chat room was deleted. On all clients, any persistent chat rooms that users create on the failed node cannot be accessed again until recovery.

If Cisco Jabber is operating in softphone mode (the user is on a voice call) during failover, the voice call is not disconnected.

Automatic Failover Detection

IM and Presence Service uses these methods to automatically detect if a node fails:

- **Peer Heartbeat** - In a subcluster, each node sends heartbeat intervals to the other node to check if the node is up and running. If a node detects a loss of heartbeat in the peer node, the node initiates a failover. You can configure the heartbeat interval and the heartbeat timeout from the Service Parameters page on Cisco Unified CM IM and Presence Administration interface.
- **Monitor Critical Services** - Each node monitors a list of critical services. If the node detects that any critical service is not running for a configurable outage period (ninety seconds is the default value), it instructs the peer node to initiate a failover. You can configure this critical service delay from the Service Parameters page on Cisco Unified CM IM and Presence Administration interface. These are the list of critical services that the node monitors:
  - Cisco DB (internal IDS database)
  - Cisco Presence Engine (if you activate this service)
  - Cisco XCP Router
  - Cisco Message Archiver (if you integrate IM and Presence Service with a third-party off-board database, and you activate this service)

- Cisco SIP Proxy (if you configure SIP federation or you enable Partitioned Intradomain Federation and you activate this service)
- Cisco XCP SIP Federation Connection Manager (if you configure SIP federation, or enable Partitioned Intradomain Federation, and you activate this service)
- Cisco Presence Datastore
- Cisco Route Datastore (if you configure SIP federation or you enable Partitioned Intradomain Federation and you activate this service)

You can view the critical services that IM and Presence Service monitors for failover on the node details screen on the Cluster Topology interface. The critical services that IM and Presence Service monitors are marked in the "Monitored" column in the services list.

Note

- IM and Presence Service only detects a failover if a critical service is not running for the duration of the outage period. It does not detect a failover in the case where one or more critical services are not running during the outage period, but not for the duration of the outage period, for example, a rolling outage. In this case, IM and Presence Service generates alarms indicating that services are starting and stopping, and you can perform a manual failover on IM and Presence Service.
- If you manually stop a critical service, and the service is stopped for longer than the permitted outage period, failover will occur.

Prior to Release 8.6, if IM and Presence Service detects the situation where both nodes in the subcluster think they own the same user, both nodes go into a failed state, and you need to perform a manual recovery from the Cluster Topology interface. In IM and Presence Service Release 9.0(1) and later, manual recovery is not required. When the network issue is resolved, auto-recovery occurs without administrator intervention.

If manual recovery is required for another reason, you may experience IDS replication delays.

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.

Related Topics

Cisco Replication Watcher Service, on page 43

Automatic Fallback

IM 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.

Cisco Server Recovery Manager (SRM)

The Cisco Server Recovery Manager (SRM) on IM and Presence Service manages the failover between nodes in a subcluster. The Cisco Server Recovery Manager manages all state changes in a node; state changes are either automatic or initiated by the administrator (manual).

After you turn on High Availability in a subcluster, the Cisco Server Recovery Manager on each node establishes heartbeat connections with the peer node, and begins to monitor the critical processes.

The SRM is responsible for the user move operations after it detects that failover has occurred. It is the SRM on the peer node, not on the failed node, that performs the user move operation. For example, if node A fails, the SRM on node B performs the user move operation. The SRM throttles the number of users moved to the peer node, it moves the users in batches or iterations. You can configure the number of users that the SRM moves per iteration (the default value is 25). On failover, the SRM will move users that are signed in first, and then move users that are not signed in. Note that if you initiate a fallback or if an automatic fallback occurs, users that are not signed in are moved first, and then users that are signed in.

If the SRM is not turned on, it does not monitor any critical processes, nor does it monitor the heartbeat connections with the peer node.

Caution Before you turn on High Availability in a subcluster, you must configure the SRM service parameters to properly reflect your deployment.

Related Topics

High Availability Login Profiles, on page 235
Node State Definitions, on page 209

Manual Failover and Fallback

From the Cluster Topology interface, you can perform the following procedures:

- Initiate a manual failover for a subcluster. When you initiate a manual failover, the Cisco Server Recovery Manager stops the critical services on the failed node, and moves all users to the backup node.

- Initiate a manual fallback from the Cluster Topology interface, where the Cisco Server Recovery Manager restarts critical services on the primary node and moves users back to the primary node.
- Perform a manual recovery for a subcluster (when both nodes in the subcluster are in a failed state). When you perform a manual recovery, IM and Presence Service restarts the Cisco Server Recovery Manager service on both nodes in the subcluster.

High Availability and Intercluster Deployment Consideration

When failover occurs, the Intercluster Sync Agent is responsible for communicating the user move information to other clusters. The Intercluster Sync Agent runs on both the publisher and subscriber nodes in a cluster. In an Active-Standby configuration, if the publisher node fails or the Intercluster Sync Agent on the publisher node fails, the Intercluster Sync Agent on the subscriber node becomes Active and resumes synchronization, meaning the other clusters will continue to receive the information that users have moved to a different node. Intercluster presence and IM continue to work. Users that have failed over will receive availability information for remote users. Remote users continue to receive availability information and IMs from users that have failed over, and all IMs they send to a failed over user are delivered. When the publisher node recovers, the publisher falls back to Active mode and the subscriber returns to Standby mode.

Turn On or Off High Availability for Subcluster

Caution Before you turn on High Availability in a subcluster, you must configure the SRM service parameters to properly reflect your deployment, see topics related to High Availability client login profiles.

You have to manually turn on High Availability in a subcluster; IM and Presence Service does not turn on High Availability in a subcluster by default. You can turn on High Availability in a subcluster when:

- there are two nodes in the subcluster, and
- both nodes have IP addresses that are resolvable addresses, and
- both nodes are running IM and Presence Service Release 9.0 or higher.

You can either assign users to the nodes in the subcluster before or after you turn on High Availability for the subcluster.

Before You Begin

- Configure the subclusters and nodes in your network, and assign nodes to the subclusters.
- Make sure critical services are running on both nodes in the subcluster before you turn on high- availability in a subcluster. If one or more critical services are not running on a node, when you turn on High Availability, that node will failover to the backup node. When one or more critical services are not running on one node in a subcluster, but all critical services are running on the second node, the subcluster will go into a failed state after you turn on High Availability.

Restriction

You can only turn on High Availability in a subcluster when there are two nodes assigned to that subcluster. The High Availability checkbox does not display when there are no nodes, or one node, assigned to the subcluster.

Procedure

Step 1 **Cisco Unified CM IM and Presence Administration** > **System** > **Cluster Topology.**

Step 2 Select the **edit** link on the appropriate subcluster.

Step 3 Check **Enable High Availability**.

Note To turn off High Availability for the sublcluster, uncheck **Enable High Availability**.

Step 4 Select **Save**.

IM and Presence Service displays the following information about High Availability for the subcluster

Field	Description
Monitored Node	The node in the subcluster that IM and Presence is monitoring for failover detection.
Node State	The state of the node.
Node Reason	The reason for the node state.
Node Action	The action you can take to change the state of the node: • **Fallback** - This option is displayed for nodes that are in Idle or Failed Over states. Select to manually initiate a fallback to this node. • **Failover** - This option is displayed for nodes that are in Normal state. Select to manually initiate a failover to this node. • **Recovery** - This option is displayed if both nodes in the subcluster are in a failed state. Select to manually initiate a recovery of the subcluster where IM and Presence Service restarts the SRM service on both nodes.

Troubleshooting Tips

- When you turn on High Availability in a subcluster, IM and Presence Service restarts the Cisco Service Recovery Manager service and it begins to monitor for failover detection. To verify this service is running, select **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Network Services**.
- You can turn off High Availability in a subcluster, so the two nodes in the subcluster act as standalone nodes. You can only turn off High Availability when the nodes in the subcluster are not in a transition state (Failing Over, Falling Back). If you turn off High Availability in a subcluster when either node is in a failed over scenario (Failed Over, Failed), users that IM and Presence Service fails over to the backup node are homed to the backup node. IM and Presence Service will not move these users back to the primary node, they remain on the backup node.
- The System Troubleshooter indicates if there are any two node subclusters without High Availability turned on. Select **Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter**.

Related Topics

High Availability Login Profiles, on page 235
Node State Definitions, on page 209
Node States, Causes and Recommended Actions, on page 210

Configure Advanced Service Parameters for Server Recovery Manager

The following table describes the advanced service parameters you can configure for the Server Recovery Manager.

