Configuration and Administration for the IM and Presence Service, Release 11.5(1)SU5

First Published: 2018-06-29
Last Modified: 2018-09-24

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

PART I Plan the System 19

CHAPTER 1 Plan the System 1

IM and Presence Service Overview 1
IM and Presence Service Components 1
Planning Overview 4
Plan Your Deployment 4
IM and Presence Service Deployment Sizing 6
Feature Deployment Options 6
Standard Deployment vs Centralized Cluster 7
Multinode Scalability Feature 8
Multinode Scalability Requirements 8
Scalability Options for Deployment 8
WAN Deployments 10
Intracluster Deployments Over WAN 10
Intercluster Deployments Over WAN 11
SAML Single Sign-On Deployments 11
Third Party Integrations 11
Third Party Client Integration 12

PART II Configure the System 15

CHAPTER 2 Configure the Domain 17

Configure the Domain Overview 17
Domain Configuration Examples 17
Configure the Domain Prerequisites 20
CHAPTER 5

Configure Redundancy 43
Presence Redundancy Group Overview 43
High Availability 44
Presence Redundancy Group Prerequisites 44
Presence Redundancy Group Task Flow 44
Verify Database Replication 45
Verify Services 45
Configure a Presence Redundancy Group 46
Configure Heartbeat Interval for Failover 47
Enable High Availability 48
Configure User Assignment Mode 49
Initiate Manual Failover, Fallback, or Recovery 49
Node State Definitions 50
Node States, Causes, and Recommended Actions 51
Redundancy Interactions and Restrictions 56

CHAPTER 6

Configure User Settings 59
End User Settings Overview 59
Service Profiles 59
Feature Group Template Overview 60
User Settings Prerequisites 60
Configure User Settings Task Flow 60
Configure the User Assignment Mode 61
Add an IM and Presence UC Service 61
Configure a Service Profile 62
Configure a Feature Group Template 63

CHAPTER 7

Configure LDAP Directory 65
LDAP Synchronization Overview 65
LDAP Authentication for End Users 66
Directory Server User Search for Cisco Mobile and Remote Access Clients and Endpoints 66
LDAP Synchronization Prerequisites 67
CHAPTER 8

Configure Cisco Unified Communications Manager for IM and Presence Service 77
Integration Overview 77
Cisco Unified Communications Manager Integration Prerequisites 77
Cisco Unified Communications Manager Integration Task Flow 79
Configure a SIP Trunk Security Profile 80
Configure SIP Trunk for IM and Presence Service 80
Configure SRV Cluster Name 81
Configure a SIP PUBLISH Trunk 81
Configure the Presence Gateway 82
Verify Services on Cisco Unified Communications Manager 82
Configure Phone Presence from Off-Cluster Cisco Unified Communications Manager 83
Add Cisco Unified Communications Manager as TLS Peer 83
Configure a TLS Context for Unified Communications Manager 84

CHAPTER 9

Configure Centralized Deployment 85
Centralized Deployment Overview 85
Centralized Cluster Deployment Architecture 87
Centralized Cluster Use Case 87
Centralized Deployment Prerequisites 88
Centralized Deployment Configuration Task Flow 90
Enable IM and Presence in Central Cluster 91
CHAPTER 10  Configure Advanced Routing  103

Advanced Routing Overview  103
Advanced Routing Prerequisites  103
Advanced Routing Configuration Task Flow  104
  Configure the Routing Communication Method  105
  Restart the Cisco XCP Router  106
  Configure Secure Router-to-Router Communications  106
  Configure the Cluster ID  107
  Configure Throttling Rate for Presence Updates  107
  Configure Static Routes  108
    Configure SIP Proxy Server Settings  108
    Configure Route Embed Templates on IM and Presence Service  108
    Configure Static Routes on IM and Presence Service  110

CHAPTER 11  Configure Certificates  113

Certificates Overview  113
Certificates Prerequisites  115
Certificate Exchange with Cisco Unified Communications Manager  115
  Import Cisco Unified Communications Manager Certificate to IM and Presence Service  116
  Download Certificate from IM and Presence Service  117
Import IM and Presence Certificate to Cisco Unified Communications Manager 117
Install Certificate Authority (CA) on IM and Presence Service 118
   Upload CA Root Certificate Chain 118
   Restart Cisco Intercluster Sync Agent Service 119
   Verify CA Certificates Have Synchronized to Other Clusters 119
Upload Certificates to IM and Presence Service 120
   Upload Certificates 121
   Restart Cisco Tomcat Service 122
   Verify Intercluster Syncing 122
   Restart the Cisco XCP Router service on all nodes 123
   Restart Cisco XCP XMPP Federation Connection Manager Service 123
   Enable Wildcards in XMPP Federation Security Certificates 123
Generate a CSR 124
   CSR Key Usage Extensions 125
Generate a Self-Signed Certificate 126
   Delete Self Signed Trust Certificates from IM and Presence Service 126
   Delete Self-Signed Tomcat-Trust Certificates from Cisco Unified Communications Manager 127
Certificate Monitoring Task Flow 128
   Configure Certificate Monitor Notifications 128
   Configure Certificate Revocation via OCSP 129

CHAPTER 12 Configure Security Settings 131
Security Overview 131
Security Settings Configuration Task Flow 131
   Create Login Banner 132
   Configure Secure XMPP Connections 132
   SIP Security Settings Configuration on IM and Presence Service 133
      Configure TLS Peer Subject 133
      Configure TLS Context 134
   FIPS Mode 134

CHAPTER 13 Configure Intercluster Peers 137
Intercluster Peers Overview 137
   Intercluster Peers Prerequisites 137
Intercluster Peers Configuration Task Flow 138
  Check User Provisioning 138
  Enable the Cisco AXL Web Service 139
  Enable the Sync Agent 139
  Configure Intercluster Peers 140
  Restart the XCP Router Service 141
  Verify the Intercluster Sync Agent is On 141
  Verify Intercluster Peer Status 141
  Update Intercluster Sync Agent Tomcat Trust Certificates 142
Intercluster Peering Interactions and Restrictions 143

---

CHAPTER 14 Configure Push Notifications for Cisco Jabber on iPhone and iPad 145
  Push Notifications Overview 145
  Push Notifications Configuration 147

---

PART III Configure Features 149

---

CHAPTER 15 Configure Availability and Instant Messaging 151
  Availability and Instant Messaging Overview 151
  Availability and Instant Messaging Prerequisites 152
  Availability and Instant Messaging Task Flow 152
    Configure Presence Sharing 153
    Enable Instant Messaging 154
  Availability and Instant Messaging Interactions and Restrictions 154

---

CHAPTER 16 Configure Chat Rooms 155
  Group Chat Rooms Overview 155
  Group Chat Prerequisites 156
  Group Chat and Persistent Chat Task Flow 156
    Configure Group Chat System Administrators 157
    Configure Chat Room Settings 157
    Restart the Cisco XCP Text Conference Manager 158
    Set up External Database for Persistent Chat 159
    Add External Database Connection 159
CHAPTER 17
Configure High Availability for Persistent Chat 163
High Availability for Persistent Chat Overview 163
  High Availability for Persistent Chat - Intercluster Example 163
  Comparison of Persistent Chat (non-HA) and Persistent Chat HA Requirements 164
High Availability for Persistent Chat Prerequisites 165
High Availability for Persistent Chat Task Flow 166
  Set up External Database 166
  Add External Database Connection 167
  Verify High Availability for Persistent Chat Settings 167
  Start Cisco XCP Text Conference Manager Service 168
  Merge External Databases 168
High Availability for Persistent Chat Use Cases 170
  High Availability for Persistent Chat Failover Use Case 171
  High Availability Persistent Chat Fallback Use Case 172

CHAPTER 18
Configure Managed File Transfer 173
Managed File Transfer Overview 173
  Managed File Transfer Call Flow 174
Managed File Transfer Prerequisites 174
  External Database Prerequisites 175
  External File Server Requirements 175
Managed File Transfer Task Flow 177
  Add External Database Connection 178
  Set up an External File Server 178
  Create User for the External File Server 179
  Set up Directory for External File Server 180
  Obtain Public Key for the External File Server 181
  Provision External File Server on IM and Presence Service 182
    External File Servers Fields 183
  Verify Cisco XCP File Transfer Manager Activation 184
  Enable Managed File Transfer 185
PART IV

Administer the System 205

CHAPTER 22

Manage Chat 207

Manage Chat Overview 207
Chat Node Alias Overview 207
Manage Chat Prerequisites 208
Manage Chat Task Flow 208
Enable Chat Room Owners to Edit Chat Room Settings 209
Allow Clients to Log Instant Message History 210
Configure Chat Room Settings 210
Set Number of Chat Rooms 210
Configure Chat Room Member Settings 210
Configure Availability Settings 212
Configure Occupancy Settings 212
Configure Chat Message Settings 213
Configure Moderated Room Settings 214
Configure History Settings 214
Reset Chat Rooms to System Defaults 215
Chat Node Alias Management 215
Manage Chat Node Aliases 215
Assign Mode for Managing Chat Aliases 215
Add Chat Node Alias Manually 216
Manage Chat Interactions 217

CHAPTER 23

Managed File Transfer Administration 219

Managed File Transfer Administration Overview 219
Managed File Transfer Administration Prerequisites 220
Managed File Transfer Administration Task Flow 220
AFT_LOG Table Example Query and Output 220
External Database Disk Usage 221
Set Service Parameter Thresholds 222
Configure XCP File Transfer Manager Alarms 223
Alarms and Counters for Managed File Transfer 223
CHAPTER 24  Manage End Users  227
Manage End Users Overview  227
Presence Authorization Overview  227
Validating User IDs and Directory URIs  228
Manage End Users Task Flow  229
Assign a Presence Authorization Policy  229
Configure Data Monitor Checks for User Data  230
Set Schedule for User ID and Directory URI Validation Check  230
Set up Email Server for Email Alerts  231
Enable Email Alerts  231
Validate User Data via the System Troubleshooter  232
Validate User IDs and Directory URIs via CLI  233
User ID and Directory URI CLI Validation Examples  233
User ID and Directory URI Errors  234
View Presence Settings for User  236
Presence Authorization Interactions and Restrictions  238

CHAPTER 25  Migrate Users  239
Migrate Users Overview  239
Migrate Users Prerequisites  239
Migrate Users Task Flow  239
Configure Standard Presence for Migration  240
Check for Intercluster Sync Errors  241
Start Essential Services for Migration  241
Export User Contact Lists  242
Migrate Users via LDAP  242
Update External LDAP Directory  243
Configure LDAP in New Cluster  244
Move Users to New Cluster Manually  244
Enable IM and Presence For User Manually  245
Import Users Manually  245
Enable Users for IM and Presence Service on New Cluster  246
Migrate Users via Bulk Administration  246
Bulk Administration Task Flow  290
Bulk Rename User Contact IDs  290
  Bulk Rename User Contact IDs File Details  291
Bulk Export User Contact Lists and Non-Presence Contact Lists  291
  File Details for Export Contact Lists  292
  File Details for Export Non-Presence Contact Lists  293
Bulk Import Of User Contact Lists  294
  Verify Maximum Contact List Size  294
Upload Input File  294
Create New Bulk Administration Job  297
Check Results of Bulk Administration Job  297

CHAPTER 31

Troubleshoot the System  299
Troubleshooting Overview  299
Run the System Troubleshooter  299
Run Diagnostics  300
  Diagnostic Tools Overview  301
Using Trace Logs for Troubleshooting  302
  Common IM and Presence Issues via Trace  302
  Common Traces via CLI  304
  Run Traces via CLI  308
  Common Traces via RTMT  309
Troubleshooting UserID and Directory URI Errors  310
  Received Duplicate UserID Error  310
  Received Duplicate or Invalid Directory URI Error  311

PART V

Reference Information  313

CHAPTER 32

Cisco Unified Communications Manager TCP and UDP Port Usage  315
Cisco Unified Communications Manager TCP and UDP Port Usage Overview  315
Port Descriptions  316
Intracluster Ports Between Cisco Unified Communications Manager Servers  317
Common Service Ports  320
Ports Between Cisco Unified Communications Manager and LDAP Directory  323
Contents

Web Requests From CCMAdmin or CCMUser to Cisco Unified Communications Manager 323
Web Requests From Cisco Unified Communications Manager to Phone 323
Signaling, Media, and Other Communication Between Phones and Cisco Unified Communications Manager 324
Signaling, Media, and Other Communication Between Gateways and Cisco Unified Communications Manager 326
Communication Between Applications and Cisco Unified Communications Manager 328
Communication Between CTL Client and Firewalls 330
Special Ports on HP Servers 330
Port References 331
  Firewall Application Inspection Guides 331
  IETF TCP/UDP Port Assignment List 331
  IP Telephony Configuration and Port Utilization Guides 331
  VMware Port Assignment List 331

CHAPTER 33

Port Usage Information for the IM and Presence Service 333
  IM and Presence Service Port Usage Overview 333
  Information Collated in Table 333
  IM and Presence Service Port List 334

CHAPTER 34

Additional Requirements 345
  XMPP Standards Compliance 345
  Configuration Changes and Service Restart Notifications 346
PART I

Plan the System

• Plan the System, on page 1
Plan the System

- IM and Presence Service Overview, on page 1
- Planning Overview, on page 4
- Plan Your Deployment, on page 4

**IM and Presence Service Overview**

IM and Presence Service Administration is a web-based application that allows you to make individual, manual configuration changes to the IM and Presence Service nodes. The procedures in this guide describe how to configure features using this application.

IM and Presence Service offers a choice of either rich-featured Cisco Jabber Unified Communications clients or any third-party XMPP-compliant IM and presence client. IM and Presence Service also provides instant messaging, file transfer, and has the ability to host and configure persistent Group Chat Rooms.

In an on-premises deployment with IM and Presence Service and Cisco Unified Communications Manager, the following services are available:

- Presence
- Instant messaging
- File Transfers
- Audio Calls
- Video
- Voicemail
- Conferencing

See Cisco Unified Communications Manager documentation for more.

**IM and Presence Service 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.
You must configure the following to enable the SIP interface:

- In Cisco Unified Communications Manager, you must configure a SIP trunk that points to the IM and Presence Service for the presence information exchange.

- On the IM and Presence Service, configure Cisco Unified Communications Manager as a Presence Gateway so that IM and Presence Service can send SIP subscribe messages to Cisco Unified Communications Manager over the SIP trunk.

**Note**

IM and Presence Service does not support clients (Cisco clients or third party) connecting to the IM and Presence Service using SIP/SIMPLE interface over TLS. Only a SIP connection over TCP is supported.

**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, the Cisco Sync Agent network service must be running.
By default, the Sync Agent load balances all users equally across all nodes within the IM and Presence Service cluster. However, 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.

---

**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.

---

**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.

---

**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 integration with Microsoft Lync for Remote Call Control (RCC). For information, see the Remote Call Control with Microsoft Lync Server for the IM and Presence Service.

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

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

---

**Cisco IM and Presence Data Monitor Service**
The Cisco IM and Presence Data Monitor monitors the IDS replication state on the IM and Presence Service. Other IM and Presence services are dependent on the Cisco IM and Presence Data Monitor so that they can delay startup until IDS replication is in a stable state.
The Cisco IM and Presence Data Monitor also checks the status of the Cisco Sync Agent sync from Cisco Unified Communications Manager. Dependent services are only allowed to start after IDS replication has set up and the Sync Agent on the IM and Presence database publisher node has completed its sync from Cisco Unified Communications Manager. After the timeout has been reached, the Cisco IM and Presence Data Monitor on the Publisher node will allow dependent services to start even if IDS replication and the Sync Agent have not completed.

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

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

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

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

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

- Use this CLI command: `utils dbreplication runtimestate`
- Use the Cisco Unified IM and Presence Reporting Tool. The “IM and Presence Database Status” report displays a detailed status of the cluster.

To check the status of the Cisco Sync Agent, navigate to the Cisco Unified CM IM and Presence Administration interface and select Diagnostics > System Dashboard. You will find the Cisco Unified Communications Manager publisher node IP address as well as the sync status.

### Planning Overview

Before you configure your system, make sure that you plan how you want to deploy your system. The IM and Presence Service offers different deployment options that are designed to meet the needs of different companies.


### Plan Your Deployment

Before you configure your system, make sure that you plan your cluster topology and how you want to deploy your system.
## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Determine which features you want to deploy</td>
<td>For details, see Feature Deployment Options, on page 6.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Determine if you will install the standard deployment or an IM and Presence central cluster deployment</td>
<td>Decide whether you want to deploy the IM and Presence Service on the same cluster as your telephony, or whether you want to deploy a centralized cluster for IM and Presence. For details, see Standard Deployment vs Centralized Cluster, on page 7.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Plan how many cluster nodes you want to deploy</td>
<td>The IM and Presence multinode scalability features allow you to size your deployment to meet your needs. For details, see Multinode Scalability Requirements, on page 8.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Plan how you are going to add redundancy</td>
<td>Scalability Options for Deployment, on page 8</td>
</tr>
<tr>
<td>Step 6</td>
<td>Plan your geographic sites</td>
<td>You can install at a single site in order to maintain your hardware from a single location. However, you can also deploy your clusters over the WAN to add geographic redundancy with deploying multiple sites. For details, see:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Intracluster Deployments Over WAN, on page 10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Intercluster Deployments Over WAN, on page 11</td>
</tr>
<tr>
<td>Step 7</td>
<td>Decide if you want to configure SAML Single-Sign On</td>
<td>For details, see SAML Single Sign-On Deployments, on page 11.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Determine if you want to integrate with a third-party application</td>
<td>This includes Microsoft Outlook calendar integration as well as federation with a third-party system. For details, see Third Party Integrations, on page 11.</td>
</tr>
</tbody>
</table>
IM and Presence Service Deployment Sizing


Feature Deployment Options

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

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

Figure 2: IM and Presence Service Feature Deployment Options

The following table lists the feature deployment options for IM and Presence Service.
### Table 1: Feature Deployment Options for the IM and Presence Service

<table>
<thead>
<tr>
<th>Core IM and Availability Features</th>
<th>Advanced IM Features (optional)</th>
<th>Rich Unified Communications Availability features (optional)</th>
<th>Remote Desk Phone Control (optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>View user availability</td>
<td>Persistent chat</td>
<td>Cisco telephony availability</td>
<td>Remote Cisco IP Phone control</td>
</tr>
<tr>
<td>Securely send and receive rich text IMs</td>
<td>Managed File Transfer</td>
<td>Microsoft Outlook calendar integration (on-premise Exchange or hosted Office 365 deployments)</td>
<td>Remote Softphone Control</td>
</tr>
<tr>
<td>File transfers</td>
<td>Message Archiver</td>
<td></td>
<td>Microsoft Remote Call Control</td>
</tr>
<tr>
<td>Ad hoc group chat</td>
<td>Calendaring Third-party XMPP client support</td>
<td></td>
<td>integration</td>
</tr>
<tr>
<td>Manage contacts</td>
<td>High availability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User history</td>
<td>Scalability: multinode support and clustering over WAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Jabber support</td>
<td>Intercluster peering</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiple client device support:</td>
<td>Enterprise federation:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft windows, MAC, Mobile,</td>
<td>• IM and Presence Service integration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tablet, IOS, Android, BB</td>
<td>• Cisco WebEx Messenger integration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Office integration</td>
<td>• Microsoft Lync/Skype for Business/Office365 server integration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDAP directory integration</td>
<td>• IBM SameTime integration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal directory and buddy lists</td>
<td>• Cisco Jabber XCP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open APIs</td>
<td>Public federation:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System troubleshooting</td>
<td>• Google Talk, AOL integration</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• XMPP services or BOTs</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Third-party Exchange Service integration</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IM Compliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SAML Single Sign On</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Custom login banner</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Standard Deployment vs Centralized Cluster

Before you even install your system, you must decide whether you want to deploy a standard deployment of the IM and Presence Service or whether you want an IM and Presence Service central cluster as this will affect your topology and installation:
• IM and Presence Service on Cisco Unified Communications Manager (Standard deployment)—In standard deployments, the IM and Presence Service cluster is installed on the same servers as the Cisco Unified Communications Manager telephony nodes. The IM and Presence cluster shares a platform and many of the same services as the telephony cluster. This option requires a 1x1 mapping of telephony clusters to IM and Presence clusters.

• Centralized IM and Presence cluster—In this deployment, the IM and Presence Service cluster is installed separately from your telephony cluster. Depending on how you plan your topology, the IM and Presence central cluster may be located on completely different hardware servers from your telephony cluster. This deployment option removes the 1x1 mapping requirement of telephony clusters and IM and Presence clusters, which allows you to better scale each deployment type to its own needs.

---

Note: The IM and Presence central cluster still has an instance of Cisco Unified Communications Manager. However, this instance is for user provisioning and database and does not handle telephony. For telephony integration, the IM and Presence central cluster must connect to a separate Cisco Unified Communications Manager telephony cluster.

The procedures in this document can be used for both standard deployments and central cluster deployments. However, for central cluster deployments, you must also complete the tasks in the Configure Centralized Deployment, on page 85 chapter to properly align your telephony cluster and IM and Presence cluster.

Multinode Scalability Feature

Multinode Scalability Requirements

IM and Presence Service supports multinode scalability:

• Six nodes per cluster

• 75,000 users per cluster with a maximum of 25,000 users per node in a full Unified Communication (UC) mode deployment

• 25,000 users in a presence redundancy group, and 75,000 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://%20docwiki.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: Scalability Options for Deployment

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

IM and Presence Service supports Clustering over WAN for both intracluster and intercluster deployments. This option allows you to add geographic redundancy to your deployment.

**Intracluster Deployments Over WAN**

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

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

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

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

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

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

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

**Multinode Configuration for Deployment Over WAN**

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

- For optimum performance, Cisco recommends that you assign the majority of your users to the home IM and Presence Service node. This deployment model decreases the volume of messages sent to the remote IM and Presence Service node over WAN, however the failover time to the secondary node depends on the number of users failing over.

- If you wish to configure a High Availability deployment model over WAN, you can configure a presence redundancy group-wide DNS SRV address. In this case, IM and Presence Service sends the initial PUBLISH request message to the node specified by DNS SRV and the response message indicates the host node for the user. IM and Presence Service then sends all subsequent PUBLISH messages for that user to the host node. Before configuring this High Availability deployment model, you must consider if you have sufficient bandwidth for the potential volume of messages that may be sent over the WAN.
Intercluster Deployments Over WAN

IM and Presence Service supports intercluster deployments over WAN, using the bandwidth recommendations provided in this module. The considerations apply when deploying intercluster deployments:

- **Intercluster Peers**—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. For details on how to set up intercluster peers, see Configure Intercluster Peers, on page 137.

- **Node Names**—The node name that you define for any IM and Presence Service node must be resolvable by every other IM and Presence Service node on every cluster. Therefore, each IM and Presence Service node name must be the FQDN of the node. If DNS is not deployed in your network, each node name must be an IP address.

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

- **Router-to-Router Communications**—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 can also configure secure router-to-router communications that use TLS to secure the connection between each router-to-router connector node in the local cluster, and each router connector node in the remote cluster.

SAML Single Sign-On Deployments

The Security Assertion Markup Language (SAML) Single Sign-On feature allows administrative users to access a number of Cisco Collaboration applications, including the IM and Presence Service, after signing into only one of those applications. This feature simplifies the administrator's job in the following ways:

- A single login is required to access a number of Cisco Collaboration applications after a single sign-in.

- Only one password is required—there's no longer any need to remember different passwords for each application.

- Administrators can manage all passwords and authentication from a single Identity Provider (IdP).


Third Party Integrations

The IM and Presence Service integrates with a variety of third-party systems. The following table outlines the integrations and provides a link to the document that describes how to configure it.
This Guide Contains ...

Guide Title: Microsoft Outlook Calendar Integration for the IM and Presence Service
This Guide Contains: Configure the IM and Presence Service to connect with an on-premise Microsoft Exchange server or a hosted Office 365 server in order to use calendar information from Microsoft Outlook in an IM and Presence user's Presence status.

Guide Title: Interdomain Federation for the IM and Presence Service
This Guide Contains: Configure the IM and Presence Service for interdomain federation with the following systems. This allows IM and Presence users to exchange IM and Presence with users on the other system.
- Microsoft Lync
- Microsoft Skype for Business
- Microsoft Office 365
- Google Talk
- AOL
- IBM SameTime
- Cisco WebEx Messenger
- another IM and Presence Service enterprise

Guide Title: Partitioned Intradomain Federation for the IM and Presence Service
This Guide Contains: Configuring the IM and Presence Service for Partitioned Intradomain Federation with Microsoft Lync or Skype for Business. You can use this integration to maintain communications within your network while you are in the process of migrating users to the IM and Presence Service.

Guide Title: Remote Call Control with Microsoft Lync Server for the IM and Presence Service
This Guide Contains: Configure Cisco Unified Communications Manager and IM and Presence Service for integration with Microsoft Lync for Microsoft Remote Call Control (RCC). This integration allows enterprise users to control their Cisco Unified IP Phone or Cisco IP Communicator Phone through Microsoft Lync, a third-party desktop instant-messaging (IM) application.

Third Party Client Integration

This section outlines some of the requirements for third-party client integrations.

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

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).


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.

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 Third-Party LDAP settings for XMPP clients 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.

Note

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

Configure the System

• Configure the Domain, on page 17
• Configure IPv6, on page 27
• Configure IM Addressing Scheme, on page 33
• Configure Redundancy, on page 43
• Configure User Settings, on page 59
• Configure LDAP Directory, on page 65
• Configure Cisco Unified Communications Manager for IM and Presence Service, on page 77
• Configure Centralized Deployment, on page 85
• Configure Advanced Routing, on page 103
• Configure Certificates, on page 113
• Configure Security Settings, on page 131
• Configure Intercluster Peers, on page 137
• Configure Push Notifications for Cisco Jabber on iPhone and iPad, on page 145


CHAPTER 2

Configure the Domain

• Configure the Domain Overview, on page 17
• Configure the Domain Prerequisites, on page 20
• Configure the Domain Task Flow, on page 20

Configure the Domain Overview

The IM and Presence Domain window displays the following types of domains:

• Administrator-managed IM address domains. These are internal domains that you have added manually but have not yet assigned to any users, or that were added automatically by the Sync Agent but the user's domain has since changed and so it is no longer in use.

• System-managed IM address domains. These are internal domains that are in use by a user in the deployment and which can be added either manually or automatically.

If the domain appears in the IM and Presence Domain window, the domain is enabled. You do not need to enable a domain. You can manually add, update, and delete local IM address domains.

It is possible to have a domain configured on two clusters, but in use on only the peer cluster. This appears as a system-managed domain on the local cluster, but is identified as being in use on only the peer cluster.

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

Domain Configuration Examples

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

• Multiple Cluster with Different DNS Domains and Subdomains

• Single Cluster with Different DNS Domains or Subdomains
• Single Cluster where the DNS Domain is Different than the Unified Communications Manager Domain

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

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

**Multiple Cluster with Different DNS Domains and Subdomains**

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

![Diagram](image)

**Single Cluster with Different DNS Domains or Subdomains**

IM and Presence Service supports having the nodes within any IM and Presence Service cluster deployed across multiple DNS domains or subdomains. The diagram below highlights a sample deployment scenario that is supported.
High availability is also fully supported in scenarios where the two nodes within a presence redundancy group are in different DNS domains or subdomains.

**Note**

Single Cluster where the DNS Domain is Different than the Unified Communications Manager Domain

IM and Presence Service supports having the IM and Presence Service nodes in a different DNS domain to their associated Cisco Unified Communications Manager cluster. The diagram below highlights a sample deployment scenario that is supported.
To support Availability Integration with Cisco Unified Communications Manager, the **CUCM Domain SIP Proxy** service parameter must match the DNS domain of the Cisco Unified Communications Manager cluster. By default, this service parameter is set to the DNS domain of the IM and Presence database publisher node. If the DNS domain of the IM and Presence database publisher node differs from the DNS domain of the Cisco Unified Communications Manager cluster, you must edit this service parameter to use the domain of the Cisco Unified Communications Manager cluster.

### Configure the Domain Prerequisites

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


### Configure the Domain Task Flow

Complete these tasks to configure domains for the IM and Presence Service.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Disable High Availability, on page 21</td>
<td>If high availability is enabled, you must temporarily disable it. Changing the default domain requires you to stop services temporarily; if you stop the services while high availability is enabled, a system failover will occur.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Deactivate IM and Presence Services, on page 22</td>
<td>Stop essential services prior to changing the domain.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Configure the Default Domain on IM and Presence Service, on page 23</td>
<td>Configure the default domain value for the IM and Presence Service cluster. This procedure is applicable for both DNS and non-DNS deployments.</td>
</tr>
</tbody>
</table>

**Step 4** Perform any of these tasks:
- Add or Update IM Address Domains, on page 23
- Delete IM Address Domains, on page 24

Optional. Complete these tasks only if you want to add, edit, or delete administrator-managed domains on your local cluster.
### Disable High Availability

If you have High Availability configured, you must disable it in each presence redundancy group before you configure the default domain. If High Availability is enabled when you stop services for the default domain change, failover occurs.

**Before you begin**

Take a record of the number of active users for each cluster node in each Presence Redundancy Group. You can find this information in the **(System > Presence Topology)** window of Cisco Unified CM IM and Presence Administration. You will need these numbers later when you re-enable High Availability.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the Cisco Unified CM Administration user interface, choose <strong>System &gt; Presence Redundancy Groups</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click <strong>Find</strong> and select the group.</td>
</tr>
<tr>
<td>Step 3</td>
<td>On the Presence Redundancy Group Configuration window, uncheck the <strong>Enable High Availability</strong> check box.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Save</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Repeat this procedure for each Presence Redundancy Group.</td>
</tr>
<tr>
<td>Step 6</td>
<td>When you are done, wait at least two minutes to sync the new HA settings across the cluster before you make any further changes</td>
</tr>
</tbody>
</table>

**What to do next**

Deactivate IM and Presence Services, on page 22
Deactivate IM and Presence Services

Use this procedure to stop IM and Presence services before you make changes to the default domain. Perform this procedure on all nodes in the cluster.

Before you begin

Make sure that High Availability is disabled. For details, see Disable High Availability, on page 21.

Procedure

Step 1  From Cisco Unified IM and Presence Serviceability, choose Tools > Control Center - Network Services.
Step 2  From the Server list, choose the node on which you want to deactivate services and click Go.
Step 3  In the IM and Presence Services area, deselect the following services:
  • Cisco Client Profile Agent
  • Cisco Sync Agent
  • Cisco XCP Router

Step 4  Click Stop.
Step 5  From the Related Links drop-down list, select Service Activation and click Go.
Step 6  In the IM and Presence Services area, deselect the following services:
  • Cisco SIP Proxy
  • Cisco Presence Engine

Step 7  Click Save.
Step 8  Make a list of all the nodes on which you have disabled these services. You will need to restart the services after you have completed the changes to the default domain.

What to do next

Configure the default domain for the IM and Presence Service:
  • Configure the Default Domain on IM and Presence Service, on page 23

Otherwise, if the default domain is already configured, complete one of these tasks to add, edit, or delete domains.
  • Add or Update IM Address Domains, on page 23
  • Delete IM Address Domains, on page 24
Configure the Default Domain on IM and Presence Service

Use this procedure to configure the default domain value for an IM and Presence Service cluster. This procedure is applicable if you have a DNS or non-DNS deployment.

This procedure changes only the default domain of the IM and Presence Service cluster. It does not change the DNS domain associated with any IM and Presence Service node within that cluster. For instructions on how to change the DNS domain of an IM and Presence Service node, see Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Note

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

Before you begin

Make sure that High Availability is disabled, and essential IM and Presence Services are stopped. For details, Deactivate IM and Presence Services, on page 22.

Procedure

Step 1 Log in to the IM and Presence Service database publisher node.
Step 2 From Cisco Unified CM IM and Presence Administration, choose Presence > Settings > Advanced Configuration.
Step 3 Choose Default Domain.
Step 4 In the Domain Name field, enter the new presence domain and click Save.

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

What to do next

If you are using TLS XMPP Federation, proceed to Regenerate XMPP Client and TLS Certificates, on page 25.

Add or Update IM Address Domains

You can add or edit administrator-managed domains on your local cluster. You cannot edit system-managed domains, or administrator-managed domains that are associated with other clusters.

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

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

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

---

**Note**

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

---

**Before you begin**

Make sure that High Availability is disabled, and essential IM and Presence Services are stopped. For details, [Deactivate IM and Presence Services, on page 22](#).
Procedure

Step 1
In Cisco Unified CM IM and Presence Administration, choose Presence > Domains.
The Find and List Domains window appears displaying all administrator-managed and system-managed IM address domains.

Step 2
Choose the administrator-managed domains to delete using one of the following methods, and then click Delete Selected.
• Check the check box beside the domains to delete.
• Click Select All to select all domains in the list of administrator-managed domains.
Tip Click Clear All to clear all selections.

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

What to do next
If you are using TLS XMPP Federation, proceed to Regenerate XMPP Client and TLS Certificates, on page 25.

Regenerate XMPP Client and TLS Certificates
After you make changes to the IM domain, you must regenerate the XMPP client or TLS certificates.

Procedure

Step 1
In Cisco Unified CM IM and Presence OS Administration, choose Security > Certificate Management.
Step 2
Click Find to generate a list of the certificates.
Step 3
Click on the cup-xmpp-s2s certificate.
Step 4
In the Certificate Details window, click Regenerate.

Start IM and Presence Services
After you have made your changes to the default domain, use this procedure to restart IM and Presence services on all cluster nodes.

Before you begin
Regenerate XMPP Client and TLS Certificates, on page 25

Procedure

Step 1
From Cisco Unified IM and Presence Serviceability, choose Tools > Control Center - Network Services.
Step 2  From the Server list, choose the node on which you want to reactivate services and click Go.

Step 3  In the IM and Presence Services area, select the following services:
  - Cisco Client Profile Agent
  - Cisco Sync Agent
  - Cisco XCP Router

Step 4  Click Restart.

Step 5  From the Related Links drop-down list, select Service Activation and click Go.

Step 6  In the IM and Presence Services area, select the following services:
  - Cisco SIP Proxy
  - Cisco Presence Engine

Step 7  Click Save.

---

**What to do next**

Enable High Availability for Presence Redundancy Groups, on page 26

---

**Enable High Availability for Presence Redundancy Groups**

You can enable high availability for the presence redundancy groups after you have changed the default domain and restarted IM and Presence services.

**Before you begin**

All services must be running on IM and Presence database publisher nodes and subscriber nodes before you enable high availability. If it has been less than 30 minutes since your services restarted, confirm that your Cisco Jabber sessions have been recreated before you enable High Availability. Otherwise, Presence won't work for Jabber clients whose sessions aren't created.

To obtain the number of Cisco Jabber sessions, run the `show perf query counter "Cisco Presence Engine" Active JsmSessions` CLI command on all cluster nodes. The number of active sessions should match the number of users that you recorded when you disabled high availability.

**Procedure**

---

Step 1  From the Cisco Unified CM Administration user interface, choose System > Presence Redundancy Groups.
Step 2  Click Find and select the group.
  The Presence Redundancy Group Configuration window displays.
Step 3  Check the Enable High Availability check box.
Step 4  Click Save.
Step 5  Repeat this procedure on each Presence Redundancy Group.
CHAPTER 3

Configure IPv6

• Configure IPv6 Overview, on page 27
• Configure IPv6 Task Flow, on page 28

Configure IPv6 Overview

You can use IPv6 for your external interfaces on IM and Presence Service even though the connection between IM and Presence Service and Cisco Unified Communications Manager uses IPv4.

If you configure IPv6 for any of the following items on the IM and Presence Service node, the node will not accept incoming IPv4 packets and will not automatically revert to using IPv4:

• connection to an external database
• connection to an LDAP server
• connection to an Exchange server
• federation deployments

For federation, you must enable IM and Presence Service for IPv6 if you need to support federated links to a foreign Enterprise that is IPv6 enabled. This is true even if there is an ASA installed between the IM and Presence Service node and the federated Enterprise. The ASA is transparent to the IM and Presence Service node.

Configure IPv6 Task Flow

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Enable IPv6 on Eth0 for IM and Presence Service, on page 28</td>
<td>Enable IPv6 on the Eth0 port of each IM and Presence Service node in the cluster. You must reboot each node to apply the changes.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Enable IPv6 Enterprise Parameter, on page 29</td>
<td>After you enable IPv6 on the Eth0 port, you must enable the IPv6 enterprise parameter for the IM and Presence Service cluster.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Restart Services , on page 29</td>
<td>You must restart IM and Presence services to apply the changes.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Assign IPv6 Addresses to IM and Presence Nodes, on page 30</td>
<td>Assign IPv6 addresses to your IM and Presence Service nodes.</td>
</tr>
</tbody>
</table>

**Enable IPv6 on Eth0 for IM and Presence Service**

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

**Procedure**

**Step 1** In Cisco Unified IM and Presence OS Administration, choose Settings > IP > Ethernet IPv6.

**Step 2** In the Ethernet IPv6 Configuration window, check the **Enable IPv6** check box.

**Step 3** Choose the **Address Source**:
- Router Advertisement
- DHCP
- Manual Entry

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

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

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

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

If you checked the **Update with Reboot** check box, the node reboots and the changes are applied.
Enable IPv6 Enterprise Parameter

Use Cisco Unified CM IM and Presence Administration to enable the IPv6 enterprise parameter for the IM and Presence Service cluster.

Before you begin
Enable IPv6 on Eth0 for IM and Presence Service, on page 28

Procedure

Step 1 In Cisco Unified CM IM and Presence Administration, choose System > Enterprise Parameters.
Step 2 In the Enterprise Parameters Configuration window, choose True in the IPv6 panel.
Step 3 Click Save.

What to do next
Restart Services, on page 29 to apply the changes.

Restart Services

Use this procedure to restart IM and Presence services after you enable the IPv6 enterprise parameter for the cluster.

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

Before you begin
Enable IPv6 Enterprise Parameter, on page 29

Procedure

Step 1 From Cisco Unified IM and Presence Serviceability, choose Tools > Control Center - Network Services.
Step 2 From the Server list, choose the node on which you want to reactivate services and click Go.
Step 3 In the IM and Presence Services area, select Cisco XCP Router.
Step 4 Click Restart.
Step 5 From the Related Links drop-down list, select Service Activation and click Go.
Step 6 In the IM and Presence Services area, select the following services:
Assign IPv6 Addresses to IM and Presence Nodes

Use this procedure in Cisco Unified Communications Manager to assign your IM and Presence nodes IPv6 addresses.

Before you begin
You must also enabled the IPv6 Eth0 port in Cisco Unified OS Administration, and enable the IPv6 enterprise parameter.

Procedure

Step 1 Log in to the Cisco Unified Communications Manager publisher node
Step 2 From Cisco Unified CM Administration, choose System > Server.
Step 3 Complete one of the following tasks:
   • To add a new server, click Add New.
   • To update an existing server, click on the server that you want to edit.
Step 4 If you are adding a new server, from the Server Type drop-down menu, select CUCM IM and Presence and click Next.
Step 5 Enter the IPv6 Address for the server.
Step 6 Click Save.
Step 7 Repeat for each IM and Presence Service cluster node.

Disable IPv6 on Eth0 for IM and Presence Service

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

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

**Step 1**  
In Cisco Unified CM IM and Presence OS Administration, choose Settings > IP > Ethernet IPv6.

**Step 2**  
In the Ethernet IPv6 Configuration window, uncheck the Enable IPv6 check box.

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

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

**Step 4**  
Click Save.

If you checked the Update with Reboot check box, the node reboots and the changes are applied.
Disable IPv6 on Eth0 for IM and Presence Service
Configure IM Addressing Scheme

• IM Addressing Scheme Overview, on page 33
• IM Addressing Scheme Prerequisites, on page 34
• Configure IM Addressing Scheme Task Flow, on page 35

IM Addressing Scheme Overview

The IM and Presence Service supports two IM addressing schemes:

• UserID@Default_Domain is the default IM address scheme when you install the IM and Presence Service.

• Directory URI IM address scheme supports multiple domains, alignment with the user's email address, and alignment with Microsoft SIP URI.

You must use the same IM address scheme across all IM and Presence Service clusters.

IM Address Using User@Default_Domain

The default addressing scheme for IM and Presence Service is UserID@Default_Domain.

When you use the UserID@Default_Domain IM address scheme, all IM addresses are part of a single, default IM domain. The default domain value must be consistent across all clusters. Because IM addresses are part of the IM and Presence default domain, multiple domains are not supported.

The UserID can be free-form or synced from LDAP. The following fields are supported:

• sAMAccountName

• User Principle Name (UPN)

• Email address

• Employee number

• Telephone number

If you map the UserID to an LDAP field on Cisco Unified Communications Manager, that LDAP mapping must be consistent across all clusters.

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

**IM Address Using Directory URI**

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

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

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

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

The Directory URI IM address settings are global and apply to all users in the cluster. You cannot set a different Directory URI IM address for individual users in the cluster.

For details on provisioning directory URIs from an external LDAP Directory, see Configure LDAP Directory, on page 65.

**Multiple IM Domains**

IM and Presence Service supports IM addressing across multiple IM address domains and automatically lists all domains in the system. You can add, edit, or delete domains. For information on configuring IM domains, see Configure the Domain Overview, on page 17.


**IM Addressing Scheme Prerequisites**

The IM and Presence Service default domain and the IM address scheme that you use must be consistent across all IM and Presence Service clusters. Before you begin, Configure the Default Domain on IM and Presence Service, on page 23.