Table 8: Advanced Server Recover Manager Service Parameters

Parameter	Description	Additional Information
Service Port	This parameter specifies the port that Cisco Server Recovery Manager uses to communicate with its peer.	If you modify this parameter, IM and Presence Service restarts the Cisco Server Recovery Manager on all nodes in the cluster.
Admin RPC Port	This parameter specifies the port that Cisco Server Recovery Manager uses to provide admin RPC requests.	If you modify this parameter, IM and Presence Service restarts the Cisco Server Recovery Manager on all nodes in the cluster.
Critical Service Down Delay	This parameter determines the duration a critical service can be down before IM and Presence Service initiates an automatic failover.	If you change this value, this affects how long a critical service can be down before IM and Presence Service initiates an automatic failover.
Enable Automatic Fallback	This parameter turns automatic fallback on or off on IM and Presence Service.	This parameter is off by default.
Initialization Keep Alive (Heartbeat) Timeout	This parameter specifies the duration that the heartbeat is lost with the peer node (SRM) when the peer SRM restarts and is in the initialization state.	We recommend that you configure this value to at least twice the value of the Keep Alive (Heartbeat) Timeout in order to avoid unnecessary failovers.
Keep Alive (Heartbeat) Timeout	This parameter specifies the duration that the heartbeat is lost with the peer node (SRM) before IM and Presence Service initiates an automatic failover.	We recommend that you configure this value to at least twice the value of KeepAliveInterval value. If this value is too close to the KeepAliveInterval value, this can cause a failover to occur.
Keep Alive (Heart Beat) Interval	This parameter specifies the interval between keep alive (heartbeat) messages sent to the peer node.	N/A

Parameter	Description	Additional Information
Users Moved Per Iteration	This parameter specifies the number of users that IM and Presence Service moves for each iteration when it performs a failover or a fallback. There is a delay of one second between each iteration.	Increasing this value will shorten the failover time at the expense of CPU. Lowering the value will lengthen failover time, but have less impact on the CPU. **Caution** Before you configure the Users Moved Per Iteration parameter value, refer to the High Availability client login profiles.
Client Re-Login Lower Limit	This parameter specifies the minimum number of seconds which Cisco Jabber will wait before attempting to re-login to this IM and Presence Service node. This waiting time occurs due to the failure of a node or a critical service on a node. **Note** This parameter is per node.	**Caution** Refer to the High Availability client login profiles for guidelines on defining the client re-login lower and upper limits.
Client Re-Login Upper Limit	This parameter specifies the maximum number of seconds which Cisco Jabber will wait before attempting to re-login to this IM and Presence Service node. This waiting time occurs due to the failure of a node or a critical service on a node. **Note** This parameter is per node.	**Caution** Refer to the High Availability client login profiles for guidelines on defining the client re-login lower and upper limits.

Procedure

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

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

Step 3 Select **Cisco Server Recovery Manager** from the **Service** menu.

Step 4 Configure the service parameters.

Step 5 Select **Save**.

Related Topics

High Availability Login Profiles, on page 235

Perform Manual Failover to Backup Node

You can perform a manual failover to the backup node in the subcluster using the Cluster Topology interface. When you initiate a manual failover, the Cisco Server Recovery Manager stops the critical services on that node, and moves all users to the backup node.

The Cisco Server Recovery Manager stops the following critical services on the node:

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Router (this causes all XCP processes to stop)
- Cisco Client Profile Agent

The Cisco Server Recovery Manager then move all users to the backup node

Restriction

You can only initiate a failover for a node that is in “Normal” state.

Before You Begin

Make sure that these services are running on the Failing Over node:

- Cisco XCP Connection Manager service
- Cisco XCP Router
- Cisco Presence Engine

Procedure

Step 1 **Cisco Unified CM IM and Presence Administration** > **System** > **Cluster Topology.**

Step 2 Select the **edit** link on the appropriate subcluster.

Step 3 Select **Failover** in the Node Action column.

Step 4 Select **Ok** to confirm the failover operation.

Step 5 To verify the failover operation is complete and successful:

a) When the failover operation is in progress, the primary node should be in the “Failing Over” state, and the backup node should be in the “Taking Over” state. When the failover operation is complete, check that the backup node is in the state “Running in Backup Mode”, and the primary node is in “Idle” state. If the failover is unsuccessful, and the nodes are in a failed state.

b) Check that the users have failed over to the backup node:

- On the subcluster details screen, check that all users are now assigned to the backup node, and no users are assigned to the primary node.
- On the node details screen, the “Failed Over” column indicates the users that have failed over to the backup node.

Related Topics

Node States, Causes and Recommended Actions, on page 210

Perform Manual Fallback to Primary Node

You can perform a manual fallback to the primary node in the Cluster Topology interface. When you initiate a manual fallback, the Cisco Server Recovery Manager restarts any critical services that are not already running on the primary node, and moves the failed over users back to the primary node.

When you manually initiate a fallback, the Cisco Server Recovery Manager restarts the following services on the primary node (if they are not already running):

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Router
- Any XCP services that were activated
- Cisco Client Profile Agent

The Cisco Server Recovery Manager then moves all failed over users back to the primary node.

Restriction

You can only initiate fallback for a node that is in 'Idle' or 'Failed Over' state.

Procedure

Step 1 **Cisco Unified CM IM and Presence Administration** > **System** > **Cluster Topology.**

Step 2 Select the **edit** link on the appropriate subcluster.

Step 3 Select **Fallback** in the Node Action column.

Step 4 Select **Ok** to confirm the fallback operation.

Step 5 To verify the fallback operation is complete and successful:

a) When fallback operation is in progress, the primary node should be in the "Taking Back" state, and the backup node should be in the "Falling Back" state. When the fallback operation is complete, check that both nodes are in 'Normal' state. If the fallback is unsuccessful, and the nodes are in a failed state.

b) Check that the users have fallen back to the primary node.

- On the subcluster details screen, check that all users are now assigned to the primary node, and no users are assigned to the backup node.
- On the node details screen, the "Failed Over" column should be empty.

Related Topics

Node States, Causes and Recommended Actions, on page 210

Perform Manual Recovery of Subcluster

When you perform a manual recovery of a subcluster, IM and Presence Service restarts the Cisco Server Recovery Manager service on both nodes in the subcluster.

Restriction

You can only initiate a recovery for a subcluster if both nodes are in a failed state.

Procedure

Step 1 **Cisco Unified CM IM and Presence Administration** > **System** > **Cluster Topology.**

Step 2 Select the **edit** link on the appropriate subcluster.

Step 3 Select **Recovery** in the Node Action column.

Step 4 Verify the status of the subcluster after you perform the manual recovery.

Troubleshooting Tips

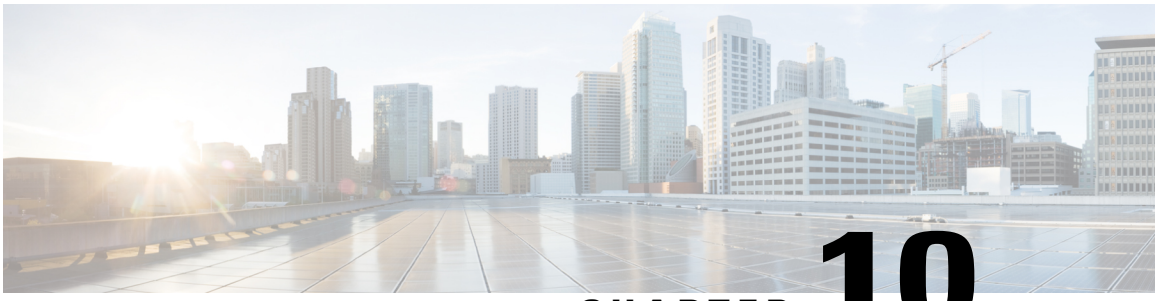
In prior releases, if two nodes in the subcluster think that they own the same user, both nodes will go into a failed state, and you had to perform a manual recovery from the Cluster Topology interface. In this release manual recovery is not required. When the network issue is resolved, auto-recovery occurs without administrator intervention.

If manual recovery is required for another reason, you may experience IDS replication delays. You can check the status of the IDS replication on a node using this CLI command:

Utils dbreplication runtimestate

Related Topics

Node States, Causes and Recommended Actions, on page 210



CHAPTER 10

IP Phone Presence Setup

- Static Route Configuration on IM and Presence Service, page 83
- Presence Gateway Configuration on IM and Presence Service, page 88
- Configure SIP Publish Trunk on IM and Presence Service, page 89
- Configure Cluster-Wide DNS SRV Name for SIP Publish Trunk, page 89

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
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. 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. Wildcard Usage You can use "." as a wildcard for a single character and "*" as a wildcard for multiple characters. 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. For phones: • 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. • An asterisk can only exist at the end of the pattern. For IP addresses and host names: • You can use an asterisk as part of the a host name. • The dot acts as a literal value in a host name. An escaped asterisk sequence, *, matches a literal * and can exist anywhere.
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. 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. 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.