The IM address scheme you set affects all user JIDs and cannot be performed in a phased manner without disrupting communication between clusters that may have different settings.
If any of the deployed clients do not support directory URI as the IM address, administrators should disable the directory URI IM address scheme.

**Configure IM Addressing Scheme Task Flow**

Complete these tasks in the following order to configure your IM addressing scheme.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Verify User Provisioning, on page 36</td>
<td>Verify that end users are correctly provisioned and that there are no duplicate or invalid users.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Disable High Availability, on page 36</td>
<td>You must temporarily disable high availability for the presence redundancy group. Configuring the IM addressing scheme requires you to stop services temporarily; if you stop the services while high availability is enabled, a system failover will occur.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Stop Services, on page 37</td>
<td>Prior to updating your IM addressing scheme configuration stop essential IM and Presence Services. Make sure to stop services in the prescribed order.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Assign IM Addressing Scheme, on page 37</td>
<td>Use this procedure to configure a new domain and IM address scheme, or to update an existing domain and address scheme.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Restart Services, on page 39</td>
<td>Once your IM addressing scheme is configured, restart services. You must do this prior to updating user address information or provisioning new users. Make sure to follow the prescribed order when you restart services.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Enable High Availability, on page 40</td>
<td>You can enable high availability for the presence redundancy groups after you have configured the IM addressing scheme and restarted IM and Presence services. All services must be running on IM and Presence database publisher nodes and subscriber nodes before you enable high availability.</td>
</tr>
</tbody>
</table>
| Step 7 | If you chose **Directory URI** as the IM addressing scheme:  
  - Assign the LDAP Source for Directory URIs, on page 41  
  - Manually Assign a Directory URI, on page 41 | Optional. If you are syncing users from an external LDAP directory, set the LDAP source field for your directory URI values. For non-LDAP users, you must provision directory URIs manually. You can do this on a user-by-user basis, or via the Bulk Administration Tool. |
Verify User Provisioning

Use this procedure to verify that end users are correctly provisioned before you configure the addressing scheme.

Procedure

Step 1   From Cisco Unified CM IM and Presence Administration, choose Diagnostics > System Troubleshooter. The System Troubleshooter runs.
Step 2   In the User Troubleshooter section, verify that end users are correctly provisioned and that there are no duplicate or invalid users.

What to do next

Disable High Availability, on page 36

Disable High Availability

Disable High Availability in each presence redundancy group in your cluster. Editing the addressing scheme requires you to stop services temporarily. If you stop services with High Availability enabled, a system failover occurs.

Before you begin

Take a record of the number of active users for each cluster node in each Presence Redundancy Group. You can find this information in the (System > Presence Topology) window of Cisco Unified CM IM and Presence Administration. You will need these numbers later when you re-enable High Availability.

Procedure

Step 1   From the Cisco Unified CM Administration user interface, choose System > Presence Redundancy Groups.
Step 2   Click Find and select the group.
Step 3   On the Presence Redundancy Group Configuration window, uncheck the Enable High Availability check box.
Step 4   Click Save.
Step 5   Repeat this procedure for each Presence Redundancy Group.
Step 6   When you are done, wait at least two minutes to sync the new HA settings across the cluster before you make any further changes.

What to do next

Stop Services, on page 37
Stop Services

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

**Before you begin**

Disable High Availability, on page 36

**Procedure**

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

**Step 2**
Stop the following IM and Presence Services, in this order, by selecting the service and clicking the Stop button:
- a) Cisco Sync Agent
- b) Cisco Client Profile Agent

**Step 3**
After both services have stopped, choose Tools > Control Center – Feature Services and stop the following services in this order:
- a) Cisco Presence Engine
- b) Cisco SIP Proxy

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

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

---

**What to do next**

Assign IM Addressing Scheme, on page 37

**Assign IM Addressing Scheme**

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

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

**Before you begin**

Stop Services, on page 37
Procedure

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

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

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

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

  **Note**  When you choose this option, all deployed clients must support Directory URI as the IM address and use either EDI-based or UDS-based directory integration. For UDS-based integration with Jabber, you must be running Jabber Release 10.6 or later.

Step 4  Click Save.

You can monitor the progress of the update in the status area.

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

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

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

What to do next

If you configured user@default_domain as the addressing scheme, and you are not using the Directory URI, then proceed to Restart Services, on page 39.

If you configured Directory URI as the addressing scheme, choose on of the following options:

  • Assign the LDAP Source for Directory URIs, on page 41
  • Manually Assign a Directory URI, on page 41

**IM Address Examples**

Sample IM address options that are available for IM and Presence Service.
**IM and Presence Service Default Domain:** cisco.com

**User:** John Smith

**User ID:** js12345

**Mail ID:** jsmith@cisco-sales.com

**SIPURI:** john.smith@webex.com

<table>
<thead>
<tr>
<th>IM Address Format</th>
<th>Directory URI Mapping</th>
<th>IM Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;userid&gt;@&lt;domain&gt;</td>
<td>n/a</td>
<td><a href="mailto:js12345@cisco.com">js12345@cisco.com</a></td>
</tr>
<tr>
<td>Directory URI</td>
<td>mailid</td>
<td><a href="mailto:jsmith@cisco-sales.com">jsmith@cisco-sales.com</a></td>
</tr>
<tr>
<td>Directory URI</td>
<td>msRTCSIP-PrimaryUserAddress</td>
<td><a href="mailto:john.smith@webex.com">john.smith@webex.com</a></td>
</tr>
</tbody>
</table>

## Restart Services

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

### Before you begin

- Assign IM Addressing Scheme, on page 37
- If you configured Directory URI as the addressing scheme, complete one of the following options before you restart services:
  - Assign the LDAP Source for Directory URIs, on page 41
  - Manually Assign a Directory URI, on page 41

### Procedure

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

**Step 2**
Start the following service by selecting the service and clicking the Start button:
- Cisco XCP Router

**Step 3**
After the service starts, choose Tools > Control Center – Feature Services and start the following services in this order:
  a) Cisco SIP Proxy
  b) Cisco Presence Engine

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

**Step 5**
Choose Tools > Control Center – Network Services and start the following services in this order:
  a) Cisco Client Profile Agent
Enable High Availability

After you have configured your IM addressing scheme and restarted services, use this procedure to re-enable high availability for each presence redundancy group in your cluster.

Before you begin

All services must be running on IM and Presence database publisher nodes and subscriber nodes before you enable high availability. If it has been less than 30 minutes since your services restarted, confirm that your Cisco Jabber sessions have been recreated before you enable High Availability. Otherwise, Presence won't work for Jabber clients whose sessions aren't created.

To obtain the number of Cisco Jabber sessions, run the `show perf query counter Cisco Presence Engine Active JsmSessions` CLI command on all cluster nodes. The number of active sessions should match the number of users that you recorded when you disabled high availability.

Procedure

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

**Step 2**
From the **Server** list, choose the node on which you want to reactivate services and click **Go**.

**Step 3**
In the **IM and Presence Services** area, select the following services:

- Cisco Client Profile Agent
- Cisco Sync Agent
- Cisco XCP Router

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

**Step 5**
From the **Related Links** drop-down list, select **Service Activation** and click **Go**.

**Step 6**
In the **IM and Presence Services** area, select the following services:

- Cisco SIP Proxy
- Cisco Presence Engine

**Step 7**
Click **Save**.
Assign the LDAP Source for Directory URIs

If you are syncing users from an external LDAP directory, you can use this procedure to assign the external LDAP Directory source field that is used to assign the directory URI. When your LDAP directory sync occurs, the directory URI will be assigned from the value of the field that you configure.

Note

You cannot apply edits to an existing LDAP configuration in Cisco Unified Communications Manager if the initial sync has already occurred. You can sync new items that were added to the external LDAP directory, but you cannot edit the LDAP configuration in Cisco Unified Communications Manager. If you've already synced your LDAP directory:

- Use the Bulk Administration Tool to assign directory URIs to users. For details, see the Bulk Administration Guide for Cisco Unified Communications Manager.
- Assign the directory URI to a user manually

Before you begin

Assign IM Addressing Scheme, on page 37

Procedure

Step 1

From Cisco Unified CM Administration, select System > LDAP > LDAP Directory.

Step 2

From the Directory URI drop-down list, select one of the following options:

- **mail**: Map the Directory URI to the user's email address to provide a consistent identity for email, IM, voice and video communications.
- **msRTCSIP-PrimaryUserAddress**: Map the Directory URI to the Microsoft OCS/Lync SIP URI.

Note

The directory URI isn't provisioned until the LDAP sync occurs. For details on configuring an LDAP Directory sync, see Configure LDAP Directory, on page 65.

What to do next

Restart Services, on page 39

Manually Assign a Directory URI

If you are not using LDAP, you can use this procedure to enter a Directory URI manually on a user-by-user basis.
You can also use the Bulk Administration Tool to provision directory URIs for a large number of end users via a csv file. For Bulk Administration details, see the Bulk Administration Guide for Cisco Unified Communications Manager at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

If you haven't yet synced your LDAP directory, you can provision directory URIs for users via an LDAP directory sync.

**Before you begin**

Assign IM Addressing Scheme, on page 37

**Procedure**

- **Step 1** In Cisco Unified CM Administration, choose User Management > End User.
- **Step 2** Enter the appropriate search criteria and click Find.
- **Step 3** Select the end user that you want to configure.
- **Step 4** In the User Information area, enter a directory URI in the Directory URI field.
- **Step 5** Click Save.

**What to do next**

Restart Services, on page 39
Configure Redundancy

- Presence Redundancy Group Overview, on page 43
- Presence Redundancy Group Prerequisites, on page 44
- Presence Redundancy Group Task Flow, on page 44
- Initiate Manual Failover, Fallback, or Recovery, on page 49
- Redundancy Interactions and Restrictions, on page 56

Presence Redundancy Group Overview

A presence redundancy group is comprised of two IM and Presence Service nodes from the same cluster. Each node in the presence redundancy group monitors the status, or heartbeat, of the peer node. You can configure a presence redundancy group to provide both redundancy and recovery for IM and Presence Service clients and applications.

- Failover—Occurs in a presence redundancy group when one or more critical services fail on an IM and Presence Service node in the group or a node in the group fails. Clients automatically connect to the other IM and Presence Service node in that group.

- Fallback—Occurs when a fallback command is issued from the CLI or Cisco Unified Communications Manager during either of these conditions:
  - The failed IM and Presence Service node comes back into service and all critical services are running. The failed-over clients in that group reconnect with the recovered node when it becomes available.
  - The backup activated IM and Presence Service node fails due to a critical service failure, and the peer node is in the Failed Over state and supports the automatic recovery fallback.

For example, if you are using presence redundancy groups, Cisco Jabber clients will fail over to a backup IM and Presence Service node if the services or hardware fail on the local IM and Presence Service node. When the failed node comes online again, the clients automatically reconnect to the local IM and Presence Service node if you have configured automatic fallback. If you have not configured automatic fallback, you can manually initiate the fallback when the failed node comes online.

In addition to redundancy and recovery, presence redundancy groups also allow you to configure high availability for your cluster.
High Availability

The IM and Presence Service supports high availability for multiple-node deployments.

After you configure a presence redundancy group, you can enable high availability for the group. A pair of nodes is required for high availability. Each node has an independent database and set of users operating with a shared availability database that is able to support common users.

All IM and Presence Service nodes must belong to a presence redundancy group, which can consist of a single IM and Presence Service node or a pair of IM and Presence Service nodes.

You can configure high availability using two different modes:

- Balanced mode: This mode provides redundant high availability with automatic user load balancing and user failover in the event that one node fails because of component failure or power outage.
- Active/standby mode: The standby node automatically takes over for the active node if the active node fails. It does not provide automatic load balancing.

We recommend that you configure your IM and Presence Service deployments as high availability deployments. Although you are permitted to have both high availability and non-high availability presence redundancy groups configured in a single deployment, this configuration is not recommended.

Presence Redundancy Group Prerequisites

For deployments over the WAN, a minimum of 10 megabits per second of dedicated bandwidth is required for each IM and Presence Service cluster, with no more than an 80-millisecond round-trip latency. Any bandwidth less than this recommendation can adversely impact performance.

Presence Redundancy Group Task Flow

An IM and Presence Service node can be assigned to only one presence redundancy group. For high availability, you must assign two nodes from the same cluster to the presence redundancy group and enable high availability for the group.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Verify Database Replication, on page 45</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Verify Services, on page 45</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configure a Presence Redundancy Group, on page 46</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configure Heartbeat Interval for Failover, on page 47</td>
</tr>
</tbody>
</table>
Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer node. You can configure the intervals by which each node monitors its peer.</td>
<td></td>
</tr>
</tbody>
</table>

Step 5  
Enable High Availability, on page 48  
Optional. Follow this procedure if you did not enable high availability when you configured the presence redundancy group.

Step 6  
Configure User Assignment Mode, on page 49  
Configure how you want the Sync Agent to distribute users across various nodes in the IM and Presence Service cluster. This setting affects how your system handles failover and load balancing.

Verify Database Replication

Ensure that database replication is setup in the IM and Presence Service cluster before you enable high availability for a presence redundancy group.

Procedure

Step 1  
Start a CLI session using one of the following methods:

• From a remote system, use SSH to connect securely to the Cisco Unified Operating System. In your SSH client, enter your `ssh adminname@hostname` and enter your password.

• From a direct connection to the serial port, enter your credentials at the prompt that displays automatically.

Step 2  
Execute the `utils dbreplication status` command to check for errors or mismatches in the database tables.

Step 3  
Execute the `utils dbreplication runtimestate` command to check if the database replication is active on the node.

The output lists all the nodes and if database replication is set up and in a good state, the `replication setup` value for each node is 2.

If a value other than 2 is returned, you must resolve the errors before proceeding.

What to do next
Verify Services, on page 45

Verify Services

Make sure critical services are running on the nodes that you plan to add to a presence redundancy group.

Critical services must be running before you turn on high availability. If critical services are not running on either node, the presence redundancy group will go into a Failed state when you turn on high availability. If critical services are not running on one node, then that node fails over to the other node when you turn on high availability.
Before you begin

Verify Database Replication, on page 45

Procedure

Step 1  From Cisco Unified IM and Presence Serviceability, choose Tools > Control Center - Network Services.
Step 2  From the Server list, choose the appropriate node and click Go.
Step 3  In the IM and Presence Services area, ensure that the following services are started:
  • Cisco Client Profile Agent
  • Cisco Sync Agent
  • Cisco XCP Router
Step 4  From the Related Links drop-down list, select Control Center - Network Services and click Go.
Step 5  In the IM and Presence Services area, ensure that the following services are started:
  • Cisco SIP Proxy
  • Cisco Presence Engine

What to do next

Configure a Presence Redundancy Group, on page 46

Configure a Presence Redundancy Group

Use Cisco Unified Communications Manager to configure redundancy for IM and Presence Service nodes.
Each presence redundancy group can contain two IM and Presence Service nodes. Each node can be assigned to only one presence redundancy group. Both nodes in the presence redundancy group must be on the same cluster and have the same IM and Presence Service database publisher node.

Before you begin

• Verify Services, on page 45
  • Ensure that the IM and Presence Service nodes you are adding to a presence redundancy group are running the same software version.

Procedure

Step 1  From Cisco Unified CM Administration, choose System > Presence Redundancy Groups.
Step 2  Click Add New.
Step 3  Enter a unique name for the presence redundancy group.
You can enter a maximum of 128 alphanumeric characters, including underscore (_) and dash (-).

**Step 4**
Enter a description of the group.
You can enter a maximum of 128 alphanumeric characters including symbols, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), forward slash (/), or angle brackets (<>).

**Step 5**
Choose two different IM and Presence Service nodes in the Presence Server fields to assign them to the group.

**Step 6**
(Optional) Check the Enable High Availability check box to enable high availability for the presence redundancy group.

**Step 7**
Click Save.

---

**What to do next**

Configure Heartbeat Interval for Failover, on page 47

---

### Configure Heartbeat Interval for Failover

Configure optional service parameters that determine the keep alive settings by which each peer in a presence redundancy group monitors the heartbeat (i.e., the status) of its peer node in order to confirm that the peer is active. A failover can be initiated if the peer node is unresponsive after a configured timer expires.

---

**Note**
Cisco recommends that you use the default values for these service parameters. However, you can also reconfigure the values to suit your needs.

---

**Procedure**

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

2. **Step 2**
   From the Server drop-down, select an IM and Presence node.

3. **Step 3**
   From the Service drop-down, select Cisco Server Recovery Manager (Active).

4. **Step 4**
   Under General Server Recovery Manager Parameters (Clusterwide), configure the clusterwide Keep Alive settings that each node in a Presence Redundancy Group uses to monitor the heartbeat of its peer node. A failover can be initiated if the peer node is unresponsive.

   - **Service Port**—This parameter specifies the port that Cisco Server Recovery Manager uses to communicate with its peer. The default is 22001.
   - **Admin RPC Port**—This parameter specifies the port that Cisco Server Recovery Manager uses to provide admin rpc requests. The default is 20075.
   - **Critical Service Delay**—This parameter specifies the duration in seconds that a critical service can be down before failover is initiated. The default is 90.
   - **Enable Automatic Fallback**—This parameter specifies whether to do automatic fallback. In the event of a failover, the IM and Presence Service moves users automatically from the backup node to the primary node thirty minutes after the primary node returns to a healthy state. The default value is False.
   - **Initialization Keep Alive (Heartbeat) Timeout**—This parameter specifies the duration in seconds that the heartbeat can be lost with the peer during initialization before failover is initiated. The default is 120.
• **Keep Alive (Heartbeat) Timeout**—This parameter specifies the duration in seconds that the heartbeat can be lost with the peer before failover is initiated. The default is 60.

• **Keep Alive (HeartBeat) Interval**—This parameter specifies the interval in seconds between keep alive (heart beat) messages being sent to the peer. The default is 15.

**Step 5** Configure the following additional parameters, which tell CUPC 8.5 and higher clients how long to wait before attempting to relogin. Unlike the above parameters, these parameters must be configured separately for each cluster node.

• **Client Re-Login Lower Limit**—This parameter specifies the minimum number of seconds which CUPC 8.5 (and higher) should wait before attempting to re-login to this server. The default is 120.

• **Client Re-Login Upper Limit**—This parameter specifies the maximum number of seconds which CUPC 8.5 (and higher) should wait before attempting to re-login to this server. The default is 537.

**Step 6** Click Save.

---

**What to do next**
If you did not enable high availability when you configured the presence redundancy group, [Enable High Availability, on page 48](#).

---

**Enable High Availability**

⚠️ **Caution**
Failure to set up replication in the IM and Presence Service cluster and ensure that all critical services are running may result in an immediate failover when high availability is enabled for the presence redundancy group.

---

**Before you begin**

• [Configure a Presence Redundancy Group, on page 46](#)

• Ensure that replication is set up in the IM and Presence Service cluster.

• Ensure that all critical services are running.

**Procedure**

**Step 1** From [Cisco Unified CM Administration](#), choose System > Presence Redundancy Groups.

**Step 2** Specify search criteria and then click **Find**.

**Step 3** Choose the presence redundancy group that you configured.

**Step 4** To enable high availability, check the **Enable High Availability** check box.

**Step 5** Click **Save**.
Configure User Assignment Mode

Use this procedure to configure the way in which the sync agent distributes users to the nodes in the cluster. This setting helps to manage failover and load balancing.

**Procedure**

**Step 1**
From Cisco Unified CM Administration, choose System > Enterprise Parameters.

**Step 2**
In the User Management Parameters Area, choose one of the following options for the User Assignment Mode for Presence Server parameter:

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

**Step 3**
Click Save.

Initiate Manual Failover, Fallback, or Recovery

Use this procedure to initiate manual failover, fallback, or recovery of IM and Presence Service nodes within a presence redundancy group.

- **Manual failover**—When you initiate a manual failover, the Cisco Server Recovery Manager stops the critical services on the failed node. All users from the failed node are disconnected and must re-login to the backup node. Critical services will not be restarted unless we invoke manual fallback.

- **Manual fallback**—When you initiate a manual fallback, the Cisco Server Recovery Manager restarts critical services on the primary node and disconnects all users that had been failed over. Those users must then re-login to their assigned node.

- **Manual recovery**—A manual recovery is necessary when both nodes in the presence redundancy group are in the failed state. In this case, the IM and Presence Service restarts the Cisco Server Recovery Manager service on both nodes in the presence redundancy group.

**Procedure**

**Step 1**
From Cisco Unified CM Administration, choose System > Presence Redundancy Groups.

**Step 2**
Click Find and select the Presence Redundancy Group with the applicable nodes.

**Step 3**
Do one of the following. Note that the available button depends on the current state of the node:

- Click **Failover** to initiate failover of an active node.
- Click **Fallback** to initiate fallback of a failed over node.
• Click **Recover** if both nodes are failed over and you want to recover them.

---

**Note**

You can also initiate these actions from Cisco Unified Communications Manager or IM and Presence Service using the CLI. See the *Command Line Interface Guide for Cisco Unified Communications Solutions* for details.

---

**Note**

You cannot add end users to an IM and Presence Service cluster while one of the nodes is in a failover state.

### Node State Definitions

**Table 3: Presence Redundancy Group Node State Definitions**

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initializing</td>
<td>This is the initial (transition) state when the Cisco Server Recovery Manager service starts; it is a temporary state.</td>
</tr>
<tr>
<td>Idle</td>
<td>IM and Presence Service is in Idle state when failover occurs and services are stopped. In Idle state, the IM and Presence Service node does not provide any availability or Instant Messaging services. In Idle state, you can manually initiate a fallback to this node using the <em>Cisco Unified CM Administration</em> user interface.</td>
</tr>
<tr>
<td>Normal</td>
<td>This is a stable state. The IM and Presence Service node is operating normally. In this state, you can manually initiate a failover to this node using the <em>Cisco Unified CM Administration</em> user interface.</td>
</tr>
<tr>
<td>Running in Backup Mode</td>
<td>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.</td>
</tr>
<tr>
<td>Taking Over</td>
<td>This is a transition state. The IM and Presence Service node is taking over for its peer node.</td>
</tr>
<tr>
<td>Failing Over</td>
<td>This is a transition state. The IM and Presence Service node is being taken over by its peer node.</td>
</tr>
<tr>
<td>Failed Over</td>
<td>This is a steady state. The IM and Presence Service node has failed over, but no critical services are down. In this state, you can manually initiate a fallback to this node using the <em>Cisco Unified CM Administration</em> user interface.</td>
</tr>
<tr>
<td>Failed Over with Critical Services Not Running</td>
<td>This is a steady state. Some of the critical services on the IM and Presence Service node have either stopped or failed.</td>
</tr>
<tr>
<td>Falling Back</td>
<td>This is a transition state. The system is falling back to this IM and Presence Service node from the node that is running in backup mode.</td>
</tr>
<tr>
<td>Taking Back</td>
<td>This is a transition state. The failed IM and Presence Service node is taking back over from its peer.</td>
</tr>
</tbody>
</table>
An error occurs during the transition states or Running in Backup Mode state.

Unknown

Node state is unknown.

A possible cause is that high availability was not enabled properly on the IM and Presence Service node. Restart the Server Recovery Manager service on both nodes in the presence redundancy group.

### Node States, Causes, and Recommended Actions

You can view the status of nodes in a presence redundancy group on the **Presence Redundancy Group Configuration** window when you choose a group using the **Cisco Unified CM Administration** user interface.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running in Failed Mode</td>
<td>An error occurs during the transition states or Running in Backup Mode state.</td>
</tr>
<tr>
<td>Unknown</td>
<td>Node state is unknown. A possible cause is that high availability was not enabled properly on the IM and Presence Service node. Restart the Server Recovery Manager service on both nodes in the presence redundancy group.</td>
</tr>
</tbody>
</table>

### Table 4: Presence Redundancy Group Node High-Availability States, Causes, and Recommended Actions

<table>
<thead>
<tr>
<th>State</th>
<th>Reason</th>
<th>Reason</th>
<th>Cause/Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>Failing Over</td>
<td>On Admin Request</td>
<td>Taking Over</td>
<td>The administrator initiated a manual failover from node 1 to node 2. The manual failover is in progress.</td>
</tr>
<tr>
<td>Idle</td>
<td>On Admin Request</td>
<td>Running in Backup Mode</td>
<td>The manual failover from node 1 to node 2 that the administrator initiated is complete.</td>
</tr>
<tr>
<td>Taking Back</td>
<td>On Admin Request</td>
<td>Falling Back</td>
<td>The administrator initiated a manual fallback from node 2 to node 1. The manual fallback is in progress.</td>
</tr>
<tr>
<td>Idle</td>
<td>Initialization</td>
<td>Running in Backup Mode</td>
<td>The administrator restarts the SRM service on node 1 while node 1 is in “Idle” state.</td>
</tr>
<tr>
<td>Idle</td>
<td>Initialization</td>
<td>Initialization</td>
<td>The administrator either restarts both nodes in the presence redundancy group, or restarts the SRM service on both nodes while the presence redundancy group was in manual failover mode.</td>
</tr>
<tr>
<td>Idle</td>
<td>On Admin Request</td>
<td>Running in Backup Mode</td>
<td>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.</td>
</tr>
<tr>
<td>Failing Over</td>
<td>On Admin Request</td>
<td>Taking Over</td>
<td>The administrator restarts the SRM service on node 2 while node 2 is taking over, but before the heartbeat on node 1 times out.</td>
</tr>
</tbody>
</table>
### Node States, Causes, and Recommended Actions

<table>
<thead>
<tr>
<th>Node 1</th>
<th>Node 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State</strong></td>
<td><strong>Reason</strong></td>
</tr>
<tr>
<td>Taking Back</td>
<td>Initialization</td>
</tr>
<tr>
<td>Taking Back</td>
<td>Automatic Fallback</td>
</tr>
</tbody>
</table>
| Failed Over | Initialization or Critical Services Down | Running in Backup Mode | Critical Service Down | Node 1 transitions to Failed Over state when either of the following conditions occur:  
  - Critical services come back up due to a reboot of node 1.  
  - The administrator starts critical services 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 presence redundancy group to Normal state. |
| Failed Over with Critical Services not Running | Critical Service Down | Running in Backup Mode | Critical Service Down | A critical service is down on node 1. IM and Presence Service performs an automatic failover to node 2.  
**Recommended Actions:**  
1. Check node 1 for any critical services that are down and try to manually start those services.  
2. If the critical services on node 1 do not start, then reboot node 1.  
3. When all the critical services are up and running after the reboot, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state. |
| Failed Over with Critical Services not Running | Database Failure | Running in Backup Mode | Database Failure | A database service is down on node 1. IM and Presence Service performs an automatic failover to node 2.  
**Recommended Actions:**  
1. Reboot node 1.  
2. When all the critical services are up and running after the reboot, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state. |
<table>
<thead>
<tr>
<th>State</th>
<th>Reason</th>
<th>State</th>
<th>Reason</th>
<th>Cause/Recommended Actions</th>
</tr>
</thead>
</table>
| Running in Failed Mode | Start of Critical Services Failed | Running in Failed Mode | Start of Critical Services Failed | Critical services fail to start while a node in the presence redundancy group is taking back from the other node.  
Recommendation actions: On the node that is taking back, perform the following actions:  
1. Check the node for critical services that are down. To manually start these services, click **Recovery** in the **Presence Redundancy Group Configuration** window.  
2. If the critical services do not start, reboot the node.  
3. When all the critical services are up and running after the reboot, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state. |
| Running in Failed Mode | Critical Service Down       | Running in Failed Mode | Critical Service Down       | Critical services go down on the backup node. Both nodes enter the failed state.  
**Recommended Actions:**  
1. Check the backup node for critical services that are down. To start these services manually, click **Recovery** in the **Presence Redundancy Group Configuration** window.  
2. If the critical services do not start, reboot the node. |
<table>
<thead>
<tr>
<th>Node 1</th>
<th>Node 2</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node 1 is down due to loss of network connectivity or the SRM service is not running.</td>
<td>Running in Backup Mode</td>
<td>Peer Down</td>
</tr>
<tr>
<td>Node 2 has lost the heartbeat from node 1. IM and Presence Service performs an automatic failover to node 2.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Recommended Action.** If node 1 is up, perform the following actions:

1. Check and repair the network connectivity between nodes in the presence redundancy group. When you reestablish the network connection between the nodes, the node may go into a failed state. Click **Recovery** in the **Presence Redundancy Group Configuration** window to restore the nodes to the Normal state.

2. Start the SRM service and perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state.

3. (If the node is down) Repair and power up node 1.

4. When the node is up and all critical services are running, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state.

<table>
<thead>
<tr>
<th>Node 1</th>
<th>Node 2</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node 1 is down (due to possible power down, hardware failure, shutdown, reboot)</td>
<td>Running in Backup Mode</td>
<td>Peer Reboot</td>
</tr>
<tr>
<td>IM and Presence Service performs an automatic failover to node 2 due to the following possible conditions on node 1:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• hardware failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• power down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• restart</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• shutdown</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Recommended Actions:**

1. Repair and power up node 1.

2. When the node is up and all critical services are running, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state.
### Node States, Causes, and Recommended Actions

<table>
<thead>
<tr>
<th>Node 1</th>
<th>Node 2</th>
<th>Reason</th>
<th>State</th>
<th>Reason</th>
<th>Cause/Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed Over with Critical Services not Running OR Failed Over</td>
<td>Initialization</td>
<td>Backup Mode</td>
<td>Peer Down During Initialization</td>
<td>Node 2 does not see node 1 during startup. <strong>Recommended Action:</strong> When node 1 is up and all critical services are running, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state.</td>
<td></td>
</tr>
<tr>
<td>Running in Failed Mode</td>
<td>Cisco Server Recovery Manager Take Over Users Failed</td>
<td>Running in Failed Mode</td>
<td>Cisco Server Recovery Manager Take Over Users Failed</td>
<td>User move fails during the taking over process. <strong>Recommended Action:</strong> Possible database error. Click <strong>Recovery</strong> in the <strong>Presence Redundancy Group Configuration</strong> window. If the problem persists, then reboot the nodes.</td>
<td></td>
</tr>
<tr>
<td>Running in Failed Mode</td>
<td>Cisco Server Recovery Manager Take Back Users Failed</td>
<td>Running in Failed Mode</td>
<td>Cisco Server Recovery Manager Take Back Users Failed</td>
<td>User move fails during falling back process. <strong>Recommended Action:</strong> Possible database error. Click <strong>Recovery</strong> in the <strong>Presence Redundancy Group Configuration</strong> window. If the problem persists, then reboot the nodes.</td>
<td></td>
</tr>
<tr>
<td>Running in Failed Mode</td>
<td>Unknown</td>
<td>Running in Failed Mode</td>
<td>Unknown</td>
<td>The SRM on a node restarts while the SRM on the other node is in a failed state, or an internal system error occurs. <strong>Recommended Action:</strong> Click <strong>Recovery</strong> in the <strong>Presence Redundancy Group Configuration</strong> window. If the problem persists, then reboot the nodes.</td>
<td></td>
</tr>
<tr>
<td>Backup Activated</td>
<td>Auto Recover Database Failure</td>
<td>Failover Affected Services</td>
<td>Auto Recovery Database Failure</td>
<td>The database goes down on the backup node. The peer node is in failover mode and can take over for all users in the presence redundancy group. Auto-recovery operation automatically occurs and all users are moved over to the primary node.</td>
<td></td>
</tr>
<tr>
<td>Backup Activated</td>
<td>Auto Recover Database Failure</td>
<td>Failover Affected Services</td>
<td>Auto Recover Critical Service Down</td>
<td>A critical service goes down on the backup node. The peer node is in failover mode and can take over for all users in the presence redundancy group. Auto-recovery operation automatically occurs and all users are moved over to the peer node.</td>
<td></td>
</tr>
</tbody>
</table>
### Redundancy Interactions and Restrictions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding Users</td>
<td>You cannot add new users to an IM and Presence Service cluster while one of the cluster nodes is in a failover state.</td>
</tr>
<tr>
<td>Multiple Device Messaging</td>
<td>The Multiple Device Messaging feature causes a delay with server recovery on the IM and Presence Service if failover occurs. If server failover occurs on a system where Multiple Device Messaging is configured, the failover times generally are twice as long as the times specified with the Cisco Server Recovery Manager service parameters.</td>
</tr>
</tbody>
</table>
High Availability is supported for Push Notifications deployments as of 11.5(1)SU3. If Push Notifications is enabled, and a node fails over, the following occurs for Cisco Jabber on iPhone and iPad clients:

- For Cisco Jabber clients in foreground mode, the Jabber client logs in automatically to the backup node, which takes over until the main node recovers. There is no interruption in services, either when the backup node takes over, or when the main node recovers.

- For Cisco Jabber clients in background mode, the backup node takes over, but there is a delay before any Push Notifications are sent. Because the Jabber client is in background mode, it does not have an active connection to the network so it doesn’t log in automatically to the backup node. The backup node must recreate JSM sessions for all failed over users who were in background mode before any Push Notifications can be sent.

The length of the delay depends on the system load. Testing has shown that for a 15,000 user OVA with users evenly distributed in an HA pair, it takes 10-20 minutes for Push Notifications to be sent following a failover. This delay is observed when the backup node takes over, and again after the main node recovers.

In the event of a node failure or unexpected crash of the Cisco XCP Router, the user's IM session, including the IM history, is maintained without the need for any user action. However, if the Cisco Jabber on iPhone or iPad client was in suspended mode, it will be unable to retrieve unread messages that were queued on the server when it crashed.

### Table: Push Notifications High Availability

<table>
<thead>
<tr>
<th>Feature</th>
<th>Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Push Notifications High</td>
<td>High Availability is supported for Push Notifications deployments as of 11.5(1)SU3. If Push Notifications is enabled, and a node fails over,</td>
</tr>
<tr>
<td>Availability</td>
<td>the following occurs for Cisco Jabber on iPhone and iPad clients:</td>
</tr>
<tr>
<td></td>
<td>- For Cisco Jabber clients in foreground mode, the Jabber client logs in automatically to the backup node, which takes over until the</td>
</tr>
<tr>
<td></td>
<td>main node recovers. There is no interruption in services, either when the backup node takes over, or when the main node recovers.</td>
</tr>
<tr>
<td></td>
<td>- For Cisco Jabber clients in background mode, the backup node takes over, but there is a delay before any Push Notifications are sent.</td>
</tr>
<tr>
<td></td>
<td>Because the Jabber client is in background mode, it does not have an active connection to the network so it doesn’t log in automatically</td>
</tr>
<tr>
<td></td>
<td>to the backup node. The backup node must recreate JSM sessions for all failed over users who were in background mode before any Push</td>
</tr>
<tr>
<td></td>
<td>Notifications can be sent.</td>
</tr>
<tr>
<td></td>
<td>The length of the delay depends on the system load. Testing has shown that for a 15,000 user OVA with users evenly distributed in an HA pair,</td>
</tr>
<tr>
<td></td>
<td>it takes 10-20 minutes for Push Notifications to be sent following a failover. This delay is observed when the backup node takes over,</td>
</tr>
<tr>
<td></td>
<td>and again after the main node recovers.</td>
</tr>
<tr>
<td></td>
<td>Note: In the event of a node failure or unexpected crash of the Cisco XCP Router, the user's IM session, including the IM history,</td>
</tr>
<tr>
<td></td>
<td>is maintained without the need for any user action. However, if the Cisco Jabber on iPhone or iPad client was in suspended mode, it will</td>
</tr>
<tr>
<td></td>
<td>be unable to retrieve unread messages that were queued on the server when it crashed.</td>
</tr>
</tbody>
</table>
Configure User Settings

- End User Settings Overview, on page 59
- User Settings Prerequisites, on page 60
- Configure User Settings Task Flow, on page 60

End User Settings Overview

You can use user settings such as Service Profiles and Feature Group Templates to apply common settings to your end users via an LDAP Directory sync. When the LDAP Directory sync occurs the configured settings get applied to all synced users.

Note

This chapter covers user settings that apply to the IM and Presence Service, specifically. For general UC user configurations, including UC services such as voicemail and conferencing, refer to the "Configure End Users" section of the System Configuration Guide for Cisco Unified Communications Manager. You can apply these configurations as a part of your LDAP sync.

Service Profiles

A service profile contains common Unified Communications (UC) Services settings. You can configure different service profiles for different groups of users so that each group of users has the appropriate services configured for their job. To enable end users to access the IM and Presence Service configure the service profile so that it includes the IM and Presence Service.

You can use the following methods to apply a service profile to an end user:

- For LDAP Synchronized Users—If you have imported end users from an LDAP directory, you can assign the service profile to a feature group template and then apply that feature group template to your end users. The settings in the template get applied to all synchronized users.

- For Active Local Users (i.e. non-LDAP users)—To apply settings to a large number of users at once, use the Bulk Administration Tool to apply service profile settings via a csv file or spreadsheet. For details on how to use the Bulk Administration Tool at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Otherwise, you can configure user settings manually, on a user-by-user basis.
Feature Group Template Overview

Feature group templates help you to quickly apply common settings to groups of end users via an LDAP directory sync. For example, you can use the Feature Group Template to enable the IM and Presence Service for your end users. This is accomplished by applying an IM and Presence-enabled Service Profile to the template. When you apply the feature group template to an LDAP directory sync, when the sync occurs the settings from the template, including the configured Service Profile and User Profile settings, get applied to all synced users.

Feature group template configuration includes the following profiles that you can assign to the feature group template:

- **User Profile**—contains a set of common phone and phone line settings. You must configure the user profile with a universal line template, which assigns the common phone line settings, and a universal device template, which assigns the common phone settings. These templates assist users who are set up for self-provisioning to configure their own phones.

- **Service Profile**—contains a group of common UC services, such as the IM and Presence Service, directory, or voicemail.

User Settings Prerequisites

If you want to move users between IM and Presence Service clusters, you must do so before you configure end users. For information about how to use Cisco Unified CM IM and Presence Administration to migrate users, and export or import contact lists, see Migrate Users, on page 239.

**Note**

Migrating users between clusters should not be confused with the User Migration Tool used for Partitioned Intra-domain Federation.

Configure User Settings Task Flow

Complete these tasks to configure user templates with common service and feature settings, such as enabling end users for the IM and Presence Service. When you complete an LDAP sync, your template settings will be applied to your end users.

**Note**

This chapter task flow user settings that apply to the IM and Presence Service, specifically. For general UC user configurations, including UC services such as voicemail and conferencing, refer to the "Configure End Users" section of the System Configuration Guide for Cisco Unified Communications Manager. You can apply these configurations as a part of your LDAP sync.
Configure the User Assignment Mode

Use this procedure to configure the way in which the sync agent will distribute users to the nodes in the cluster.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Configure the User Assignment Mode, on page 61</td>
<td>Set the user assignment mode to balanced, active-stand-by, or none.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Add an IM and Presence UC Service, on page 61</td>
<td>Set up an IM and Presence UC service on Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure a Service Profile, on page 62</td>
<td>Configure a service profile that contains the IM and Presence UC service that you added.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure a Feature Group Template, on page 63</td>
<td>Configure a feature group template that includes the service profile that you set up in addition to other common feature settings.</td>
</tr>
</tbody>
</table>

What to do next

Complete an LDAP sync to apply the settings to LDAP-synchronized users.

Add an IM and Presence UC Service

Use this procedure in Cisco Unified Communications Manager add a UC service for the IM and Presence Service.
Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management > User Settings > UC Service.**
Step 2 Click **Add New.**
Step 3 From the **UC Service Type** drop-down list box, choose **IM and Presence.**
Step 4 From the **Product Type** drop-down list box, choose **Unified CM (IM and Presence).**
Step 5 Enter a **Name** and **Description** for the IM and Presence service.
Step 6 In the **Hostname/IP Address** field, enter a hostname, IP address, or DNS SRV for the server that hosts the IM and Presence Service.
Step 7 Click **Save.**

What to do next
To enable users for the IM and Presence Service, assign the UC Service to a Service Profile and assign that profile to your users.

Configure a Service Profile, on page 62.

Configure a Service Profile

Use this procedure to configure a service profile that contains the IM and Presence Service.

**Before you begin**

Add an IM and Presence UC Service, on page 61

**Procedure**

Step 1 From Cisco Unified CM Administration, choose **User Management > User Settings > Service Profile.**
Step 2 Do either of the following
- Click **Find** and select an existing profile
- Click **Add New** to create a new profile
Step 3 In the **IM and Presence Profile** section, select the **Primary** IM and Presence server.
Step 4 Complete the remaining fields in the **Service Profile Configuration** window. For help with the fields and their settings, see the online help
Step 5 Click **Save.**

What to do next

Configure a Feature Group Template, on page 63
Configure a Feature Group Template

Configure a feature group template that includes common feature settings as well as the IM and Presence-enabled service profile that you set up.

Before you begin
Configure a Service Profile, on page 62

Procedure

Step 1 In Cisco Unified CM Administration, choose User Management > User/Phone Add > Feature Group Template.
Step 2 Click Add New.
Step 3 Check the Home Cluster check box if you want to use the local cluster as the home cluster for all users whom use this template.
Step 4 Check the Enable Users for Unified CM IM and Presence check box to allow users whom use this template to exchange instant messaging and presence information.
Step 5 From the drop-down menus, select a Service Profile and User Profile.
Step 6 Complete the remaining fields in the Feature Group Template Configuration window. Refer to the online help for field descriptions.
Step 7 Click Save.