Field	Description
Route Type	Specifies the route type: User or Domain. The default value is user. 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. Value range: 1-65535
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. Value range: 1-65535 **Example:** Consider these three routes with associated priorities and weights: • 1, 20 • 1, 10 • 2, 50 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. 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 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 185
Presence Gateway Configuration Option, on page 88

Configure SIP Publish Trunk on IM and Presence Service

When you turn on this setting, Cisco 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 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.

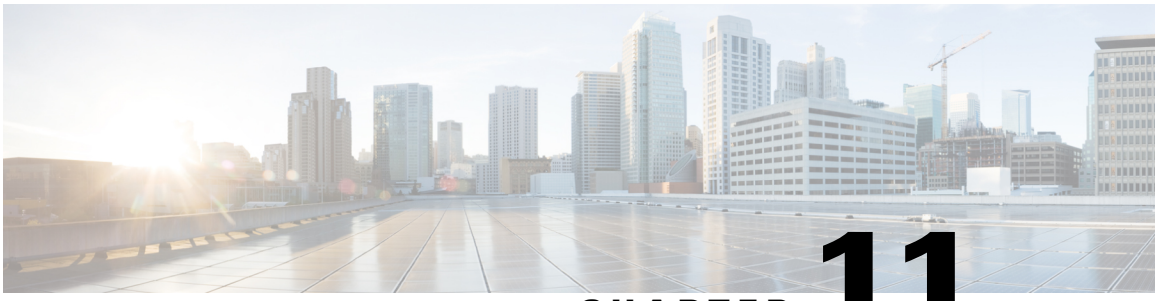
Step 3 Choose **Cisco SIP Proxy** from the Service menu.

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 19
Scalability Options for Deployment, on page 18



CHAPTER 11

LDAP Directory Integration

- LDAP Server Name, Address, and Profile Configuration, page 91
- LDAP Directory Integration with Cisco Unified Communications Manager Task List, page 91
- LDAP Directory Integration for Contact Searches on XMPP Clients, page 96

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 7: 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. **Tip** You must upload the LDAP SSL certificate as a tomcat-trust certificate on Cisco Unified Communications Manager Release 8.x and later.
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. **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. **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

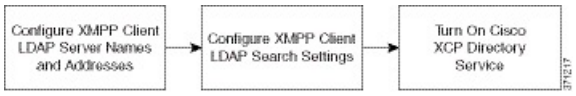
These topics describe how to configure the LDAP settings on IM and Presence Service to allow users of third-party XMPP client to search and add contacts from the LDAP directory.

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.

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

Figure 8: LDAP Directory Integration for Contact Searches on XMPP Clients Workflow



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. **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. **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.
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. **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.

Before You Begin

Obtain the hostnames or IP addresses of the LDAP directories.

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.

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 92
Configure Secure Connection Between IM and Presence Service and LDAP Directory, on page 95

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: • Microsoft Active Directory • 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. 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.
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. If you use Microsoft Active Directory, the default value is sAMAccountName.
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.

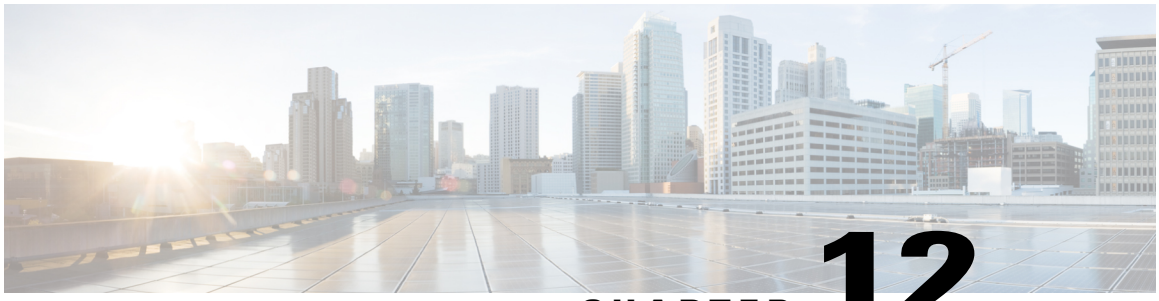
Procedure

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 12

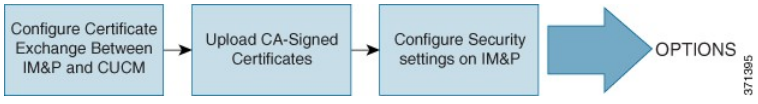
Security Configuration on IM and Presence Service

- Security Setup Task List, page 101
- Create Login Banner, page 102
- IM and Presence Service Certificate Types, page 103
- Certificate Exchange Configuration Between IM and Presence Service and Cisco Unified Communications Manager, page 104
- Single-Server CA Signed Certificate Upload to IM and Presence Service , page 107
- Delete Self-Signed Trust Certificates , page 117
- SIP Security Settings Configuration on IM and Presence Service, page 119
- XMPP Security Settings Configuration on IM and Presence Service, page 120

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 9: 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: • Import Cisco Unified Communications Manager certificate to IM and Presence Service node, and then restart the SIP proxy service. **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**. • Download the certificate from IM and Presence Service, and then upload the certificate to Callmanager-trust on Cisco Unified Communications Manager. • Restart the Cisco Unified Communications Manager service. **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. • tomcat certificate • cup-xmpp certificate • cup-xmpp-s2s certificate **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. 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, IM and Presence Disaster Recovery System, and Cisco Unified CM IM and Presence User Options.

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.

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 for Client Applications on IM and Presence Service

Client	Certificate
SIP client (Cisco Unified Communications Manager)	tomcat
XMPP client (Cisco Jabber, third-party client)	cup-xmpp

Table 17: Certificate Types for IM and Presence Services

Service	Certificate	Certificate Trust Store	Notes
SIP Proxy	cup	cup-trust	
Presence Engine	cup	cup-trust	
SOAP	tomcat	directory-trust	
AXL	tomcat	directory-trust	
LDAP	tomcat	directory-trust	LDAP uses the tomcat certificate because directory/directory-trust is now tomcat/ttrust.

Service	Certificate	Certificate Trust Store	Notes
Microsoft Exchange		cup-trust	
Microsoft Lync/OCS/LCS Call Control	cup	cup-trust	
SIP Federation	cup	cup-trust	
XMPP Federation	Cup-xmpp-s2s	cup-xmpp-trust	The trust certificates for cup-xmpp-s2s are stored in cup-xmpp-trust along with the general XMPP trust certificates.

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 95

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

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

If you migrate from self-signed to CA-signed certificates, the original self-signed certificates persist in the service trust store of the IM and Presence Service node. Leaving the original self-signed certificates in the service trust store is not an issue because no service will present them. However, if needed, you can delete these trust store certificates.

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.

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 18: 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. 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.
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.

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 121

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.

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
Cisco Replication Watcher Service, on page 43

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:

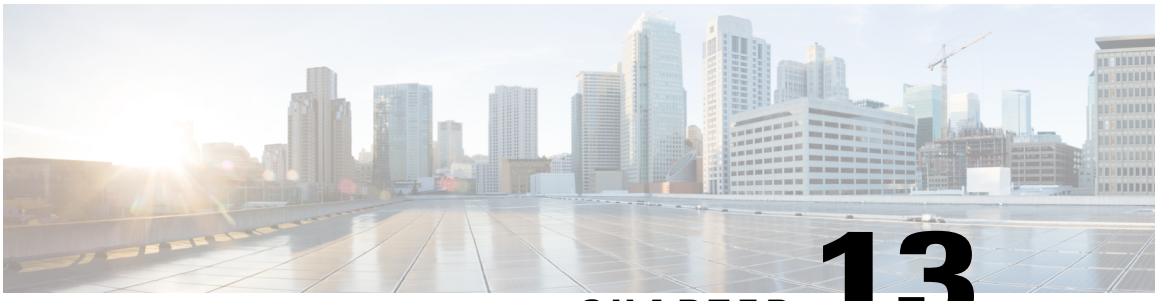
- Cisco XCP Connection Manager - Turn on this service if you are integrating XMPP clients, or XMPP-based API clients on IM and Presence Service.
- Cisco XCP Authentication Service - Turn on this service if you are integrating XMPP clients, or XMPP-based API clients, or XMPP-based API clients on IM and 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



CHAPTER 13

Intercluster Peer Configuration

- Prerequisites for Intercluster Deployment, page 123
- Intercluster Peer Configuration, page 124

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.

Related Topics

Multinode Update Configuration After Deployment, on page 44

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 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.

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 to create the remote intercluster peer, and then restart the Cisco XCP Router service on all nodes in the remote cluster.

Tip If you configure the intercluster peer connection before the Sync Agent completes the user synchronization from Cisco 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 56
Node Name Value for Intercluster Deployments, on page 22
IM and Presence 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 17

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**.

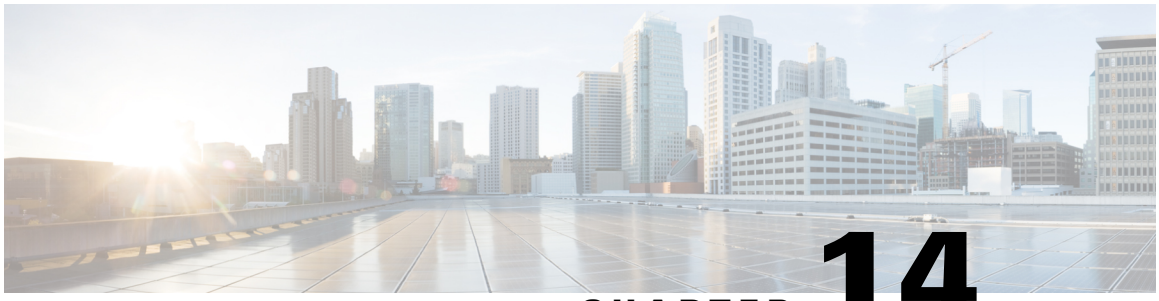
Step 4 Click **OK**.

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.

PART III

Feature Configuration

- Availability and Instant Messaging on IM and Presence Service Configuration , page 131
- Single Sign-On Setup, page 137



CHAPTER 14

Availability and Instant Messaging on IM and Presence Service Configuration

- Availability Setup on IM and Presence Service, page 131
- IM Setup On IM and Presence Service, page 134

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**.

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 either the Cisco Jabber client and the Cisco Unified CM IM and Presence User Options interface.

- 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**.

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 56

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.

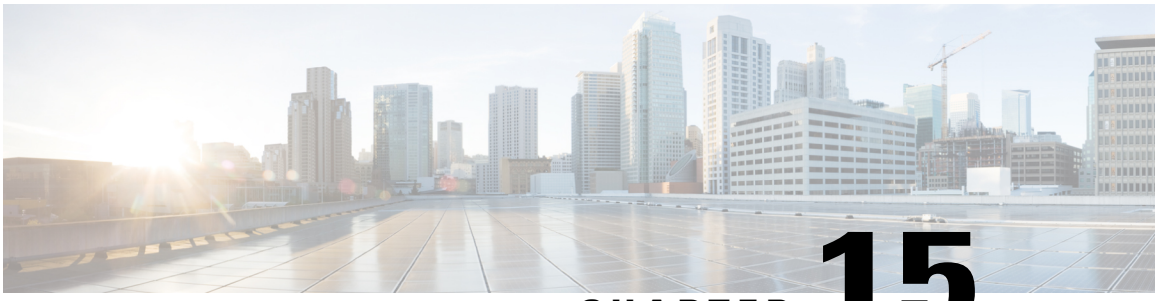
Procedure

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**.



CHAPTER 15

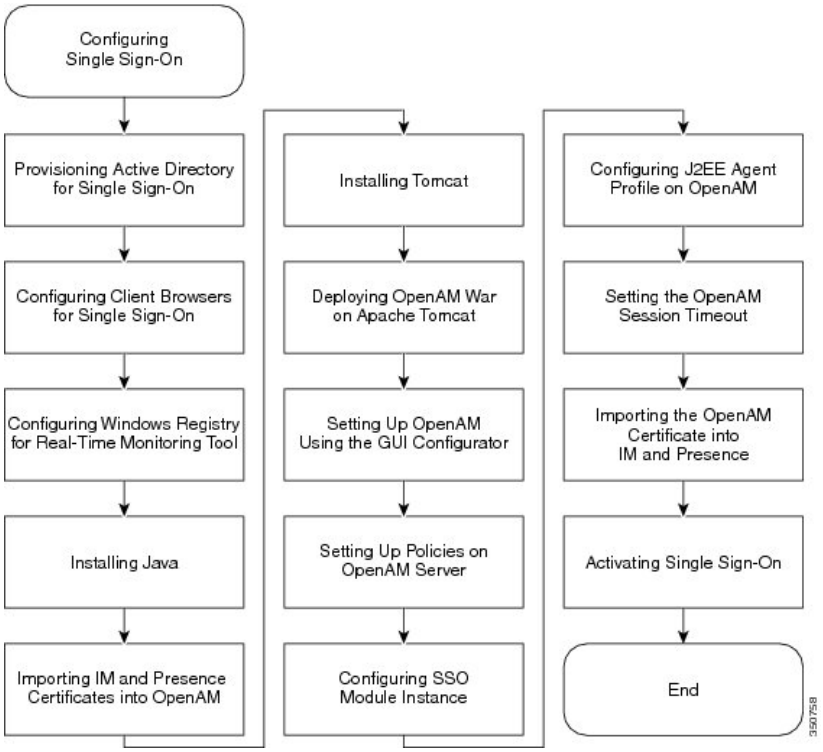
Single Sign-On Setup

- Single Sign-On Setup Task List, page 138
- Single Sign-On Setup Preparation, page 140
- Single Sign-On Setup and Management Tasks, page 142

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 10: 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. **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).

Item	Task
4	Install Java Runtime Environment (JRE). **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. **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.
14	Activate Single Sign-On. **Caution** 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

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

Component	Version
Desktop Operating System for end user clients	Windows 7 Professional (SP1)
OpenAM	OpenAM Release 9.5.4 RC1 http://forgerock.org/openam-archive.html For more information: 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 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

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.

Parameter	Description
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 140

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 140

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 I.

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\jdkl.7.0_03\bin\keytool.exe" -genkey -alias tomcat -keyalg RSA -validity 1825 -keystore C:\keystore -ext BC:c=ca:true`
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.

Note The keytool command with -ext option requires JDK 7. Using the -ext option with the above value results in an OpenAM/Tomcat certificate with the CA flag set to True. The CA flag must be set to True or the Cisco Unified IM and Presence Operating System Administration interface may fail to upload the certificate into the tomcat-trust trust store. For more information, see topics related to importing OpenAM certificates into IM and Presence Service.

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 140
Import OpenAM Certificate Into IM and Presence Service, on page 162

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\jdk1.7.0_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.

Related Topics

Third-Party Software and System Requirements for Single Sign-On, on page 140

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 140

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. For example, `HTTP/server1.cisco.com@CISCO.COM` (using openAM server name and domain).

Parameter	Description
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. 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. **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. Choose **Centralized**
Server URL	The complete URL of the OpenAM server. For example, `https://<OpenAM FQDN>:8443/opensso` where `opensso` is the name of the OpenAM WAR file with the .war extension removed
Agent URL	The URL of the J2EE Policy Agent to which OpenAM publishes notifications. For example, `https://<IMP FQDN>:8443/agentapp` **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 Unified CM IM and Presence User Options	`/cupuser/WEB-INF/pages/logoncontrol.jsp`

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.

Related Topics

Enable Single Sign-On Using GUI, on page 166

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 141
Certificate Failure, on page 222

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 • Cisco Unified CM IM and Presence Administration • IM and Presence Serviceability • 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. The default administrator application user that was created at the time of installation has the following: Groups: • Standard Audit Users • Standard IM and Presence Service Super Users • Standard RealtimeAndTraceCollection Roles: • Standard AXL API Access • Standard Audit Log Administration • Standard CCM Admin Users • Standard CCMADMIN Administration • Standard CUReporting • Standard RealtimeAndTraceCollection* • Standard SERVICEABILITY Administration 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. To view the default application user on IM and Presence Service, choose **Cisco Unified CM IM and Presence Administration** > **User Management** > **Application User** > **Find**. Choose the default application user (that was created during install) to view their details. To assign an end user to these groups on IM and Presence Service, choose **Cisco Unified CM IM and Presence Administration** > **User Management** > **Access Control Groups** > **Find**. Choose a group and click **Add End Users**. Search for the desired end user, choose the user, and click **Add Selected**.
Cisco Unified IM and Presence User Options	Ensure that the end users are members of the Standard CCM End User group on the corresponding Cisco Unified Communications Manager node.

Cisco Unified IM and Presence Operating System Administration • IM and Presence Operating System Administration • 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. 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. 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 CM IM and Presence User Options – Enables SSO for End User Options.
- 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.

Note You can enable SSO using either the GUI, as described in this procedure, or the CLI. For information about how to enable SSO using the CLI, see the **utils sso enable** command in the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

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.

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. The default administrator application user that was created at the time of installation has the following: Groups: • Standard Audit Users • Standard IM and Presence Super Users • Standard RealtimeAndTraceCollection Roles: • Standard AXL API Access • Standard Audit Log Administration • Standard CCM Admin Users • Standard CCMADMIN Administration • Standard CUReporting • Standard RealtimeAndTraceCollection* • Standard SERVICEABILITY Administration 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. To view the application users on IM and Presence, select **Cisco Unified CM IM and Presence Administration** > **User Management** > **Application User** > **Find**. Select a user to view their details.
Cisco Unified IM and Presence User Options	Ensure that passwords exist for the end users and that they are aware of their password values. This information is required by each end user to access the application in question.
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 167
Disable Single Sign-On, on page 169
Install Tomcat, on page 151

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**.