What to do next
Configure an LDAP Directory sync that includes this feature group template. When you complete the LDAP Sync, the IM and Presence settings in the template get applied to synchronized users. See LDAP Synchronization Configuration Task Flow, on page 67.
Configure a Feature Group Template
CHAPTER 7

Configure LDAP Directory

- LDAP Synchronization Overview, on page 65
- LDAP Synchronization Prerequisites, on page 67
- LDAP Synchronization Configuration Task Flow, on page 67

LDAP Synchronization Overview

Lightweight Directory Access Protocol (LDAP) synchronization helps you to provision and configure end users for your system. During LDAP synchronization, the system imports a list of users and associated user data from an external LDAP directory into the Cisco Unified Communications Manager database. You can also configure your end users while the import occurs. In addition, a regular synchronization schedule picks up any changes in your employee data.

Note

Cisco Unified Communications Manager supports LDAPS (LDAP with SSL) but does not support LDAP with StartTLS. Ensure that you upload the LDAP server certificate to Cisco Unified Communications Manager as a Tomcat-Trust.

Importing End Users

You can use LDAP synchronization during the initial system set up to import your user list from a company LDAP directory into the Cisco Unified Communications Manager database. The LDAP synchronization process imports the list of users as well as user-specific data, such as phone numbers or email addresses, and stores the data in the corresponding fields in the End User Configuration window.

If you want to limit the LDAP import to a subset of users from the LDAP directory you can configure and apply an LDAP filter to your LDAP sync.

Configuring Imported End Users

If you have already configured items such as access control groups, credential policies and feature group templates, you can also configure your imported end users at the same time as the users are being imported. The LDAP Directory Configuration window allows you to configure the following items for your end users. Cisco Unified Communications Manager assigns these configurations to the imported end users while the synchronization occurs. For example, you can assign the following for your end users:

- Assign your end users to an access control group
• Assign a default credential policy
• Assign a universal line template to be applied to the user's primary extension
• Assign a universal device template to be applied to the user's phones
• Assign a primary extension
• Enable the user to provision his or her own phones

When applying configurations to your end users, make sure to use LDAP filters so that the end user configurations are applied only to those end users who meet specific requirements. You can set up additional LDAP directory configurations in Cisco Unified Communications Manager for other end users who meet the same criteria.

Scheduled Updates
You can configure Cisco Unified Communications Manager to synchronize with multiple LDAP directories at scheduled intervals to ensure that the database is updated regularly and that all user data stays current. For example, if you have a sync schedule set up and you update a phone number in the company LDAP directory, that update propagates to Cisco Unified Communications Manager automatically when the next scheduled LDAP sync occurs. Synchronization schedules help you to manage your company network on an ongoing basis by creating a single repository for you to manage and update employee data.

LDAP Authentication for End Users
LDAP synchronization allows you to configure your system to authenticate end user passwords against the LDAP directory rather than the Cisco Unified Communications Manager database. LDAP authentication provides companies with the ability to assign a single password to end users for all company applications. This functionality does not apply to PINs or application user passwords.

Directory Server User Search for Cisco Mobile and Remote Access Clients and Endpoints
In previous releases, when a user with a Cisco mobile and remote access client (for example, Cisco Jabber) or endpoint (for example, Cisco DX 80 phone) performed a user search while outside the enterprise firewall, results were based on those user accounts that are saved in the Cisco Unified Communications Manager database. The database contains user accounts which are either configured locally or synchronized from the corporate directory.

With this release, Cisco mobile and remote access clients and endpoints can now search a corporate directory server even when operating outside the enterprise firewall. When this feature is enabled, the User Data Service (UDS) acts as a proxy and sends the user search request to the corporate directory instead of sending it to the Cisco Unified Communications Manager database.

Use this feature to achieve the following results:
• Deliver the same user search results regardless of geographic location—Mobile and remote access clients and endpoints can perform user searches by using the corporate directory; even when they are connected outside the enterprise firewall.
• Reduce the number of user accounts that are configured in the Cisco Unified Communications Manager database—Mobile clients can now search users in the corporate directory. In the previous releases, user
search results were based on the users that are configured in the database. Now, administrators no longer need to configure or synchronize user accounts to the database solely for user searches. Administrators need to configure only those user accounts that are served by a cluster. Reducing the total number of user accounts in the database shortens software upgrade time frames while improving overall database performance.

To configure this feature, you must enable the Enable user search to Enterprise Directory Server option in the LDAP Search Configuration window, and configure the LDAP directory server details. For details, see the Configure Enterprise Directory User Search, on page 72 procedure.

LDAP Synchronization Prerequisites

**Prerequisite Tasks**

Before you import end users from an LDAP directory, complete the following tasks:

- Configure User Access
- Configure Credential Policy
- Configure Feature Group Template

For users whose data you want to synchronize to your system, ensure that their email ID fields on the active directory server are unique entries or left blank.

LDAP Synchronization Configuration Task Flow

Perform the following tasks to synchronize the Cisco Unified Communications Manager database with a company LDAP directory. LDAP synchronization allows you to pull a user list from the external LDAP directory and import it into the Cisco Unified Communications Manager database. This process helps administrators to provision end users during first time setup.

**Note**

If you have already synced the LDAP directory once, you can still sync new items from your external LDAP directory, but you cannot add new configurations in Cisco Unified Communications Manager to the LDAP directory sync. In this case, you can use the Bulk Administration Tool and menus such as Update Users or Insert Users. Refer to the Bulk Administration Guide for Cisco Unified Communications Manager.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Log in to Cisco Unified Serviceability and activate the Cisco DirSync service.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enable LDAP directory synchronization in Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 3</strong> Create an LDAP Filter, on page 70</td>
<td>Optional. Create an LDAP filter if you want Cisco Unified Communications Manager to synchronize only a subset of users from your corporate LDAP directory. For example, you could create a filter that imports only those users who belong to a specific access control group, or whom use a specific user profile.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Configure LDAP Directory Sync, on page 70</td>
<td>Configure settings for the LDAP directory sync such as field settings, LDAP server locations, synchronization schedules, and assignments for access control groups, feature group templates and primary extensions.</td>
</tr>
<tr>
<td><strong>Step 5</strong> Configure Enterprise Directory User Search, on page 72</td>
<td>Optional. Configure the system for enterprise directory server user searches. Follow this procedure to configure phones and clients in your system to perform user searches against an enterprise directory server instead of the database.</td>
</tr>
<tr>
<td><strong>Step 6</strong> Configure LDAP Authentication, on page 74</td>
<td>Optional. If you want to use the LDAP directory for end user password authentication, configure LDAP authentication settings.</td>
</tr>
</tbody>
</table>
| **Step 7** Customize LDAPS Agreement Service Parameters, on page 74 | Optional. Configure LDAPS Synchronization service parameters. For most deployments, the default values will be sufficient. However, you can reconfigure the following values:  
  • Maximum number of LDAP synchronization agreements  
  • Maximum number of LDAP hostnames for failover  
  • Delay timers for host failure or hostlist failure  
  • Connection timeouts  
  • Delays for LDAPS syncs |
| **Step 8** Convert LDAPS Synchronized User to Local User, on page 75 | Optional. If you need to update to an End User Configuration setting that is synchronized with an LDAP attribute, and you do not want to use the field from the LDAP directory, convert the LDAP user to a local user. |
**Activate the Cisco DirSync Service**

Perform this procedure to activate the Cisco DirSync Service in Cisco Unified Serviceability. You must activate this service if you want to synchronize end user settings from a corporate LDAP directory.

**Procedure**

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

**Step 2**
From the **Server** drop-down list box, choose the publisher node.

**Step 3**
Under **Directory Services**, click the **Cisco DirSync** radio button.

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

**What to do next**

Enable LDAP Directory Synchronization, on page 69

**Enable LDAP Directory Synchronization**

Perform this procedure if you want to configure Cisco Unified Communications Manager to synchronize end user settings from a corporate LDAP directory.

**Note**

If you have already synced the LDAP directory once, you can still sync new items from your external LDAP directory, but you cannot add new configurations in Cisco Unified Communications Manager to the LDAP directory sync. In this case, you can use the Bulk Administration Tool and menus such as Update Users or Insert Users. Refer to the *Bulk Administration Guide for Cisco Unified Communications Manager*.

**Before you begin**

Activate the Cisco DirSync Service, on page 69

**Procedure**

**Step 1**
In Cisco Unified CM Administration, choose **System > LDAP > LDAP System**.

**Step 2**
If you want Cisco Unified Communications Manager to import users from your LDAP directory, check the **Enable Synchronizing from LDAP Server** check box.

**Step 3**
From the **LDAP Server Type** drop-down list box, choose the type of LDAP directory server that your company uses.

**Step 4**
From the **LDAP Attribute for User ID** drop-down list box, choose the attribute from your corporate LDAP directory that you want Cisco Unified Communications Manager to synchronize with for the **User ID** field in **End User Configuration**.

**Step 5**
Click **Save**.
What to do next

Perform one of the following procedures:

• Create an LDAP Filter, on page 70 if you want to limit the LDAP sync to a subset of users.
• Configure LDAP Directory Sync, on page 70 to configure the LDAP directory.

Create an LDAP Filter

Perform this optional procedure if you want to create an LDAP filter to limit your LDAP synchronization to a subset of users from your LDAP directory. When you apply the LDAP filter to your LDAP directory, Cisco Unified Communications Manager imports only those users from the LDAP directory who match the filter.

Any LDAP filter that you configure must comply with the LDAP search filter standards that are specified in RFC4515.

Before you begin

Enable LDAP Directory Synchronization, on page 69

Procedure

Step 1 In Cisco Unified CM Administration, choose System > LDAP > LDAP Filter.
Step 2 Click Add New to create a new LDAP filter.
Step 3 In the Filter Name text box, enter a name for your LDAP filter.
Step 4 In the Filter text box, enter a filter. The filter can contain a maximum of 1024 UTF-8 characters and must be enclosed in parentheses ().
Step 5 Click Save.

What to do next

Go to Configure LDAP Directory Sync, on page 70 to apply the LDAP filter to an LDAP directory.

Configure LDAP Directory Sync

Use this procedure to configure Cisco Unified Communications Manager to synchronize with an LDAP directory. LDAP directory synchronization allows you to import end user data from an external LDAP directory into the Cisco Unified Communications Manager database such that it displays in End User Configuration window. You can set up a sync schedule so that updates made to the LDAP directory propagate to Cisco Unified Communications Manager regularly.

In addition, if you have already planned your access control groups, feature group templates, and universal line and device templates then you can immediately configure your imported end users with access control groups, a primary extension, and self-provisioning capability.
If you are assigning access control groups or feature group templates, you can use an LDAP filter to limit the import to the group of users with the same configuration requirements.

### Before you begin
- Enable LDAP Directory Synchronization, on page 69
- Create an LDAP Filter, on page 70 if you want to limit the LDAP sync to a subset of users.

### Procedure

**Step 1**
In Cisco Unified CM Administration, choose **System > LDAP > LDAP Directory**.

**Step 2**
Perform one of the following steps:
- Click **Find** and select an existing LDAP directory.
- Click **Add New** to create a new LDAP directory.

**Step 3**
Complete the fields in the **LDAP Directory Configuration** window. For help with the fields and their descriptions, refer to the online help.

**Step 4**
In the **LDAP Configuration Name** text box, assign a unique name to the LDAP directory.

**Step 5**
In the **LDAP Manager Distinguished Name** field, enter a user ID with access to the LDAP directory server.

**Step 6**
Enter and confirm the password details.

**Step 7**
Optional. If you want to limit the import to only a subset of users who meet a specific profile, from the **LDAP Custom Filter** drop-down list box, select an LDAP filter.

**Step 8**
In the **LDAP Directory Synchronization Schedule** fields, create a schedule that Cisco Unified Communications Manager uses to synchronize data with the external LDAP directory.

**Step 9**
Complete the **Standard User Fields to be Synchronized** section. For each End User field, choose an LDAP attribute. The synchronization process assigns the value of the LDAP attribute to the end user field in Cisco Unified Communications Manager.

**Step 10**
To assign the imported end users to an access control group that is common to all the imported end users, do the following:
   a) Click **Add to Access Control Group**.
   b) In the popup window, click the corresponding check box for each access control group that you want to assign to the imported end users.
   c) Click **Add Selected**.

**Step 11**
If you want to assign a feature group template, select the template from the **Feature Group Template** drop-down list box.

The user profile, service profile, universal line and device templates, and self-provisioning settings that are associated to the feature group template get assigned to the synced end users.

**Note**
The end users will be synced with the assigned **Feature Group Template** only for the first time when the users are not present. If an existing **Feature Group Template** is modified and a full sync is performed for the associated LDAP, the modifications will not get updated.

**Step 12**
If you want to assign primary extension by applying a mask to imported telephone numbers, do the following:
a) Check the **Apply Mask to synced telephone numbers to create a new line for inserted users** check box.
b) Enter a **Mask**. For example, a mask of 11XX will create a primary extension of 1145 if the imported telephone number is 8889945.

**Step 13**
If you want to assign primary extensions from a pool of directory numbers, do the following:
a) Check the **Assign new line from the pool list if one was not created based on a synced LDAP telephone number** check box.
b) In the **DN Pool Start** and **DN Pool End** text boxes, enter the range of directory numbers from which to select primary extensions.

**Step 14**
In the **LDAP Server Information** area, enter the hostname or IP address of the LDAP server.

**Step 15**
If you want to use SSL to create a secure connection to the LDAP server, check the **Use SSL** check box.

**Step 16**
Click **Save**.

---

**What to do next**

Configure LDAP Authentication, on page 74

---

**Configure Enterprise Directory User Search**

Use this procedure to configure phones and clients in your system to perform user searches against an enterprise directory server instead of the database.

**Before you begin**

- Ensure that the primary, secondary, and tertiary servers, which you choose for LDAP user search, are network reachable to the Cisco Unified Communications Manager subscriber nodes.
- Configure the type of LDAP server from the **LDAP Server Type** drop-down list in the **LDAP System Configuration** window by choosing **System > LDAP > LDAP System**.

**Procedure**

**Step 1**
In Cisco Unified CM Administration, choose **System > LDAP > LDAP Search**.

**Step 2**
To enable user searches to be performed using an enterprise LDAP directory server, check the **Enable user search to Enterprise Directory Server** check box. The fields in this window are enabled.

**Step 3**
Configure the fields in the **LDAP Search Configuration** window. See the online help for more information about the fields and their configuration options.

**Step 4**
Click **Save**.
LDAP Attributes for UDS Search of Directory Server

The following table lists the LDAP attributes that UDS users search request uses when the Enable user search to Enterprise Directory Server option is enabled. For these types of directory requests, UDS acts as a proxy and relays the search request to the corporate directory server.

UDS users response tag may be mapped to one of the LDAP attributes. The mapping of the attributes is determined by the option you select from the LDAP Server Type drop-down list. Access this drop-down list from System > LDAP > LDAP System Configuration window.

<table>
<thead>
<tr>
<th>UDS Users Response Tag</th>
<th>LDAP Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>userName</td>
<td>• samAccountName</td>
</tr>
<tr>
<td></td>
<td>• uid</td>
</tr>
<tr>
<td>firstName</td>
<td>givenName</td>
</tr>
<tr>
<td>lastName</td>
<td>sn</td>
</tr>
<tr>
<td>middleName</td>
<td>• initials</td>
</tr>
<tr>
<td></td>
<td>• middleName</td>
</tr>
<tr>
<td>nickName</td>
<td>nickName</td>
</tr>
<tr>
<td>displayName</td>
<td>displayName</td>
</tr>
<tr>
<td>phoneNumber</td>
<td>• telephonenumber</td>
</tr>
<tr>
<td></td>
<td>• ipPhone</td>
</tr>
<tr>
<td>homeNumber</td>
<td>homephone</td>
</tr>
<tr>
<td>mobileNumber</td>
<td>mobile</td>
</tr>
<tr>
<td>email</td>
<td>mail</td>
</tr>
<tr>
<td>directoryUri</td>
<td>• msRTCSIP-primaryuseraddress</td>
</tr>
<tr>
<td></td>
<td>• mail</td>
</tr>
<tr>
<td>department</td>
<td>• department</td>
</tr>
<tr>
<td></td>
<td>• departmentNumber</td>
</tr>
<tr>
<td>manager</td>
<td>manager</td>
</tr>
<tr>
<td>title</td>
<td>title</td>
</tr>
<tr>
<td>pager</td>
<td>pager</td>
</tr>
</tbody>
</table>
Configure LDAP Authentication

Perform this procedure if you want to enable LDAP authentication so that end user passwords are authenticated against the password that is assigned in the company LDAP directory. LDAP authentication gives system administrators the ability to assign an end user a single password for all company applications. This configuration applies to end user passwords only and does not apply to end user PINs or application user passwords.

Before you begin

Configure LDAP Directory Sync, on page 70

Procedure

Step 1 In Cisco Unified CM Administration, choose System > LDAP > LDAP Authentication.
Step 2 Check the Use LDAP Authentication for End Users check box to use your LDAP directory for user authentication.
Step 3 In the LDAP Manager Distinguished Name field, enter the user ID of the LDAP Manager who has access rights to the LDAP directory.
Step 4 In the Password field, enter the password for the LDAP Manager.
Step 5 Click Save.

What to do next

Customize LDAP Agreement Service Parameters, on page 74

Customize LDAP Agreement Service Parameters

Perform this procedure to configure service parameters that customize the system-level settings for LDAP agreements. If you do not configure these service parameters, Cisco Unified Communications Manager applies the default settings for LDAP directory integration.

You can use service parameters to customize the below settings:

• Maximum number of LDAP agreements
• Maximum number of hosts
• Retry delay on host or hostlist failure
• Connection timeouts
• Delayed start time for LDAP synces
Procedure

Step 1 In Cisco Unified CM Administration, choose System > Service Parameters.

Step 2 From the Server drop-down list box, choose the publisher node.

Step 3 From the Service drop-down list box, choose Cisco DirSync.

Step 4 Configure values for the Cisco DirSync service parameters. See the Related Topics for service parameter descriptions.

Step 5 Click Save.

Related Topics

LDAP Directory Service Parameters, on page 75

LDAP Directory Service Parameters

<table>
<thead>
<tr>
<th>Service Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Number Of Agreements</td>
<td>The maximum number of LDAP directories that you can configure. The default setting is 20.</td>
</tr>
<tr>
<td>Maximum Number Of Hosts</td>
<td>The maximum number of LDAP hostnames that you can configure for failover purposes. The default value is 3.</td>
</tr>
<tr>
<td>Retry Delay On Host Failure (secs)</td>
<td>After a host failure, the number of seconds that Cisco Unified Communications Manager delays before it retries the connection to the first LDAP server (hostname). The default value is 5.</td>
</tr>
<tr>
<td>Retry Delay On HostList Failure (mins)</td>
<td>After a hostlist failure, the number of minutes that Cisco Unified Communications Manager delays before it retries every configured LDAP server (hostnames). The default is 10.</td>
</tr>
<tr>
<td>LDAP Connection Timeout (secs)</td>
<td>The number of seconds that Cisco Unified Communications Manager allows for establishing the LDAP connection. The LDAP service provider aborts the connection attempt if a connection cannot be established in the specified amount of time. The default is 5.</td>
</tr>
<tr>
<td>Delayed Sync Start time (mins)</td>
<td>The number of minutes that Cisco Unified Communications Manager delays in starting the directory synchronization process after the Cisco DirSync service starts. The default is 5.</td>
</tr>
</tbody>
</table>

Convert LDAP Synchronized User to Local User

When you synchronize your LDAP directory with Cisco Unified Communications Manager, for LDAP-synchronized end users, you cannot edit any of the fields within the End User Configuration window unless you convert the LDAP-synchronized user to a local user.

To edit to an LDAP-synchronized field in the End User Configuration window, convert the user to a local user. However, if you perform this conversion, the end user will not be updated when Cisco Unified Communications Manager synchronizes with the LDAP directory.
Assign LDAP Synchronized Users to an Access Control Group

Perform this procedure to assign LDAP synchronized users to an access control group.

Before you begin
Cisco Unified Communications Manager must be configured to synchronize end users with an external LDAP directory.

Procedure

Step 1  In Cisco Unified CM Administration, choose System > LDAP > LDAP Directory.
Step 2  Click Find and select a configured LDAP Directory.
Step 3  Click the Add to Access Control Group button.
Step 4  Select the access control groups that you want to apply to the end users in this LDAP directory.
Step 5  Click Add Selected.
Step 6  Click Save.
Step 7  Click Perform Full Sync.
Cisco Unified Communications Manager syncs with the external LDAP directory and synchronized users get inserted into the correct access control group.

Note  The synchronized users get inserted into the selected access group only when you add an access control group for the first time. Any subsequent group that you add to LDAP will not be applied to the synchronized users after performing a full sync.
CHAPTER 8

Configure Cisco Unified Communications Manager for IM and Presence Service

- Integration Overview, on page 77
- Cisco Unified Communications Manager Integration Prerequisites, on page 77
- Cisco Unified Communications Manager Integration Task Flow, on page 79

Integration Overview

This section details the tasks that you should have completed on Cisco Unified Communications Manager in order to complete configuration on IM and Presence Service.