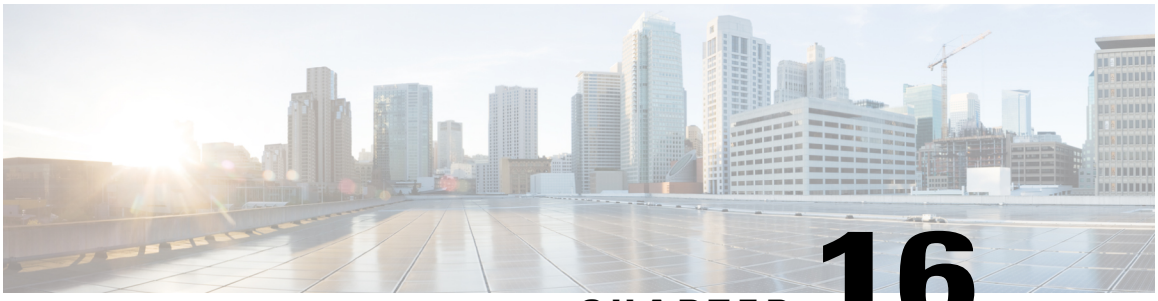
Step 7 Retrieve the logs using Cisco Unified Real Time Monitoring Tool for IM and Presence Service by browsing and downloading the logs for the Cisco SSO component.

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, page 173
- End User Setup and Handling, page 183
- User Migration, page 193
- Multilingual Support Configuration For IM and Presence Service, page 199



CHAPTER 16

Chat Setup and Management

- Chat Deployments, page 173
- Chat Administration Settings, page 176
- Chat Node Alias Management, page 178

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). 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: • change the Domain from cisco.com to linksys.com and use conference-1-mycup.linksys.com instead of conference-1-mycup.cisco.com.

	• 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 **System** > **Cluster Topology** > **Settings**. **2** Edit the domain using the Cluster Topology interface and change it to linksys.com.
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

Cluster Topology Configuration on IM and Presence Service, on page 63
IM and Presence Service Default Domain Configuration

Chat Deployment Scenario 3

Deployment Scenario:	You: • want to change the Cluster ID from mycup to ireland to use conference-1-ireland.cisco.com instead of conference-1-mycup.cisco.com. • 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** > **System** > **Cluster Topology** > **Settings**. **2** Edit the Cluster ID and change it to ireland. **3** Choose **Messaging** > **Group Chat Server Alias Mapping**. **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: • delete a node associated with an existing alias from the System Topology, for example, conference-3-mycup.cisco.com. • add a new node with a new node ID (node id: 7) to the System Topology, for example, conference-7-mycup.cisco.com. • maintain the address of chat rooms that were created using the old alias.
Configuration Steps:	Option 1 **1** Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **Group Chat Server Alias Mapping**. **2** Click **Add New** to add the additional alias, conference-3-mycup.cisco.com. Option 2 **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). **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. Option 1 • If you add an additional alias, the node is addressable via both aliases, conference-7-mycup.cisco.com and conference-3-mycup.cisco.com. Option 2 • 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 Deployment Scenario 5

Deployment Scenario:	You want to: • change the Cluster ID from mycup to ireland to use conference-1-ireland.cisco.com instead of conference-1-mycup.cisco.com. • only maintain chat room addressing via the old alias (does not need to associate nodes with the new system-generated alias).
Configuration Steps:	**1** Log in to **Cisco Unified CM IM and Presence Administration**, choose **System** > **Cluster Topology** > **Settings**.

	2 Edit the Cluster ID and change it to ireland. 3 Choose **Messaging** > **Group Chat and Persistent Chat** and turn off the new system-generated alias, conference-1-ireland.cisco.com. (This is on by default). 4 Choose **Messaging** > **Group Chat Server Alias Mapping**. 5 Deletes the new alias conference-1-ireland.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. When you turn off the new system-generated alias, conference-1-ireland.cisco.com reverts to a standard, editable alias listed under Group Chat Server Aliases. Because (in this example) the administrator has no need to maintain the new alias address, it is appropriate to delete it. 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 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 56

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 56

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** > **Cluster 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 Cluster Topology, chat rooms created using the old alias may not be addressable unless you take further action.

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 173

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**.

Step 3 The **Number of messages in chat history displayed for new conference participants** setting controls the number of instant messages from the recent message history that IM and Presence Service pushes to the client application of a user when that user joins a chat room. Increase this number if you want to display more text message history to users.

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
- The **Number of messages in chat history displayed for new chat participants** setting updates dynamically; You do not need to restart the Cisco XCP Text Conference Manager service.

Related Topics

Chat Deployment Scenario 1, on page 173

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 **System** > **Cluster Topology: 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 173

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

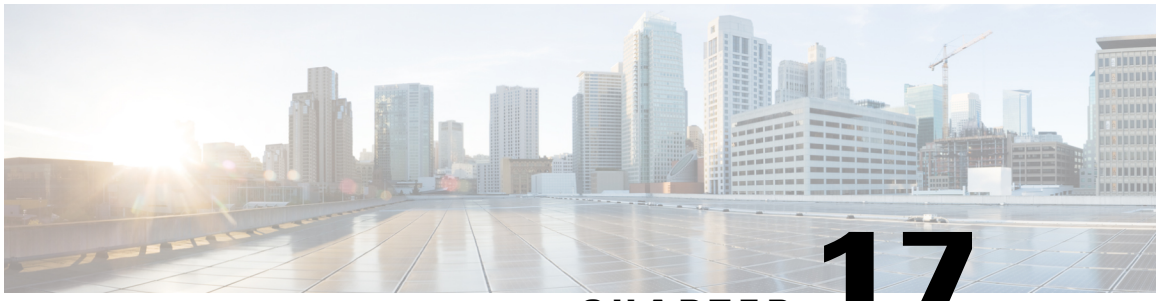
Step 1 Log in to **Cisco Unified IM and Presence Serviceability**, choose **Tools** > **Control Center - Feature Services**.

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.



CHAPTER 17

End User Setup and Handling

- End User Handling on IM and Presence Service, page 183
- Authorization Policy Setup On IM and Presence Service, page 183
- Bulk Export User Contact Lists, page 186
- Bulk Import Of User Contact Lists, page 187

End User Handling on IM and Presence Service

You can setup the authorization policy for IM and Presence Service end users and perform bulk user contact list imports and exports.

To set up users on IM and Presence Service, see topics related to configuring user assignments using Common Topology to setup users.

Related Topics

Configure User Assignment in System Topology, on page 69

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 either the Cisco Jabber client or the Cisco Unified CM IM and Presence User Options interface. 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.

On the Cisco Unified CM IM and Presence User Options interface, the user can also choose an “ask me” setting so that the user is prompted to set their own Allow/Block policy for external contacts (except those external contacts that a user explicitly adds to their Allowed/Blocked list).

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 56
Chat Configuration on IM and Presence Service

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 subcluster to a CSV data file. You can then use BAT to import the user contact lists to another node or subcluster 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.
User Domain	The Presence domain of the IM and Presence Service user.
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. 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. 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 27: Description of Input File Parameters

Parameter	Description
User ID	This is a mandatory parameter. The user ID of the IM and Presence Service user. It can have a maximum 132 characters.

Parameter	Description
User Domain	This is a mandatory parameter. The Presence domain of the IM and Presence Service user. It can have a maximum of 128 characters.
Contact ID	This is a mandatory parameter. The user ID of the contact list entry. It can have a maximum of 132 characters.
Contact Domain	This is a mandatory parameter. The Presence domain of the contact list entry. The following restrictions apply to the format of the domain name: • Length must be less than or equal to 128 characters • Contains only numbers, upper- and lowercase letters, and hyphens (-) • Must not start or end with hyphen (-) • Length of label must be less than or equal to 63 characters • 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.
Group Name	This is a mandatory parameter. 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 subcluster 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 server 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 132
Configure Maximum Number of Watchers Per User, on page 133

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.

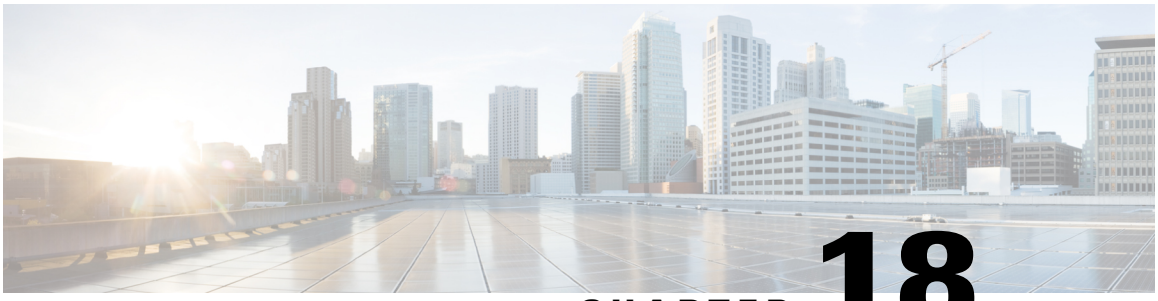
Procedure

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.