Cisco Unified Communications Manager Integration Prerequisites

Before you configure the IM and Presence Service to integrate with Cisco Unified Communications Manager, make sure that you complete the following general configuration tasks on Cisco Unified Communications Manager. For details on how to configure Cisco Unified Communications Manager, refer to the System Configuration Guide for Cisco Unified Communications Manager at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

The table below lists essential configuration tasks for IM and Presence Service integration. Refer to the online help for descriptions of fields and their options.
Table 5: Required Configuration on Cisco Unified Communications Manager

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Modify the User Credential Policy                                   | We recommend 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 | Enable *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                             | For details, see:  
   *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*                                                                                                                                                                                                         |
| Certificate exchange                                                | The certificate exchange between Cisco Unified Communications Manager and the IM and Presence Service is handled automatically during the installation process. However, if there is an issue and you need to complete the certificate exchange manually, refer to *Certificate Exchange with Cisco Unified Communications Manager*, on page 115.                                                                                       |

**Note** If Cisco Unified Communications Manager Tomcat certificates that you upload to the IM and Presence Service contain hostnames in the SAN field, all of them should be resolvable from the IM and Presence Service. The IM and Presence Service must be able to resolve the hostname via DNS or the Cisco Sync Agent service will not start. This is true regardless of whether you use a hostname, IP Address, or FQDN for the Node Name of the Cisco Unified Communications Manager server.
### Cisco Unified Communications Manager Integration Task Flow

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Configure a SIP Trunk Security Profile, on page 80</td>
<td>Configure a SIP Trunk Security Profile for the trunk connection between Cisco Unified Communications Manager and the IM and Presence Service.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configure SIP Trunk for IM and Presence Service, on page 80</td>
<td>Assign the SIP Trunk Security Profile to a SIP trunk and configure the trunk connection between Cisco Unified Communications Manager and IM and Presence Service.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configure SRV Cluster Name, on page 81</td>
<td>Optional. Complete this procedure only if you are using DNS SRVs on the SIP trunk between Cisco Unified Communications Manager and the IM and Presence Service and you use an SRV address other than the IM and Presence default domain. In this case, configure the <strong>SRV Cluster Name</strong> service parameter. Otherwise, you can skip this task.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configure the Presence Gateway, on page 82</td>
<td>On the IM and Presence Service, assign Cisco Unified Communications Manager as a presence gateway, thereby allowing the systems to exchange Presence information.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configure a SIP PUBLISH Trunk, on page 81</td>
<td>Optional. Use this procedure to configure a SIP PUBLISH trunk for IM and Presence. When you turn on this setting, Cisco Unified Communications Manager publishes phone presence for all line appearances that are associated with users licensed on Cisco Unified Communications Manager for the IM and Presence Service.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Verify Services on Cisco Unified Communications Manager, on page 82</td>
<td>Verify that required services are running on Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Configure Phone Presence from Off-Cluster Cisco Unified Communications Manager, on page 83</td>
<td>Configure Cisco Unified Communications Manager as a TLS Peer subject of the IM and Presence Service. TLS is required if you want to allow phone presence from a Cisco Unified Communications Manager that is outside of the IM and Presence Service cluster.</td>
</tr>
</tbody>
</table>
Configure a SIP Trunk Security Profile

On Cisco Unified Communications Manager, configure a SIP Trunk Security Profile for the trunk connection with the IM and Presence Service.

Procedure

**Step 1** In Cisco Unified CM Administration > System > Security > SIP Trunk Security Profile, click Find.
**Step 2** Click Non Secure SIP Trunk Profile.
**Step 3** Click Copy.
**Step 4** Enter a Name for the profile. For example, IMP-SIP- Trunk-Profile.
**Step 5** Complete the following settings:
- The **Device Security Mode** is set to Non Secure.
- The **Incoming Transport Type** is set to TCP+UDP.
- The **Outgoing Transport Type** is set to TCP.
**Step 6** Check the following check boxes:
- Accept Presence Subscription
- Accept Out-of-Dialog REFER
- Accept Unsolicited Notification
- Accept Replaces Header
**Step 7** Click Save.

What to do next

Configure SIP Trunk for IM and Presence Service, on page 80

Configure SIP Trunk for IM and Presence Service

Set up the SIP trunk connection between Cisco Unified Communications Manager and the IM and Presence Service cluster.

Before you begin

Configure a SIP Trunk Security Profile, on page 80

Procedure

**Step 1** From Cisco Unified CM Administration, choose Device > Trunk
**Step 2** Click Add New.
**Step 3** From the **Trunk Type** drop-down list box, choose SIP Trunk.
**Step 4** From the **Device Protocol** drop-down list box, choose SIP.
**Step 5** From the **Trunk Service Type** drop-down list box, choose None.
Step 6  Click Next.
Step 7  In the **Device Name** field, enter a name for the trunk. For example, **IMP-SIP-Trunk**.
Step 8  Select a **Device Pool** from the drop-down list box.
Step 9  In the **SIP Information** section, assign the trunk to the IM and Presence Service by entering the address information for the IM and Presence cluster:
   - If you are using a DNS SRV record for the IM and Presence Service, check the **Destination Address is an SRV** check box and enter the SRV in the **Destination Address** field.
   - Otherwise, in the **Destination Address** field, enter the IP address or FQDN of the IM and Presence node. Click the (+) button to add additional nodes. You can enter up to 16 nodes.
Step 10 For the **Destination Port**, enter **5060**.
Step 11 From the **SIP Trunk Security Profile** drop-down list box, choose the SIP trunk security profile that you created in the previous task.
Step 12 From the **SIP Profile** drop-down list box, choose a profile. For example, the **Standard SIP Profile**.
Step 13 Click **Save**.

**What to do next**

If you are using DNS SRVs on the SIP trunk between Cisco Unified Communications Manager and the IM and Presence Service and you use an address other than the IM and Presence default domain, Configure **SRV Cluster Name** on page 81.

Otherwise, Configure a SIP PUBLISH Trunk, on page 81.

**Configure SRV Cluster Name**

If you are using DNS SRVs on the SIP trunk between Cisco Unified Communications Manager and the IM and Presence Service and you use an address other than the IM and Presence default domain, configure the **SRV Cluster Name** service parameter. Otherwise, you can skip this task.

**Procedure**

Step 1  From Cisco Unified CM IM and Presence Serviceability, choose **System > Service Parameters**.
Step 2  From the **Server** drop-down menu, select the IM and Presence publisher node and click **Go**.
Step 3  From the **Service** drop-down, select the **Cisco SIP Proxy** service.
Step 4  In the **SRV Cluster Name** field, enter the SRV address.
Step 5  Click **Save**.

**Configure a SIP PUBLISH Trunk**

Use this optional procedure to configure a SIP PUBLISH trunk for IM and Presence. When you turn on this setting, Cisco Unified Communications Manager publishes phone presence for all line appearances that are associated with users licensed on Cisco Unified Communications Manager for the IM and Presence Service.
Procedure

Step 1  From Cisco Unified CM IM and Presence Administration, choose Presence > Settings > Standard Configuration.

Step 2  From the CUCM IM and Presence Publish Trunk drop-down, select the SIP trunk that you configured on Cisco Unified Communications Manager for the IM and Presence Service.

Step 3  Click Save.

Note  When you save this new setting, the IM and Presence Publish Trunk service parameter in Cisco Unified Communications Manager also updates with this new setting.

What to do next

Verify Services on Cisco Unified Communications Manager, on page 82

Configure the Presence Gateway

Use this procedure on the IM and Presence Service to assign Cisco Unified Communications Manager as a presence gateway. This configuration enables the presence information exchange between Cisco Unified Communications Manager and the IM and Presence Service.

Procedure

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

Step 2  Click Add New.

Step 3  From the Presence Gateway drop-down list box, choose CUCM.

Step 4  Enter a Description.

Step 5  In the Presence Gateway field, enter one of the following options:

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

Step 6  Click Save.

What to do next

Configure a SIP PUBLISH Trunk, on page 81

Verify Services on Cisco Unified Communications Manager

Use this procedure to verify that required services are running on Cisco Unified Communications Manager nodes.
Procedure

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

**Step 2**  
From the Server menu, choose Cisco Unified Communications Manager cluster node and click **Go**.

**Step 3**  
Make sure that the following services are running. If they are not running, start them.

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

**Step 4**  
If any of the above services are not running, select the service and click **Start**.

---

**Configure Phone Presence from Off-Cluster Cisco Unified Communications Manager**

You can allow phone presence from a Cisco Unified Communications Manager that is outside of the IM and Presence Service cluster. However, in order for the IM and Presence Service to accept a SIP PUBLISH from a Cisco Unified Communications Manager outside of its cluster, the Cisco Unified Communications Manager needs to be listed as a TLS Trusted Peer of the IM and Presence.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Add Cisco Unified Communications Manager as TLS Peer, on page 83</td>
<td>Add Cisco Unified Communications Manager as a TLS peer of the IM and Presence Service.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Configure a TLS Context for Unified Communications Manager, on page 84</td>
<td>Add the Cisco Unified Communications Manager TLS peer</td>
</tr>
</tbody>
</table>

**Add Cisco Unified Communications Manager as TLS Peer**

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

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In <strong>Cisco Unified CM IM and Presence Administration &gt; System &gt; Security &gt; TLS Peer Subjects</strong>, click <strong>Add New</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Enter the IP Address of the external Cisco Unified Communications Manager in the <strong>Peer Subject Name</strong> field.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enter the name of the node in the <strong>Description</strong> field.</td>
</tr>
</tbody>
</table>
Configure a TLS Context for Unified Communications Manager

Use the following procedure to add the Cisco Unified Communications Manager TLS peer that you configured in the previous task to a selected TLS peer.

Before you begin
Add Cisco Unified Communications Manager as TLS Peer, on page 83

Procedure

Step 1 In Cisco Unified CM IM and Presence Administration > System > Security > TLS Context Configuration, click Find.
Step 2 Click Default_Cisco_UP_SIP_Proxy_Peer_Auth_TLS_Context.
Step 3 From the list of available TLS peer subjects, choose the TLS peer subject that you configured for Cisco Unified Communications Manager.
Step 4 Move this TLS peer subject to Selected TLS Peer Subjects.
Step 5 Click Save.
Step 6 Restart the Cisco OAMAgent on all cluster nodes:
   a) From Cisco Unified IM and Presence Serviceability, choose Tools > Control Center - Network Services.
   b) From the Server drop-down list box, choose the IM and Presence server and click Go.
   c) Under IM and Presence Services, select Cisco OAMAgent and click Restart.
   d) Restart the service on all cluster nodes.
Step 7 After the OAM Agent restarts, restart the Cisco Presence Engine.
   a) Choose Tools > Control Center - Feature Services.
   b) From the Server drop-down list box, choose the IM and Presence node and click Go.
   c) Under IM and Presence Services, select Cisco Presence Engine and click Restart.
   d) Restart the service on all cluster nodes.

What to do next
Verify Services on Cisco Unified Communications Manager, on page 82
Centralized Deployment Overview

The IM and Presence centralized deployment allows you to deploy your IM and Presence deployment and your telephony deployment in separate clusters. The central IM and Presence cluster handles IM and Presence for the enterprise, while the remote Cisco Unified Communications Manager telephony cluster handles voice and video calls for the enterprise.

The Centralized Deployment option provides the following benefits when compared to standard deployments:

- The Centralized Deployment option does not require a 1x1 ratio of telephony clusters to IM and Presence Service clusters—you can scale your IM and Presence deployment and your telephony deployment separately, to the unique needs of each.

- Full mesh topology is not required for the IM and Presence Service

- Version independent from telephony—you IM and Presence central cluster can be running a different version than your Cisco Unified Communications Manager telephony clusters.

- Can manage IM and Presence upgrades and settings from the central cluster.

- Lower cost option, particularly for large deployments with many Cisco Unified Communications Manager clusters

- Easy XMPP Federation with third parties.

Scalability

With a 25K OVA template, and a six-node cluster with High Availability enabled, the IM and Presence Service central deployment supports up to 75,000 clients. To support 75K users with 25K OVA, default trace level for XCP router needs to be changed from Info to Error.
Interclustering for Centralized Deployment

Interclustering is supported between two Centralize cluster. Intercluster is tested with one cluster with 25K (with 25K OVA) and another with 15K (with 15K OVA) devices and no performance issues were observed.

Centralized Deployment Setup vs Standard Deployments

The following table discusses some of the differences in setting up an IM and Presence Centralized Cluster Deployment as opposed to standard deployments of the IM and Presence Service.

<table>
<thead>
<tr>
<th>Setup Phase</th>
<th>Differences with Standard Deployments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Phase</td>
<td>The installation process for an IM and Presence central deployment is the same as for the standard deployment. However, with central deployments, the IM and Presence central cluster is installed separately from your telephony cluster, and may be located on separate hardware servers. Depending on how you plan your topology, the IM and Presence central cluster may be installed on separate physical hardware from your telephony cluster. For the IM and Presence central cluster, you must still install Cisco Unified Communications Manager and then install the IM and Presence Service on the same servers. However, the Cisco Unified Communications Manager instance of the IM and Presence central cluster is for database and user provisioning primarily, and does not handle voice or video calls.</td>
</tr>
<tr>
<td>Configuration Phase</td>
<td>Compared to standard deployments, the following extra configurations are required to set up the IM and Presence Service Central Deployment:</td>
</tr>
<tr>
<td></td>
<td>• Users must be synced into both the telephony cluster and the IM and Presence Service central cluster so that they exist in both databases.</td>
</tr>
<tr>
<td></td>
<td>• In your telephony clusters, end users should not be enabled for IM and Presence.</td>
</tr>
<tr>
<td></td>
<td>• In your telephony clusters, the Service Profile must include the IM and Presence Service and must point to the IM and Presence central cluster.</td>
</tr>
<tr>
<td></td>
<td>• In the IM and Presence central cluster, users must be enabled for the IM and Presence Service.</td>
</tr>
<tr>
<td></td>
<td>• In the IM and Presence central cluster's database publisher node, add your remote Cisco Unified Communications Manager telephony cluster peers.</td>
</tr>
<tr>
<td></td>
<td>The following configurations, which are used with Standard Deployments of the IM and Presence Service, but are not required with Central Deployments:</td>
</tr>
<tr>
<td></td>
<td>• A Presence Gateway is not required.</td>
</tr>
<tr>
<td></td>
<td>• A SIP Publish trunk is not required.</td>
</tr>
<tr>
<td></td>
<td>• A Service Profile is not required on the IM and Presence central cluster—the Service Profile is configured on the telephony cluster to which the central cluster connects</td>
</tr>
</tbody>
</table>
Centralized Cluster Deployment Architecture

The following diagram highlights the cluster architecture for this deployment option. Cisco Jabber clients connect to multiple Cisco Unified Communications Manager clusters for voice and video calling. In this example, the Cisco Unified Communications Manager telephony clusters are leaf clusters in a Session Management Edition deployment. For Rich Presence, Cisco Jabber clients connect to the IM and Presence Service central cluster. The IM and Presence central cluster manages instant messaging and presence for the Jabber clients.

**Note**

Your IM and Presence cluster still contains an instance for Cisco Unified Communications Manager. However, this instance is for handling shared features such as database and user provisioning—it does not handle telephony.

**Centralized Cluster Use Case**

To connect your telephony and IM and Presence clusters, a new system for exchanging access keys is introduced. This diagram shows the flow for SSO logins:

- [1]-[2]: Query DNS to get SRV record.
• [3]-[4]: Query UDS to get the Home Cisco Unified Communications Manager cluster.
• [5]-[8]: Get Access Token and Refresh Token from Cisco Unified Communications Manager cluster through SAML SSO.
• [9]: Read UC Service Profile. The service profile contains an IM and Presence profile and points to the IM and Presence central cluster.
• [10]: Client registers to the IM and Presence cluster using the same Access Token through SOAP and XMPP interfaces.
• [11]: The token is validated and a response is sent back to Jabber client.

Centralized Deployment Prerequisites

The following requirements apply for the IM and Presence Service centralized deployment:

- The IM and Presence Service central cluster must be running Release 11.5(1)SU4 or higher.
- The local Cisco Unified Communications Manager instance that runs with the IM and Presence central cluster must be running the same release as the IM and Presence central cluster.
- The remote Cisco Unified Communications Manager telephony cluster must be running Release 10.5(2) or higher.
- Cisco Jabber must be running Release 11.9 or higher.
- For Push Notifications instant messaging support, the IM and Presence Service must be running at least 11.5(1)SU4.
- Cisco Unified Communications Manager functionality is based on the Cisco Unified Communications Manager version that is running on your remote telephony clusters rather than on the local instance that runs with the IM and Presence central cluster. For example:
  - For Push Notifications call support, the remote telephony cluster must be running at least 11.5(1)SU4.
  - For OAuth Refresh Logins support, the remote Cisco Unified Communications Manager telephony cluster must be running at least 11.5(1)SU4.
  - For SAML SSO support, the remote telephony cluster must be running at least 11.5(1)SU4.
The Cisco AXL Web Service feature service must be running in all clusters. This service is enabled by default, but you can confirm that it is activated from the Service Activation window of Cisco Unified Serviceability.

With Centralized Deployments, rich presence is handled by Cisco Jabber. The user's phone presence displays only if the user is logged in to Cisco Jabber.

**DNS Requirements**

The IM and Presence central cluster must have a DNS SRV record that points to the publisher node of the Cisco Unified Communications Manager telephony cluster. If your telephony deployment includes an ILS network, the DNS SRV must point to the hub cluster. This DNS SRV record should be referring to "_cisco-uds".

The SRV record is a Domain Name System (DNS) resource record that is used to identify computers that host specific services. SRV resource records are used to locate domain controllers for Active Directory. To verify SRV locator resource records for a domain controller, use the following method:

Active Directory creates its SRV records in the following folders, where Domain Name indicates the name of the installed domain:

- Forward Lookup Zones/Domain_Name/_msdcs/dc/_sites/Default-First-Site-Name/_tcp
- Forward Lookup Zones/Domain_Name/_msdcs/dc/_tcp

In these locations, an SRV record should appear for the following services:

- _kerberos
- _ldap
- _cisco_uds: indicates the SRV record

The below mentioned parameters has to be set during the SRV record creation.

- Service: _cisco_uds
- Protocol: _tcp
- weight: starts from 0 (0 is the highest priority)
- port no: 8443
- host: fqdn name of the server

An example of a DNS SRV record from a computer running a Jabber client is:

```
nslookup -type=all _cisco-uds._tcp.dcloud.example.com
Server: ad1.dcloud.example.com
Address: x.x.x.x
_cisco-uds._tcp.dcloud.example.com SRV service location:
priority = 10
weight = 10
port = 8443
svr hostname = cucm2.dcloud.example.com
cucm2.dcloud.example.com internet address = x.x.x.y
```
Centralized Deployment Configuration Task Flow

Complete these tasks if you want to configure an IM and Presence centralized cluster deployment.

**Table 6: Centralized Cluster Configuration Task Flow**

<table>
<thead>
<tr>
<th>Step</th>
<th>IM and Presence Central Cluster</th>
<th>Remote Telephony Clusters</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Enable IM and Presence in Central Cluster, on page 91</td>
<td></td>
<td>In your IM and Presence central cluster, configure a template that enables the IM and Presence Service.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Complete LDAP Sync on IM and Presence Central Cluster, on page 91</td>
<td></td>
<td>Complete an LDAP sync to propagate settings to LDAP-synced users in your IM and Presence central cluster.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enable Users for IM and Presence via Bulk Admin, on page 92</td>
<td></td>
<td>Optional. If you have already completed an LDAP sync, use Bulk Administration to enable IM and Presence for users.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Add Remote Telephony Clusters, on page 93</td>
<td></td>
<td>Add your remote telephony clusters to the IM and Presence central cluster.</td>
</tr>
<tr>
<td>Step 5</td>
<td></td>
<td>Configure an IM and Presence UC Service, on page 94</td>
<td>In your telephony clusters, add a UC service that points to the IM and Presence central cluster.</td>
</tr>
<tr>
<td>Step 6</td>
<td></td>
<td>Create Service Profile for IM and Presence, on page 94</td>
<td>Add your IM and Presence UC service to a service profile. Cisco Jabber clients use this profile to find the IM and Presence central cluster.</td>
</tr>
<tr>
<td>Step 7</td>
<td></td>
<td>Update Presence Users in Telephony Cluster, on page 95</td>
<td>In the telephony cluster, edit Presence user settings to point to the IM and Presence central cluster.</td>
</tr>
<tr>
<td>Step 8</td>
<td></td>
<td>Configure an ILS Network, on page 96</td>
<td>If more than one telephony cluster exists, you must configure ILS.</td>
</tr>
<tr>
<td>Step 9</td>
<td></td>
<td>MRA Configuration</td>
<td>Configuration of MRA in case of centralized deployment.</td>
</tr>
</tbody>
</table>
Enable IM and Presence in Central Cluster

Use this procedure to configure a feature group template with IM and Presence settings for the central cluster. You can add the feature group template to an LDAP Directory configuration to configure IM and Presence for synced users.