CHAPTER 18

User Migration

- User Migration Between IM and Presence Service Clusters, page 193

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. Export the contact lists of the migrating users from their current home cluster.
3. Disable the migrating users for IM and Presence Service and Cisco Jabber on their current home cluster from Cisco Unified Communications Manager.
4. 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.
5. If LDAP Sync is not enabled on Cisco Unified Communications Manager, manually provision the migrating users on Cisco Unified Communications Manager.
6. Enable users for IM and Presence Service and Cisco Jabber.
7. 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 IM and Presence Administration** > **System** > **Cluster Topology**.

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.

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 197

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.

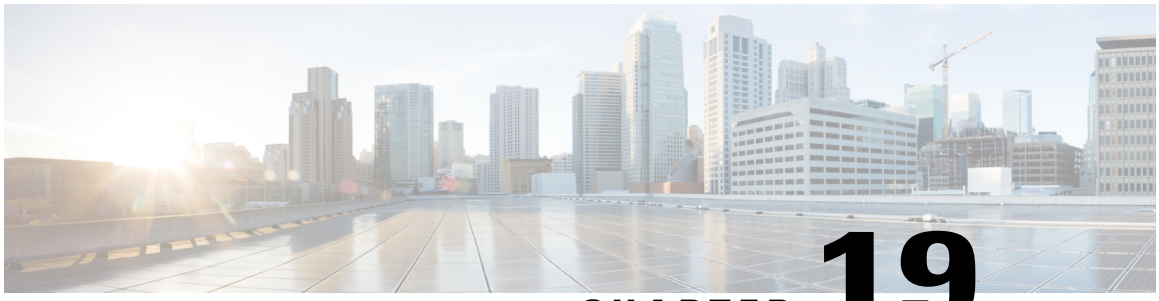
Step 2 Run the import contact list job.

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 19

Multilingual Support Configuration For IM and Presence Service

- Install Locale Installer on IM and Presence Service, page 199
- Error Messages, page 201
- Localized Applications, page 203

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 Cisco Unified Communications Manager user options pages 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.

Note IM and Presence Service does not currently support Safari browser.

a) If you use Internet Explorer Version 6.x, perform the following steps:

1. Choose **Tools** > **Internet Options**.
2. Choose the General tab.
3. Click **Languages.**
4. Use the Move Up button to move your preferred language to the top of the list.
5. Click **OK**.

b) If you use Mozilla Firefox Version 3.x, perform the following steps:

1. Choose **Tools** > **Options**.
2. Choose the Content tab.
3. Click **Choose** in the Languages section of the window.
4. Use the Move Up button to move your preferred language to the top of the list.
5. Click **OK**.

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 28: 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.
[LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maDialogs_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maMessages_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maGlobalUI_<ll>_<CC>.properties.Checksum. [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.

Message	Description
[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. 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 registration failed	The locale installer could not register with the Disaster Recovery System. A backup or restore record will not include the locale installer. Record the installation log and contact Cisco TAC.
[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.
[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. **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. **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. **Note** Manual reapplication of the locale installer will restore the locale fully.

Message	Description
[LOCALE] Failed to build script to reinstall COP files!	The platform could not dynamically create the script used to reinstall locales. **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 29: List of Localized Applications and Supported Languages

Interface	Supported Languages
End User Applications	
Cisco Unified CM IM and Presence User Options	

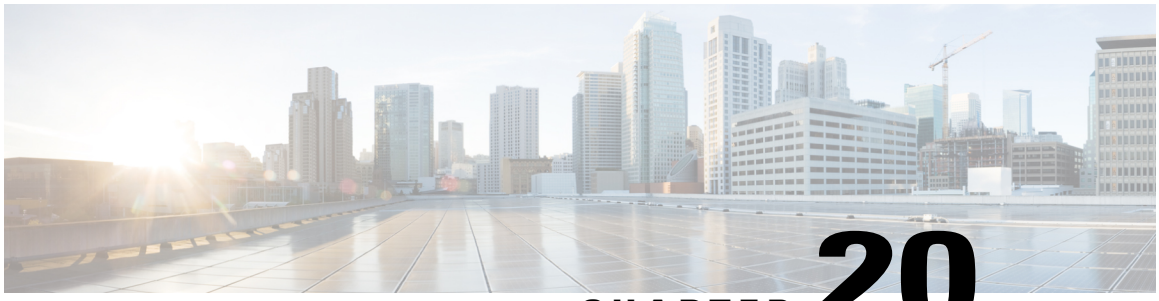
Interface	Supported Languages
End User Applications	
	Arabic (Algeria, Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Morocco, Oman, Qatar, Saudi Arabia, Tunisia, United Arab Emirates, Yemen) Bulgarian Catalan (Spain) Chinese (China, Hong Kong, Taiwan) Croatian Czech (Czech Republic) Danish (Denmark) Dutch (Netherlands) English Estonian (Estonia) Finnish (Finland) French (France) German (Germany) Greek (Greece) Hebrew (Israel) Hungarian (Hungary) Italian (Italy) Japanese (Japan) Korean (Korean Republic) Latvian (Latvia) Lithuanian (Lithuania) Norwegian (Norway) Polish (Poland) Portuguese (Brazil, Portugal) Romanian (Romania) Russian (Russian Federation) Serbian (Republics of Montenegro and Serbia) Slovak (Slovakia) Slovenian (Slovenia) Spanish (Columbia and Spain) Swedish (Sweden) Thai (Thailand)

Interface	Supported Languages
End User Applications	
	Turkish (Turkey)
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, page 209
- Troubleshooting Single Sign-On, page 217
- Traces Used To Troubleshoot IM and Presence Service, page 225



CHAPTER 20

Troubleshooting High Availability

- Node State Definitions, page 209
- Node States, Causes and Recommended Actions, page 210

Node State Definitions

The following table describes the different node states, and associated reasons. You can view the state of an existing node by either viewing the node details or the subcluster details on the Cluster Topology interface.

Note These fields are only displayed on the Cluster Topology interface if you turn on High Availability in a subcluster.

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 from the Cluster Topology 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 from the Cluster Topology 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.

State	Description
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 stable 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 from the Cluster Topology interface.
Failed Over with Critical Services Not Running	This is a stable 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 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	State unknown.

Node States, Causes and Recommended Actions

The following table describes the node states, reasons, causes, and recommended actions for failed states.

Table 30: Node High Availability States, Causes and Recommended Actions

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Normal	Normal	Normal	Normal	High Availability is running on both nodes in the subcluster. Subcluster is running normally (it is in non failover mode). The critical services on both nodes in the subcluster are running.
Failing Over	On Admin Request	Taking Over	On Admin Request	The administrator initiates 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 (initiated by the administrator) is complete.

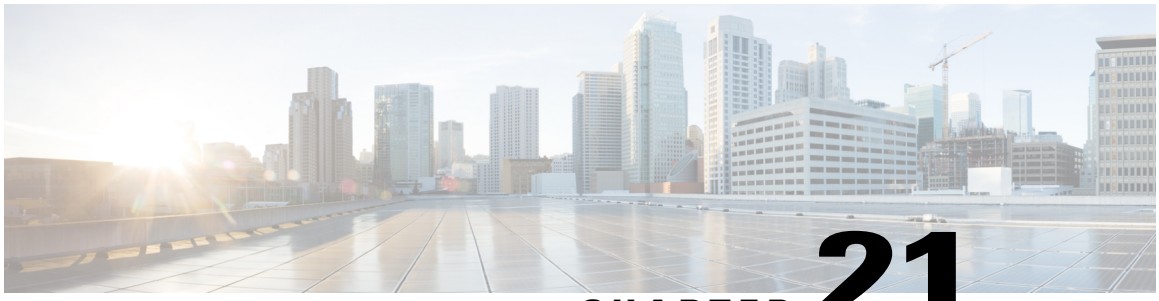
Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Taking Back	On Admin Request	Falling Back	On Admin Request	The administrator initiates a manual fallback from node 2 to node 1. The manual fallback is in progress.
Idle	Initialization	Running in Backup Mode	On Admin 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 restarts both nodes in the subcluster, or restarts the SRM service on both nodes in the subcluster, while the subcluster was in manual failover mode (failover initiated by the administrator).
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.
Failed Over	Initialization or Critical Services Down	Running in Backup Mode	Critical Service Down	Node 1 transitions to Failed Over state when: • Critical service(s) come back up due to reboot of node 1, or • The administrator starts critical service(s) on node 1 while node 1 is in "Failed Over with Critical Services Not Running" state 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 subcluster to Normal state.

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
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 performs an automatic failover to node 2. **Recommended Actions:** **1** Check what critical services are down on node 1, and try to start these services manually. **2** If the critical services on node 1 do not start, reboot node 1. **3** After the reboot and when all the critical services are running, perform a manual fallback to restore the nodes in the subcluster to 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 performs an automatic failover to node 2. **Recommended Actions:** **1** Reboot Node 1. **2** After the reboot and when all the critical services are running, perform a manual fallback to restore the nodes in the subcluster to Normal state.
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 subcluster is taking back from the other node. **Recommended Actions:** (on the node that is taking back) **1** Check what critical services are down on the node. To start these services manually, select **Recovery** on the subcluster details screen. **2** If the critical services do not start, reboot the node. **3** After the reboot and when all the critical services are running, perform a manual fallback to restore the nodes in the subcluster to Normal state.

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Running in Failed Mode	Critical Service Down	Running in Failed Mode	Critical Service Down	Critical services go down while a node in subcluster is running in backup mode for the other node. **Recommended Actions:** **1** Check what critical services are down on backup node. To start these services manually, select **Recovery** on the subcluster details screen. **2** If the critical services do not start, reboot the subcluster.
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 its heartbeat with node 1. IM and Presence performs an automatic failover to node 2. Recommended Action: (If node 1 is up) **1** Check and repair the network connectivity between nodes in the subcluster. When you reestablish the network connection between the nodes, the node may go into a failed state. Select **Recovery** on the subcluster details screen to restore the nodes in the subcluster to Normal state. **2** Start the SRM service, and perform manual fallback to restore the nodes in the subcluster to Normal state. (If the node is down) **3** Repair/Power up node 1. **4** When node is up and all critical services are running, perform manual fallback to restore the nodes in the subcluster to Normal state.

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Node 1 is down (due to possible power down, hardware failure, shutdown, reboot)		Running in Backup Mode	Peer Reboot	IM and Presence performs an automatic failover to node 2 due to possible hardware failure/power down/restart /shutdown of Node 1. Recommended Action: **1** Repair/Power up node 1. **2** When node is up and all critical services are running, perform manual fallback to restore the nodes in the subcluster to Normal state.
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. Recommended Action: When node1 is up and all critical services are running, perform manual fallback to restore the nodes in the subcluster to 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 taking over process. **Recommended Action:** Possible database error. Select **Recovery** on the subcluster details screen. If that doesn't resolve the issue, reboot the subcluster.
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. **Recommended Action:** Possible database error. Select **Recovery** on the subcluster details screen. If that doesn't resolve the issue, reboot the subcluster.
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. **Recommended Action:** Select **Recovery** on the subcluster details screen. If that does not resolve the issue, reboot the subcluster.

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
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 subcluster. 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 subcluster. Auto-recovery operation automatically occurs and all users are moved over to the peer node.



CHAPTER 21

Troubleshooting Single Sign-On

- Security Trust Error Message, page 217
- "Invalid Profile Credentials" Message, page 218
- "Module Name Is Invalid" Message, page 218
- "Invalid OpenAM Access Manager (Openam) Server URL" Message, page 218
- Web Browser Indicates a 401 Error, page 219
- Web Browser Indicates a 403 Error or Displays a Blank Screen , page 219
- "User is not Authorized to Perform this Function" Error, page 219
- Web Browser Indicates an HTTP 404 Error , page 219
- Web Browser Indicates an HTTP 500 Error or Displays a Blank Screen, page 220
- "Authentication Failed" Message, page 220
- Web Browser Displays OpenAM Login Screen, page 221
- Web Browser Displays IM and Presence Service Login Screen, page 221
- Internet Explorer Prompts for Username and Password, page 221
- "User has no profile on this organization" Message, page 222
- Problems Enabling SSO, page 222
- Certificate Failure, page 222

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 that 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 or CLI 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 146

"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 159

"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 158

"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 or CLI 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 143

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 156

"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 accessing the User Options web application is failing, ensure that the user is a member of the *Standard CCM End Users* group on the corresponding Cisco Unified Communications Manager node. If access to any other IM and Presence Service web applications is failing, ensure that the user is a member of the *Standard CUP 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 156
Set Up J2EE Agent Profile On OpenAM Server, on page 159

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 159

"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 158

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 159

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 159

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 143

"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 155

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 or the IM and Presence Administration CLI, 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.

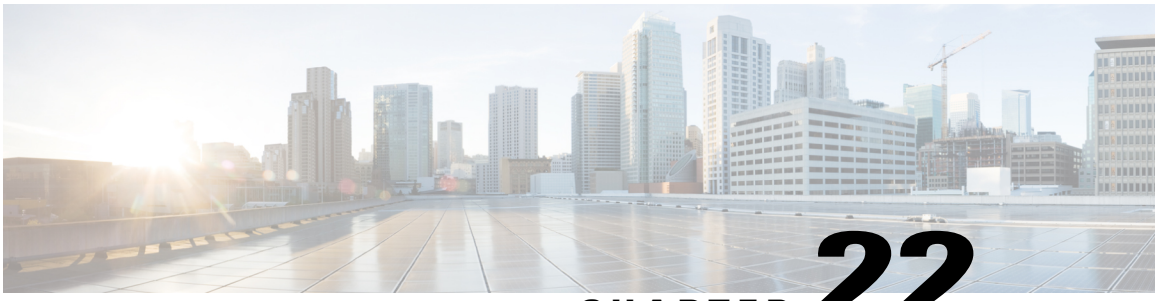
5 Re-run the **Certificate Import Tool** and import the OpenAM certificate into IM and Presence Service.

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 162



CHAPTER 22

Traces Used To Troubleshoot IM and Presence Service

- Troubleshooting IM and Presence Service Using Trace, page 225
- Common Traces and Log File Locations for IM and Presence Service Nodes, page 226
- IM and Presence Service Login and Authentication Traces, page 227
- Availability, IM, Contact List, and Group Chat Traces, page 227
- Availability and IM Traces for Partitioned Intradomain Federation MOC Contact Issues, page 229
- Availability and IM Traces for XMPP-Based Interdomain Federation Contact Issues, page 229
- Availability and IM Traces for SIP-Based Interdomain Federation Contact Issues, page 230
- Calendaring Traces, page 231
- Intercluster Synchronization Traces and Inter-Clustering Troubleshooter, page 231
- SIP Federation Traces, page 232
- XMPP Federation Traces, page 232
- High CPU and Low VM Alert Troubleshooting, page 232

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 31: 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`

Service	Trace Log Filename
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
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 32: 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/xmpp-cm-4*.log
Cisco XCP Router	/epas/trace/xcp/log/rtr-jsm-*.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 33: 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. 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 • Cisco XCP Router • Cisco Presence Engine
End user has issues with their self availability status, including on-the-phone or meeting status. Perform traces for the listed services on the IM and Presence Service node on which the end user is provisioned.	• Cisco XCP Connection Manager • Cisco XCP Router • Cisco Presence Engine
End user has issues sending or receiving instant messages. 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 • Cisco XCP Router
End user is experiencing any of the following issues: • Difficulty creating or joining a chat room. • Chat room messages are not being delivered to all members. • Any other issues with the chat room. 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 • Cisco XCP Router • 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. 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 • 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/xmpp-cm-4*.log`

- 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 34: 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 35: 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 XCP XMPP Federation Connection Manager 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 36: 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 37: 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 38: 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/log4/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 39: 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-*.log`
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 40: Traces Used to Investigate XMPP Federation Issues

Service	Trace Log Filename
Cisco XCP Router	`/epas/trace/xcp/log/rtr-jsm-*.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 41: CLI Commands Used to Investigate High CPU and Low VM Alerts

Solution	CLI Command

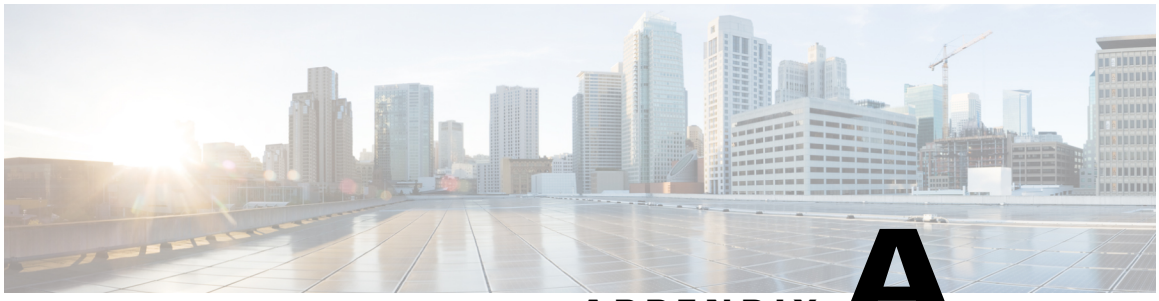
Use the CLI to run the following commands on the node.	`show process using-most cpu`
	`show process using-most memory`
	`utils dbreplication runtimestate`
	`utils service list`

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 42: 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, page 235
- 1000 Full UC Active/Standby, page 237
- 2 GB Active/Standby Profile, page 238
- 4 GB Active/Active Profile, page 238
- 4 GB Active/Standby Profile, page 239
- 6 GB Active/Active Profile, page 240
- 6 GB Active/Standby Profile, page 242

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 subcluster. 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 subcluster 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 OVA (2, 4 or 6 GB), 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 **Users Moved Per Iteration** service parameter. This parameter determines the number of users moved per iteration during a failover or a fallback operation. We provide a recommended value for the **Users Moved Per Iteration** service parameter for each High Availability login profile table.
    - The total number of users in the subcluster 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, and the **Users Moved Per Iteration** service parameter on both nodes in a subcluster. You must manually configure all these values on both nodes in the subcluster.
- The upper and lower client re-login limit values must be the same on each node in the subcluster.
- 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.