Note
You can apply a feature group template only to an LDAP directory configuration where the initial sync has not yet occurred. Once you’ve synced your LDAP configuration from the central cluster, you cannot apply edits to the LDAP configuration in Cisco Unified Communications Manager. If you have already synced your directory, you will need to use Bulk Administration to configure IM and Presence for users. For details, see Enable Users for IM and Presence via Bulk Admin, on page 92.

Procedure

Step 1 Log into the Cisco Unified CM Administration interface of the IM and Presence centralized cluster. This server should have no telephony configured.

Step 2 Choose User Management > User Phone/Add > Feature Group Template.

Step 3 Do one of the following:

• Click Find and select an existing template
• Click Add New to create a new template

Step 4 Check both of the following check boxes:

• Home Cluster
• Enable User for Unified CM IM and Presence

Step 5 Complete the remaining fields in the Feature Group Template Configuration window. For help with the fields and their settings, refer to the online help.

Step 6 Click Save.

What to do next
To propagate the setting to users, you must complete an LDAP sync.

Complete LDAP Sync on IM and Presence Central Cluster, on page 91

Complete LDAP Sync on IM and Presence Central Cluster

Complete an LDAP sync on your IM and Presence Service central cluster to configure users with IM and Presence feature functionality via the feature group template.
Enable Users for IM and Presence via Bulk Admin

If you have already synced users into the central cluster, and those users were not enabled for the IM and Presence Service, use Bulk Administration's Update Users feature to enable those users for the IM and Presence Service.

You can also use Bulk Administration's Import Users or Insert Users feature to import new users via a csv file. For procedures, see the Bulk Administration Guide for Cisco Unified Communications Manager. Make sure that imported users have the below options selected.

- Home Cluster
- Enable User for Unified CM IM and Presence
Procedure

Step 1 From Cisco Unified CM Administration, choose Bulk Administration > Users > Update Users > Query.
Step 2 From the Filter, select Has Home Cluster Enabled and click Find. The window displays all of the end users for whom this is their Home Cluster.
Step 3 Click Next.
   In the Update Users Configuration window, the check boxes on the far left indicate whether you want to edit this setting with this query. If you don't check the left check box, the query will not update that field. The field on the right indicates the new setting for this field. If two check boxes appear, you must check the check box on the left to update the field, and in the right check box, enter the new setting.
Step 4 Under Service Settings, check the left check box for each of the following fields to indicate that you want to update these fields, and then edit the adjacent field setting as follows:
   • Home Cluster — Check the right check box to enable this cluster as the home cluster.
   • Enable User for Unified CM IM and Presence — Check the right check box. This setting enables the central cluster as the provider of IM and Presence Service for these users.
Step 5 Complete any remaining fields that you want to update. For help with the fields and their settings, see the online help.
Step 6 Under Job Information, select Run Immediately.
Step 7 Click Submit.

Add Remote Telephony Clusters

Use this procedure to add your remote telephony clusters to the centralized IM and Presence Service cluster.

Procedure

Step 1 Log in to database publisher node on the IM and Presence Service centralized cluster.
Step 2 From Cisco Unified CM IM and Presence Administration, choose System > Centralized Deployment.
Step 3 Click Find to view the list of current remote Cisco Unified Communications Manager clusters. If you want to edit the details of a cluster, select the cluster and click Edit Selected.
Step 4 Click Add New to add a new remote Cisco Unified Communications Manager telephony cluster.
Step 5 Complete the following fields for each telephony cluster that you want to add:
   • Peer Address — The FQDN, hostname, IPv4 address, or IPv6 address of the publisher node on the remote Cisco Unified Communications Manager telephony cluster.
   • AXL Username — The login username for the AXL account on the remote cluster.
   • AXL Password — The password for the AXL account on the remote cluster.
Step 6 Click the Save and Synchronize button.
The IM and Presence Service synchronizes keys with the remote cluster.
Configure an IM and Presence UC Service

Use this procedure in your remote telephony clusters to configure a UC service that points to the IM and Presence Service central cluster.

Procedure

Step 1 Log in to the Cisco Unified CM Administration interface on your telephony cluster.
Step 2 Choose User Management > User Settings > UC Service.
Step 3 Do either of the following:
   a) Click Find and select an existing service to edit.
   b) Click Add New to create a new UC service.
Step 4 From the UC Service Type drop-down list box, select IM and Presence and click Next.
Step 5 From the Product type drop-down list box, select IM and Presence Service.
Step 6 Enter a unique Name for the cluster. This does not have to be a hostname.
Step 7 From HostName/IP Address, enter the hostname, IPv4 address, or IPv6 address of the IM and Presence central cluster database publisher node.
Step 8 Click Save.
Step 9 Recommended. Repeat this procedure to create a second IM and Presence service where the HostName/IP Address field points to a subscriber node in the central cluster.

Create Service Profile for IM and Presence

Use this procedure in your remote telephony clusters to create a service profile that points to the IM and Presence central cluster. Cisco Jabber clients will use this profile to find the IM and Presence central cluster.

Before you begin

Configure an IM and Presence UC Service, on page 94

Procedure

Step 1 From Cisco Unified CM Administration, choose User Management > User Settings > Service Profile.
Step 2 Do one of the following:
   a) Click Find and select an existing service profile to edit.
   b) Click Add New to create a new service profile.
Step 3
In the **IM and Presence Profile** section, configure IM and Presence services that you configured in the previous task:

a) From the **Primary** drop-down, select the database publisher node service.

b) From the **Secondary** drop-down, select the subscriber node service.

Step 4
Click **Save**.

---

**What to do next**

*Update Presence Users in Telephony Cluster, on page 95*

---

### Update Presence Users in Telephony Cluster

If you've already completed an LDAP sync in your telephony deployment, use the Bulk Administration Tool to edit user settings in the Telephony cluster for IM and Presence users. This configuration will point Presence users to the Central Cluster for the IM and Presence Service.

---

**Note**

This procedure assumes that you have already completed an LDAP sync in your telephony cluster. However, if you haven't yet completed the initial LDAP sync, you can add the Central Deployment settings for Presence users into your initial sync. In this case, do the following in your telephony cluster:

- Configure a Feature Group Template that includes the **Service Profile** that you just set up. Make sure that have the **Home Cluster** option selected and the **Enable User for Unified CM IM and Presence** option unselected.

- In **LDAP Directory Configuration**, add the **Feature Group Template** to your LDAP Directory sync.

- Complete the initial sync.

For additional details on configuring Feature Group Templates and LDAP Directory, see the "Configure End Users" part of the *System Configuration Guide for Cisco Unified Communications Manager*.

---

**Procedure**

**Step 1**
From Cisco Unified CM Administration, choose **Query > Bulk Administration > Users > Update Users > Query**.

**Step 2**
From the Filter, select **Has Home Cluster Enabled** and click **Find**. The window displays all of the end users for whom this is their Home Cluster.

**Step 3**
Click **Next**.
In the **Update Users Configuration** window, the check boxes on the far left indicate whether you want to edit this setting with this query. If you don't check the left check box, the query will not update that field. The field on the right indicates the new setting for this field. If two check boxes appear, you must check the check box on the left to update the field, and in the right check box, enter the new setting.

**Step 4**
Under **Service Settings**, check the far left check box for each of the following fields to indicate that you want to update these fields, and then edit the adjacent setting as follows:

- **Home Cluster**—Check the right check box to enable the telephony cluster as the home cluster.
Configure an ILS Network

For IM and Presence centralized clusters where there are more than one remote telephony clusters, you can use the Intercluster Lookup Service (ILS) to provision remote telephony clusters for the IM and Presence central cluster. ILS monitors the network and propagates network changes such as new clusters or address changes to the entire network.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Configure Cluster IDs for ILS, on page 97</td>
<td>Set unique Cluster IDs for each telephony cluster. ILS will not work while the Cluster ID is set to StandAloneCluster (the default setting).</td>
</tr>
</tbody>
</table>

**Before you begin**

If you are deploying ILS, make sure that you have done the following:

- Plan your ILS network topology. You must know which telephony clusters will be hubs and spokes.
- The telephony cluster to which the IM and Presence central cluster connects must be a hub cluster.
- You must configure a DNS SRV record that points to the publisher node of the hub cluster.

Configure Cluster IDs for ILS

Each cluster within the ILS network must have a unique Cluster ID. Use this procedure to give your telephony clusters unique cluster IDs.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log in to Cisco Unified CM Administration on the publisher node.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Choose <strong>System &gt; Enterprise Parameters.</strong></td>
</tr>
<tr>
<td>Step 3</td>
<td>Change the value of the <strong>Cluster ID</strong> parameter from StandAloneCluster to a unique value that you set. ILS will not work while the Cluster ID is StandAloneCluster.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Save.</strong></td>
</tr>
<tr>
<td>Step 5</td>
<td>Repeat this procedure on the publisher node of each telephony cluster that you want to join into the ILS network. Each cluster must have a unique ID.</td>
</tr>
</tbody>
</table>

What to do next

Enable ILS on Telephony Clusters, on page 97

Enable ILS on Telephony Clusters

Use this procedure to configure and activate ILS on your Cisco Unified Communications Manager telephony clusters.

Note

- Configure your hub clusters before configuring your spoke clusters.
- For help with the fields and their settings, refer to the online help.

Before you begin

Configure Cluster IDs for ILS, on page 97
Procedure

Step 1 Log into Cisco Unified CM Administration on the publisher node of your telephony cluster.
Step 2 Choose Advanced Features > ILS Configuration.
Step 3 From the Role drop-down list box, select Hub Cluster or Spoke Cluster depending on which type of cluster you are setting up.
Step 4 Check the Exchange Global Dial Plan Replication Data with Remote Clusters check box.
Step 5 Configure ILS Authentication Details.
   a) If you want to use TLS authentication between the various clusters, check the Use TLS Certificates check box.
      Note If you use TLS, you must exchange CA-signed certificates between the nodes in your cluster.
   b) If you want to use password authentication (regardless of whether TLS is used), check the Use Password check box and enter the password details.
Step 6 Click Save.
Step 7 In the ILS Cluster Registration popup, configure your registration details:
   • In the Registration Server text box, enter the publisher node IP address or FQDN for the hub cluster to which you want to connect this cluster. If this is the first hub cluster in your network, you can leave the field blank.
   • Make sure that the Activate the Intercluster Lookup Service on the publisher in this cluster check box is checked.
Step 8 Click OK.
Step 9 Repeat this procedure on the publisher node of each telephony cluster that you want to add to the ILS network. Depending on the sync values that you configured, there may be a delay while the cluster information propagates throughout the network.

If you chose to use Transport Layer Security (TLS) authentication between clusters, you must exchange Tomcat certificates between the publisher node of each cluster in the ILS network. From Cisco Unified Operating System Administration, use the Bulk Certificate Management feature to:
   • Export certificates from the publisher node of each cluster to a central location
   • Consolidate exported certificates in the ILS network
   • Import certificates onto the publisher node of each cluster in your network

For details, see the "Manage Certificates" chapter of the Administration Guide for Cisco Unified Communications Manager.

What to do next

After ILS is up and running, and you have exchanged certificates (if required), Verify ILS Network is Running, on page 98

Verify ILS Network is Running

Use this procedure to confirm that your ILS network is up and running.
**Procedure**

**Step 1** Log in to the publisher node on any of your telephony clusters.

**Step 2** From Cisco Unified CM Administration choose **Advanced Features > ILS Configuration**.

**Step 3** Check the **ILS Clusters and Global Dial Plan Imported Catalogs** section. Your ILS network topology should appear.

---

**MRA Configuration**

Cisco Unified Communications Mobile and Remote Access is a core part of the Cisco Collaboration Edge Architecture. It allows endpoints such as Cisco Jabber to have their registration, call control, provisioning, messaging and presence services provided by Cisco Unified Communications Manager when the endpoint is not within the enterprise network. The Expressway provides secure firewall traversal and line-side support for Unified CM registrations.

The overall solution provides:

1. **Off-premises access**: A consistent experience outside the network for Jabber and EX/MX/SX series clients.
3. **Cloud services**: Enterprise grade flexibility and scalable solutions providing rich WebEx integration and Service Provider offerings.
4. **Gateway and interoperability services**: Media and signalling normalization, and support for non-standard endpoints.

**Configuration**

To configure MRA on all telephony leaf clusters in Expressway-C. Choose **Configuration → Unified Communications → Unified CM Servers**.

To configure MRA on centralized IM&P nodes cluster in Expressway-C. Choose **Configuration → Unified Communications → IM and Presence Service nodes**.

To Enable the "Mobile and Remote Access" in Expressway-C. Choose **Configuration → Enable "Mobile and Remote Access"** and select the control options as per the table below.

**Table 7: OAuth Enable Configuration**

<table>
<thead>
<tr>
<th>Authentication path</th>
<th>UCM / LADP basic authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorize by OAuth token with refresh</td>
<td>ON</td>
</tr>
<tr>
<td>Authorize by OAuth token</td>
<td>ON</td>
</tr>
<tr>
<td>Authorize by user credentials</td>
<td>No</td>
</tr>
<tr>
<td>Allow Jabber iOS clients to use embedded Safari browser</td>
<td>No</td>
</tr>
<tr>
<td>Check for internal authentication availability</td>
<td>Yes</td>
</tr>
</tbody>
</table>
**Table 8: OAuth Disable Configuration**

<table>
<thead>
<tr>
<th>Authentication path</th>
<th>UCM / LADP basic authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorize by OAuth token with refresh</td>
<td>Off</td>
</tr>
<tr>
<td>Authorize by user credentials</td>
<td>On</td>
</tr>
<tr>
<td>Allow Jabber iOS clients to use embedded Safari browser</td>
<td>Off</td>
</tr>
<tr>
<td>Check for internal authentication availability</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Note**


---

**Centralized Deployment Field Descriptions**

From Cisco Unified CM IM and Presence Administration, choose **System > Centralized Deployment** to access the Centralized Deployment window. If you are deploying the IM and Presence Centralized Cluster deployment, you can create connections to your remote Cisco Unified Communications Manager clusters in this configuration window.

Click the **Add New** button to add a Cisco Unified Communications Manager cluster. Click **Synchronize Selected** to synchronize access keys with the remote cluster.

**Table 9: Centralized Deployment Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer Address</td>
<td>The FQDN, hostname, IPv4 address, or IPv6 address of the remote Cisco Unified Communications Manager cluster publisher node.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The Peer Address cannot point to any IM and Presence Service node or to the Cisco Unified Communications Manager instance of another IM and Presence Service central cluster.</td>
</tr>
<tr>
<td>Peer AXL Username</td>
<td>The login username for the AXL account on the remote cluster.</td>
</tr>
<tr>
<td>Peer AXL Password</td>
<td>The password for the AXL account on the remote cluster.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the current sync status with the remote cluster.</td>
</tr>
<tr>
<td>Last Synchronized</td>
<td>Displays the last time a sync occurred with the remote cluster.</td>
</tr>
<tr>
<td>Save and Synchronize</td>
<td>After you have entered your details, click this button to save your settings and to sync access keys with the remote cluster.</td>
</tr>
</tbody>
</table>
## Centralized Deployment Interactions and Restrictions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>ILS Hub Cluster</td>
<td>If the ILS hub cluster is down, and more than one telephony cluster exists, the Central Cluster feature does not work.</td>
</tr>
<tr>
<td>ILS Deployments</td>
<td>If you are deploying an IM and Presence central cluster and you are also deploying ILS, you can deploy ILS in the telephony clusters only. You cannot deploy ILS on the Cisco Unified Communications Manager instance for the IM and Presence central cluster. This instance is for provisioning only and does not handle telephony.</td>
</tr>
<tr>
<td>Rich Presence</td>
<td>In a Centralized deployment, users' rich presence is computed by Cisco Jabber. Users' telephony presence is displayed only when if the user is logged in to Jabber.</td>
</tr>
</tbody>
</table>
Centralized Deployment Interactions and Restrictions
CHAPTER 10

Configure Advanced Routing

• Advanced Routing Overview, on page 103
• Advanced Routing Prerequisites, on page 103
• Advanced Routing Configuration Task Flow, on page 104

Advanced Routing Overview

Configure advanced routing to determine how the system establishes the following types of connections:

• Intracluster connections between IM and Presence Service nodes within a cluster.

• Intercluster connections between IM and Presence Service clusters that share the same presence domain.

• SIP static routes for federation connections between different presence domains. Static routes are a fixed path and take precedence over dynamic routes.

Intracluster and Intercluster Connections

There are two modes to establish intercluster and intracluster connections:

• Multicast DNS (MDNS)—MDNS routing uses DNS records to set up the connections between the nodes. You can use MDNS routing when all nodes in the cluster are in the same multicast domain.

• Router-to-router (the default option)—Router-to-router uses IP address and user information to dynamically configure connections between the nodes. Use router-to-router connections when the nodes in the cluster are not in the same multicast domain, or when they are in different subnets.

Note

Cisco recommends MDNS routing because it can seamlessly support new XCP routers joining the XCP route fabric.

Advanced Routing Prerequisites

Before you configure your routing, make sure that your system meets these requirements. The requirement depends on which type of routing method you want to use: MDNS routing or router-to-router:
MDNS Routing Prerequisites

The following prerequisites exist:

- You must have multicast DNS configured in the IOS network. When multicast DNS is disabled in the network, MDNS packets cannot reach the other nodes in a cluster. In some networks, multicast is enabled by default or enabled in a certain area of the network. For example, it may be enabled 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. If multicast DNS is disabled in your network, you must perform a configuration change to your network equipment to use MDNS routing.

- Make sure that all nodes are in the same multicast domain.

Router-to-Router Prerequisites

If DNS is available in the network then you can use IP addresses, hostnames or FQDNs as for your cluster node names. However, if DNS is not available in your network, you must use IP addresses for node names.

If you need to reset your node names to use IP addresses, refer to the "Node Name Change" topics in the Changing the IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service guide at http://www.cisco.com/c/en/us/support/%20unified-communications/unified-communications-manager-callmanager/%20products-maintenance-guides-list.html.

Advanced Routing Configuration Task Flow

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Configure the Routing Communication Method, on page 105</td>
<td>The Routing Communication type determines the routing method the IM and Presence Service uses to establish router connections between cluster nodes. For single node IM and Presence Service deployments, we recommend that you leave the routing communication type at the default setting.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Restart the Cisco XCP Router, on page 106</td>
<td>If you edited the Routing Communication Type, you must restart the Cisco XCP Router.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configure Secure Router-to-Router Communications, on page 106.</td>
<td>Optional. If you have Router-to-Router communication configured, you can configure secure TLS connections between XMPP routers in the same cluster or different clusters. <strong>Note</strong> You should enable this option only if the IM and Presence Service runs over an unsecure network as this option may degrade performance</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configure the Cluster ID, on page 107</td>
<td>If you use MDNS routing, confirm that the Cluster ID is shared by all nodes within the</td>
</tr>
</tbody>
</table>
### Configure the Routing Communication Method

The Routing Communication type determines the routing method the IM and Presence Service uses to establish router connections between cluster nodes. 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, MDNS must be enabled throughout your IOS network.

**Procedure**

**Step 1**
On the IM and Presence database publisher node, log in to Cisco Unified CM IM and Presence Administration.

**Step 2**
Choose System > Service Parameters.

**Step 3**
From the Server drop-down list box, select an IM and Presence Service node.

**Step 4**
From the Service drop-down list box, choose Cisco XCP Router

**Step 5**
Under XCP Router Global Settings (Clusterwide), select a routing type for the Routing Communication Type service parameter:

- **Multicast DNS (MDNS)**—Choose this method if the nodes in your cluster are in the same multicast domain.

- **Router-to-Router (auto)**—Choose this method if the nodes in your cluster are not in the same multicast domain. This is the default setting.

**Note**
When you use router-to-router connections, your deployment will incur additional performance overhead while IM and Presence Service establishes the XCP route fabric.
Step 6  
Click Save.

What to do next
If you edited this setting, you must Restart the Cisco XCP Router, on page 106

Restart the Cisco XCP Router
If you edited the Routing Communication Type, restart the Cisco XCP Router service

Before you begin
Configure the Routing Communication Method, on page 105

Procedure

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

Step 2  
From the Server list, choose the node on which you want to reactivate services and click Go.

Step 3  
In the IM and Presence Services area, select Cisco XCP Router.

Step 4  
Click Restart.

What to do next
If you have Router-to-Routerr routing configured, Configure Secure Router-to-Router Communications, on page 106.
If you have MDNS routing configured, Configure the Cluster ID, on page 107.

Configure Secure Router-to-Router Communications
If you have Router-to-Router communication configured, you can use this optional procedure to use secure TLS connections between XMPP routers in the same cluster or different clusters. The IM and Presence Service automatically replicates the XMPP certificate within the cluster, and across clusters, as an XMPP trust certificate.