Related Topics

Configure Advanced Service Parameters for Server Recovery Manager, on page 77

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.
- **Users Moved Per Iteration** service parameter value.

Procedure

Step 1 Choose a profile table based on your memory size, 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 subcluster, 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 Retrieve the corresponding **Users Moved Per Iteration** service parameter value for your High Availability login profile table.

Step 6 Configure the **Users Moved Per Iteration** value on IM and Presence by choosing **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters**, and choosing **Cisco Server Recovery Manager** from the **Service** menu.

Example High Availability Login Configurations

Example 1: 6GB Active/Standby Standard Deployment

You have 3000 users in your subcluster, with 2000 users on one node, and 1000 users on the second node. For active/standby deployments, we recommend 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:

Number of Users	Lower Retry Limit	Upper Retry Limit
2000	40	107

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.

You also configure the corresponding **Users Moved per Iteration** service parameter value for the 6 GB active/standby profile, which is 50.

Example 2: 4GB Active/Active IM-Only Deployment

You have 6800 users on the first node in your subcluster in an IM-only deployment. We recommend 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 7000:

Number of Users	Lower Retry Limit	Upper Retry Limit
7000	280	1447

You also configure the corresponding **Users Moved per Iteration** service parameter value for the 6 GB active/standby profile, which is 25.

1000 Full UC Active/Standby

Table 43: 1000 Full UC Active/Standby

Number of Users	Lower Retry Limit	Upper Retry Limit
100	90	115
250	90	153
500	90	215
750	90	278
1000	90	340
1250 (IM only)	90 (IM only)	403 (IM only)
1500	90	465
1750	90	528

Number of Users	Lower Retry Limit	Upper Retry Limit
2000	90	590

2 GB Active/Standby Profile

Corresponding **Users Moved per Iteration** service parameter value: 6

Table 44: User Login Retry Limits for Standard Deployment (2 GB Active/Standby)

Number of Users	Lower Retry Limit	Upper Retry Limit
100	17	57
250	42	142
500	83	283
750	125	425
1000	167	567

4 GB Active/Active Profile

Corresponding **Users Moved per Iteration** service parameter value: 25

Table 45: User Login Retry Limits for Standard Deployment (4GB Active/Active)

Number of Users	Lower Retry Limit	Upper Retry Limit
100	4	21
500 (Default)	20 (Default)	103 (Default)
1000	40	207
1500	60	310
2000	80	413
2500	100	517

Corresponding **Users Moved per Iteration** service parameter value: 25

Table 46: User Login Retry Limits for IM-Only Deployment (4GB Active/Active)

Number of Users	Lower Retry Limit	Upper Retry Limit
3000	120	620
3500	140	723
4000	160	827
4500	180	930
5000	200	1033
6000	240	1240
7000	280	1447
7500	300	1550

4 GB Active/Standby Profile

Corresponding **Users Moved per Iteration** service parameter value: 25

Table 47: User Login Retry Limits for Standard Deployment (4GB Active/Standby)

Number of Users	Lower Retry Limit	Upper Retry Limit
100	4	14
500	20	70
1000	40	140
1500	60	210
2000	80	280
2500	100	350
3000	120	420
3500	140	490
4000	160	560
4500	180	630

Number of Users	Lower Retry Limit	Upper Retry Limit
5000	200	700

Corresponding **Users Moved per Iteration** service parameter value: 25

Table 48: User Login Retry Limits for IM-Only Deployment (4GB Active/Standby)

Number of Users	Lower Retry Limit	Upper Retry Limit
6000	240	840
7000	280	980
8000	320	1120
9000	360	1260
10000	400	1400
11000	440	1540
12000	480	1680
13000	520	1820
14000	560	1960
15000	600	2100

6 GB Active/Active Profile

This section includes the upper and lower user login retry limits for both standard and IM-only deployments.

User login retry limits for standard deployments

Corresponding **Users Moved per Iteration** service parameter value: 50

Table 49: User Login Retry Limits for Standard Deployments (6 GB Active/Active)-IM and Presence Release 9.0(1) and Later

Number of Users	Lower Retry Limit	Upper Retry Limit
100	2	10
500 (Default)	10 (Default)	52 (Default)

Number of Users	Lower Retry Limit	Upper Retry Limit
1000	20	103
1500	30	155
2000	40	207
2500	50	258
3000	60	310
3500	70	362
4000	80	413
4500	90	465
5000	100	517
6000	120	620
7000	140	723
7500	150	775

User retry limits for IM-only deployments

Corresponding **Users Moved per Iteration** service parameter value: 50

Table 50: User Login Retry Limits for IM-Only Deployments (6 GB Active/Active)-IM and Presence Release 9.0(1) and Later

Number of Users	Lower Retry Limit	Upper Retry Limit
3000	60	227
3500	70	264
4000	80	302
4500	90	340
5000	100	378
6000	120	453
7000	140	529
7500	150	569

Number of Users	Lower Retry Limit	Upper Retry Limit
8000	160	827
9000	180	930
10000	200	1033
11000	220	1137
12000	240	1240
12500	250	1292

6 GB Active/Standby Profile

This section includes the upper and lower retry limits for both standard and IM-only deployments.

User Login Retry Limits for Standard Deployments

Corresponding **Users Moved per Iteration** service parameter value: 50

Table 51: User Login Retry Limits for Standard Deployments (6 GB Active/Standby)-IM and Presence Release 9.0(1) and Later

Number of Users	Lower Retry Limit	Upper Retry Limit
100	2	7
500 (Default)	10 (Default)	33 (Default)
1000	20	65
1500	30	98
2000	40	131
2500	50	164
3000	60	196
3500	70	229
4000	80	262
4500	90	295
5000	100	327

Number of Users	Lower Retry Limit	Upper Retry Limit
6000	120	393
7000	140	458
8000	160	524
9000	180	589
10000	200	655
11000	220	720
12000	240	785
13000	260	851
14000	280	916
15000	300	982

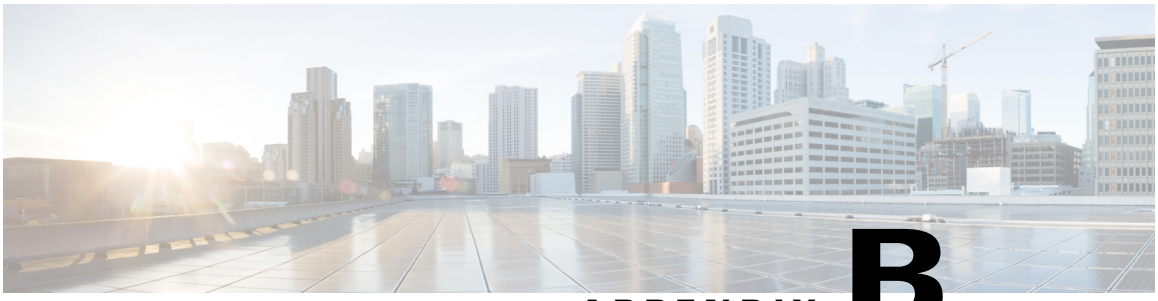
User Login Retry Limits for IM-only Deployments

Corresponding **Users Moved per Iteration** service parameter value: 50

Table 52: User Login Retry Limits for IM-Only Deployments (6 GB Active/Standby)-IM and Presence Release 9.0(1) and Later

Number of Users	Lower Retry Limit	Upper Retry Limit
6000	120	320
7000	140	373
8000	160	427
9000	180	480
10000	200	533
11000	220	587
12000	240	640
13000	260	693
14000	280	747
15000	300	800

Number of Users	Lower Retry Limit	Upper Retry Limit
16000	320	1047
17000	340	1113
18000	360	1178
19000	380	1244
20000	400	1309
21000	420	1375
22000	440	1440
23000	460	1505
24000	480	1571
25000	500	1636



APPENDIX B

XMPP Standards Compliance

- XMPP Standards Compliance, page 245

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)