Note
You should enable this option only if the IM and Presence Service runs over an unsecure network as this option may degrade performance.

Procedure

Step 1  
From Cisco Unified CM IM and Presence Administration, choose System > Security > Settings.

Step 2  
Check the Enable XMPP Router-to-Router Secure Mode check box.
Configure the System

Configure the Cluster ID

If you use MDNS routing, confirm that the Cluster ID is shared by all nodes within the cluster and that the value is unique for each cluster. If required, you can use this procedure to update the Cluster ID.

**Note**

At installation, the system assigns a default unique Cluster ID to each IM and Presence Service cluster. Cisco recommends that you leave the default setting value, unless it's necessary to change it.

**Procedure**

Step 1 On the IM and Presence Service database publisher node, log in to Cisco Unified CM IM and Presence Administration.

Step 2 Choose Presence > Settings > Standard Configuration.

Step 3 Check the value in the Cluster ID field. If you need to edit the ID, enter the new value.

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.

Step 4 Click Save.

If you edited the Cluster ID, the new setting replicates to all cluster nodes.

What to do next

Configure Throttling Rate for Presence Updates, on page 107

Configure Throttling Rate for Presence Updates

Use this optional procedure to configure the rate of availability (presence) changes sent to the Cisco XCP Router in messages per second. This configuration may help to prevent an overload when the IM and Presence Service throttles the rate of availability (presence) changes back to meet the configured value.

**Procedure**

Step 1 In Cisco Unified CM IM and Presence Administration, choose System > Service Parameters.

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

Step 3 From the Service drop-down list box, choose Cisco Presence Engine.
Step 4  In the Clusterwide Parameters (Parameters that apply to all servers) section, edit the Presence Change Throttle Rate service parameter. The valid range is 10 – 100 with a default setting of 50.

Step 5  Click Save.

What to do next

If you want to configure a SIP static route for federation connections, Configure Static Routes, on page 108.

Configure Static Routes

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Configure SIP Proxy Server Settings, on page 108</td>
<td>Configure your SIP Proxy Server settings. For WAN Deployments, Cisco recommends that you enable TCP method event routing on IM and Presence Service.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure Route Embed Templates on IM and Presence Service, on page 108</td>
<td>If your static route includes an embedded wildcard, you must configure a route embed template.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure Static Routes on IM and Presence Service, on page 110</td>
<td>Configure static route settings.</td>
</tr>
</tbody>
</table>

Configure SIP Proxy Server Settings

<table>
<thead>
<tr>
<th>Step</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In Cisco Unified CM IM and Presence Administration, choose Presence &gt; Routing &gt; Settings.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Choose On for the Method/Event Routing Status. For WAN deployments, Cisco recommends that you configure TCP method event routing on IM and Presence Service.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose Default SIP Proxy TCP Listener for the Preferred Proxy Server.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>

Configure Route Embed Templates on IM and Presence Service

If your static route includes an embedded wildcard, you must configure a route embed template.

<table>
<thead>
<tr>
<th>Step</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In Cisco Unified CM IM and Presence Administration, choose System &gt; Service Parameters.</td>
</tr>
<tr>
<td>Step 2</td>
<td>From the Server drop-down, select an IM and Presence Service node.</td>
</tr>
</tbody>
</table>
Step 3
From the Service drop-down, select Cisco SIP Proxy.

Step 4
Under Routing Parameters (Clusterwide), enter your template in the RouteEmbedTemplate field. You can define up to five templates. There is no limit to the number of static routes that you can define for a single route embed template.

Step 5
Click Save.

What to do next
Configure Static Routes on IM and Presence Service, on page 110

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>
<thead>
<tr>
<th>Destination Pattern</th>
<th>Next Hop Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>74..7812345*</td>
<td>1.2.3.4:5060</td>
</tr>
<tr>
<td>74..7867890*</td>
<td>5.6.7.8.9:5060</td>
</tr>
<tr>
<td>74..7811993*</td>
<td>10.10.11.37:5060</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Destination Pattern</th>
<th>Next Hop Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>471….34*</td>
<td>20.20.21.22</td>
</tr>
</tbody>
</table>
Configure Static Routes on IM and Presence Service

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)

Procedure

Step 1  In Cisco Unified CM IM and Presence Administration, choose Routing > Static Routes.
Step 2  Click Add New.
Step 3  in the Destination Pattern, enter the route pattern.
Step 4  In the Next Hop field, enter the IP Address, FQDN or hostname of the next hop server.
Step 5  In the Next Hop Port, enter the destination port on the Next Hop server. The default port is 5060.
Step 6  From the Route Type drop-down, select the type of route: User or Domain.
Step 7  From the Protocol Type drop-down list box, select the protocol for the static route: TCP, UDP, or TLS.
Step 8  Complete the remaining fields in the Static Route Configuration window.
Step 9  Click Save.

Static Route Parameters Settings

The following table lists the static route parameter settings that you can configure for IM and Presence Service.
**Table 12: Static Route Parameters Settings for IM and Presence Service**

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Pattern</td>
<td>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.</td>
</tr>
<tr>
<td>Wildcard Usage</td>
<td>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.</td>
</tr>
<tr>
<td>For phones:</td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• An asterisk can only exist at the end of the pattern.</td>
</tr>
<tr>
<td>For IP addresses and host names:</td>
<td>• You can use an asterisk as part of the a host name.</td>
</tr>
<tr>
<td></td>
<td>• The dot acts as a literal value in a host name.</td>
</tr>
<tr>
<td></td>
<td>An escaped asterisk sequence, \*, matches a literal * and can exist anywhere.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies the description of a particular static route, up to a maximum of 255 characters.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Next Hop Port</td>
<td>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.</td>
</tr>
<tr>
<td>Route Type</td>
<td>Specifies the route type: User or Domain. The default value is user. For example, in the SIP URI “sip:<a href="mailto:19194762030@myhost.com">19194762030@myhost.com</a>” 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.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Protocol Type</td>
<td>Specifies the protocol type for this route, TCP, UDP, or TLS. The default value is TCP.</td>
</tr>
<tr>
<td>Priority</td>
<td>Specifies the route priority level. Lower values indicate higher priority. The default value is 1.</td>
</tr>
<tr>
<td></td>
<td>Value range: 1-65535</td>
</tr>
<tr>
<td>Weight</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Value range: 1-65535</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Consider these three routes with associated priorities and weights:</td>
</tr>
<tr>
<td></td>
<td>• 1, 20</td>
</tr>
<tr>
<td></td>
<td>• 1, 10</td>
</tr>
<tr>
<td></td>
<td>• 2, 50</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Allow Less-Specific Route</td>
<td>Specifies that the route can be less specific. The default setting is On.</td>
</tr>
<tr>
<td>In Service</td>
<td>Specifies whether this route has been taken out of service. Specifies whether this route has been taken out of service.</td>
</tr>
<tr>
<td>Block Route Check Box</td>
<td>Check to block the static route. The default setting is Unblocked.</td>
</tr>
</tbody>
</table>
Chapter 11

Configure Certificates

- Certificates Overview, on page 113
- Certificates Prerequisites, on page 115
- Certificate Exchange with Cisco Unified Communications Manager, on page 115
- Install Certificate Authority (CA) on IM and Presence Service, on page 118
- Upload Certificates to IM and Presence Service, on page 120
- Generate a CSR, on page 124
- Generate a Self-Signed Certificate, on page 126
- Certificate Monitoring Task Flow, on page 128

Certificates Overview

Certificates are used to secure identities and to build a trust relationship between the IM and Presence Service and another system. You can use certificates to connect the IM and Presence Service to Cisco Unified Communications Manager, to Cisco Jabber clients, or to any external server. Without certificates, it would be impossible to know if a rogue DNS server was used, or if you were routed to another server.

There are two main classes of certificates that the IM and Presence Service can use:

- Self-signed Certificates—Self-signed certificates are signed by the same server that issues the certificate. Within an enterprise, you may use self-signed certificates to connect with another internal system, provided none of those connections are travelling over an unsecured network. For example, the IM and Presence Service might generate self-signed certificates for an internal connection to Cisco Unified Communications Manager.

- CA-signed Certificates—These are certificates that are signed by a third-party Certificate Authority (CA). These can be signed by a public CA (such as Verisign, Entrust or DigiCert) or a server (like Windows 2003, Linux, Unix, IOS) that controls the validity of the server/service certificate. CA-signed certificates are more secure than self-signed certificates and are typically used for any WAN connections. For example, a Federation connection with another enterprise or an intercluster peer configuration that uses WAN connections would require CA-signed certificates to build a trust relationship with the external system.

CA-signed certificates are more secure than self-signed certificates. In general, self-signed certificates are considered fine for internal connections, but for any WAN connections or connections that go across the public internet, you should use CA-signed certificates.
Multi-Server Certificates

The IM and Presence Service also supports multi-server SAN certificates for some system services. When you generate a Certificate Signing Request (CSR) for a multi-server certificate, the resulting multi-server certificate and its associated chain of signing certificates are distributed automatically to all cluster nodes once the certificate is uploaded to any cluster node.

Certificate Types in the IM and Presence Service

Within the IM and Presence Service, the different system components require different types of certificates. The following table describes the different certificates that are required for clients and services on the IM and Presence Service.

Note

If the certificate name ends in -ECDSA, then the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.

Table 13: Certificate Types and Services

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Service</th>
<th>Certificate Trust Store</th>
<th>Multi-Server Support</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>tomcat,</td>
<td>Cisco Client Profile Agent,</td>
<td>tomcat- trust</td>
<td>Yes</td>
<td>Presented to a Cisco Jabber client as part of client authentication for IM and Presence Service.</td>
</tr>
<tr>
<td>tomcat-ECDSA</td>
<td>Cisco AXL Web Service,</td>
<td></td>
<td></td>
<td>Presented to a web browser when navigating the Cisco Unified CM IM and Presence Administration user interface.</td>
</tr>
<tr>
<td></td>
<td>Cisco Tomcat</td>
<td></td>
<td></td>
<td>The associated trust-store is used to verify connections made by IM and Presence Service for the purposes of authenticating user credentials with a configured LDAP server.</td>
</tr>
<tr>
<td>ipsec</td>
<td></td>
<td>ipsec-trust</td>
<td>No</td>
<td>Used when an IPSec policy is enabled.</td>
</tr>
<tr>
<td>cup,</td>
<td>Cisco SIP Proxy,</td>
<td>cup-trust</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>cup-ECDSA</td>
<td>Cisco Presence Engine</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate Type</td>
<td>Service</td>
<td>Certificate Trust Store</td>
<td>Multi-Server Support</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------------</td>
<td>-------------------------</td>
<td>----------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>cup-xmpp,</td>
<td>Cisco XCP Connection Manager,</td>
<td>cup-xmpp-trust</td>
<td>Yes</td>
<td>Presented to a Cisco Jabber client, third-Party XMPP client, or a CAXL based application when the XMPP session is being created. The associated trust-store is used to verify connections made by Cisco XCP Directory service in performing LDAP search operations for third-party XMPP clients. The associated trust-store is used by the Cisco XCP Router service when establishing secure connections between IM and Presence Service servers if the Routing Communication Type is set to Router-to-Router.</td>
</tr>
<tr>
<td>cup-xmpp-ECDSA</td>
<td>Cisco XCP Web Connection Manager,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco XCP Directory service,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco XCP Router service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cup-xmpp-s2s,</td>
<td>Cisco XCP XMPP Federation Connection Manager</td>
<td>cup-xmpp-trust</td>
<td>Yes</td>
<td>Presented for XMPP interdomain federation when connecting to externally federated XMPP systems.</td>
</tr>
<tr>
<td>cup-xmpp-s2s-ECDSA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Certificates Prerequisites**

Configure the following items on Cisco Unified Communications Manager:

- Configure a SIP trunk 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.

**Certificate Exchange with Cisco Unified Communications Manager**

Complete these tasks to exchange certificates with Cisco Unified Communications Manager.

**Note**

The certificate exchange between Cisco Unified Communications Manager and the IM and Presence Service gets handled during the installation process automatically. However, complete these tasks if you need to complete the certificate exchange manually.
## Import Cisco Unified Communications Manager Certificate to IM and Presence Service

Use this procedure to import a certificate from Cisco Unified Communications Manager into the IM and Presence Service.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Import Cisco Unified Communications Manager Certificate to IM and Presence Service, on page 116</td>
<td>Import a certificate from Cisco Unified Communications Manager into the IM and Presence Service.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Download Certificate from IM and Presence Service, on page 117</td>
<td>Download a certificate from the IM and Presence Service. The certificate will need to be imported into Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Import IM and Presence Certificate to Cisco Unified Communications Manager, on page 117</td>
<td>To complete the certificate exchange, import the IM and Presence Service certificate into the Callmanager-trust store of Cisco Unified Communications Manager.</td>
</tr>
</tbody>
</table>

### Import Cisco Unified Communications Manager Certificate to IM and Presence Service

Use this procedure to import a certificate from Cisco Unified Communications Manager into the IM and Presence Service.

### Procedure

**Step 1**
In Cisco Unified CM IM and Presence Administration, choose 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.

**Note**
Depending on the negotiated TLS cipher, the Certificate Import Tool will download either an RSA-based certificate or an ECDSA-based certificate.

**Step 6**
Restart the Cisco SIP Proxy service:

a) From Cisco Unified IM and Presence Serviceability, choose Tools > Control Center - Feature Services on IM and Presence Service.

b) From the Server drop-down list box, select an IM and Presence Service cluster node and click Go.
c) Choose **Cisco SIP Proxy** and click **Restart**.

---

**What to do next**

*Download Certificate from IM and Presence Service, on page 117*

---

## Download Certificate from IM and Presence Service

Use this procedure to download a certificate from the IM and Presence Service. The certificate will need to be imported into Cisco Unified Communications Manager.

### Procedure

**Step 1**

From **Cisco Unified IM and Presence OS Administration**, choose **Security > Certificate Management** on IM and Presence Service.

**Step 2**

Click **Find**.

**Step 3**

Choose the **cup.pem** file.

*Note*  
*cup-ECDSA.pem* is also an available option.

**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**

*Import IM and Presence Certificate to Cisco Unified Communications Manager, on page 117*

---

## Import IM and Presence Certificate to Cisco Unified Communications Manager

To complete the certificate exchange, import the IM and Presence Service certificate into the Callmanager-trust store of Cisco Unified Communications Manager.

### Before you begin

*Download Certificate from IM and Presence Service, on page 117*

### Procedure

**Step 1**

Log into Cisco Unified OS Administration.

**Step 2**

Choose **Security > Certificate Management**

**Step 3**

Click **Upload Certificate**.
Install Certificate Authority (CA) on IM and Presence Service

In order to use certificates signed by a third-party Certificate Authority (CA) in the IM and Presence Service, you must first install that CA’s root certificate chain of trust on the IM and Presence Service.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Upload CA Root Certificate Chain, on page 118</td>
<td>Use this procedure to upload the CA root certificate chain from the third-party Certificate Authority to the IM and Presence Service.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Restart Cisco Intercluster Sync Agent Service, on page 119</td>
<td>After you have uploaded certificates, restart the Cisco Intercluster Sync Agent service.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Verify CA Certificates Have Synchronized to Other Clusters, on page 119</td>
<td>Verify that your CA certificate chain has replicated to all peer clusters.</td>
</tr>
</tbody>
</table>

**Upload CA Root Certificate Chain**

Use this procedure to upload the certificate chain from the signing Certificate Authority (CA) to the IM and Presence database publisher node. The chain may consist of multiple certificates in a chain, with each certificate signing the subsequent certificate:


### Procedure

- **Step 1** On the IM and Presence database publisher node, log in to Cisco Unified IM and Presence OS Administration.
- **Step 2** Choose Security > Certificate Management.
- **Step 3** Click Upload Certificate/Certificate chain.
- **Step 4** From the Certificate Name drop-down list, choose one of the following:
  - If you are uploading a CA-signed tomcat certificate, choose tomcat-trust
• If you are uploading a CA-signed cup-xmpp certificate or a CA signed cup-xmpp-s2s, choose cup-xmpp-trust

Step 5 Enter a Description for the signed certificate.
Step 6 Click Browse to locate the file for the Root Certificate.
Step 7 Click Click Upload File.
Step 8 Upload each intermediate certificate in the same way using the Upload Certificate/Certificate chain window. For each intermediate certificate, you must enter the name of the preceding certificate in the chain.

What to do next
Restart Cisco Intercluster Sync Agent Service, on page 119

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 restart ensures that the CA certificates are synced immediately to all other clusters.

Procedure

Step 1 From Cisco Unified IM and Presence Serviceability, choose Tools > Control Center - Network Services.
Step 2 From the Server drop-down list box, select the IM and Presence Service node on which you imported the certificate and click Go.

Note You can also restart the Cisco Intercluster Sync Agent service from the Command Line Interface with the utils service restart Cisco Intercluster Sync Agent command.

Step 3 Select the Cisco Intercluster Sync Agent service and click Restart.

What to do next
Verify Intercluster Syncing, on page 122

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.

Note The information in the following procedure also applies to certificates ending in –ECDSA.
Procedure

Step 1  In Cisco Unified CM IM and Presence Administration, choose 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 it 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: utilss 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 Certificates to IM and Presence Service

Complete these tasks to upload certificates to the IM and Presence Service. You can upload CA-signed certificates or self-signed certificates.

Before you begin
To use CA-signed certificates that are signed by a third-party Certificate Authority (CA), you must already have installed that CA's root certificate chain on the IM and Presence Service. For details, Install Certificate Authority (CA) on IM and Presence Service, on page 118.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Upload Certificates, on page 121</td>
<td>Upload signed certificates to the IM and Presence Service.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Restart Cisco Tomcat Service, on page 122</td>
<td>(Tomcat certificates only). Restart the Cisco Tomcat Service.</td>
</tr>
</tbody>
</table>
## Upload Certificates

Use this procedure to upload certificates 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.

### Note

The information in the following procedure also applies to certificates ending in 

### Before you begin

If the certificate is signed by a CA, you must have also installed that CA's root certificate chain or the CA-signed certificate will be untrusted. When the CA certificates have correctly synced to all clusters, you can upload the appropriate signed certificate to each IM and Presence Service node.

### Procedure

- **Step 1**  
  In *Cisco Unified IM and Presence OS Administration*, choose *Security > Certificate Management*.

- **Step 2**  
  Click *Upload Certificate/Certificate chain*.

- **Step 3**  
  Select the *Certificate Purpose*. For example, *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.

What to do next
Restart the Cisco Tomcat service.

Restart Cisco Tomcat Service

After you upload tomcat certificates 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  In Cisco Unified CM IM and Presence Administration, choose 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.

---

**Restart the Cisco XCP Router service on all nodes**

After you upload a cup-xmpp and/or cup-xmpp-ECDSA certificate to each IM and Presence Service node, you must restart the Cisco XCP Router service on each node.

**Note** You can also restart the Cisco XCP Router service from the Cisco Unified IM and Presence Serviceability GUI.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Log into the admin CLI.</td>
</tr>
<tr>
<td>2</td>
<td>Run the following command: utils service restart Cisco XCP Router.</td>
</tr>
<tr>
<td>3</td>
<td>Repeat for each node.</td>
</tr>
</tbody>
</table>

---

**Restart Cisco XCP XMPP Federation Connection Manager Service**

After you upload the cup-xmpp-s2s and/or cup-xmpp-s2s-ECDSA 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Log into the admin CLI.</td>
</tr>
<tr>
<td>2</td>
<td>Run the following command: utils service restart Cisco XCP XMPP Federation Connection Manager.</td>
</tr>
<tr>
<td>3</td>
<td>Repeat for each federation node.</td>
</tr>
</tbody>
</table>

---

**Enable Wildcards in XMPP Federation Security Certificates**

To support group chat between XMPP federation partners over TLS, you must enable wildcards for XMPP security certificates.
By default, the XMPP federation security certificates `cup-xmpp-s2s` and `cup-xmpp-s2s-ECDSA` contains all domains hosted by the IM and Presence Service deployment. These are added as Subject Alternative Name (SAN) entries within the certificate. You must supply wildcards for all hosted domains within the same certificate. So instead of a SAN entry of "example.com", the XMPP security certificate must contain a SAN entry of "*.example.com". The wildcard is needed because the group chat server aliases are sub-domains of one of the hosted domains on the IM and Presence Service system. For example: “conference.example.com”.

To view the `cup-xmpp-s2s` or `cup-xmpp-s2s-ECDSA` certificates on any node, choose Cisco Unified IM and Presence OS Administration > Security > Certificate Management and click on the `cup-xmpp-s2s` or `cup-xmpp-s2s-ECDSA` links.

### Procedure

**Step 1** Choose System > Security Settings.

**Step 2** Check Enable Wildcards in XMPP Federation Security Certificates.

**Step 3** Click Save.

### What to do next

You must regenerate the XMPP federation security certificates on all nodes within the cluster where the Cisco XMPP Federation Connection Manager service is running and XMPP Federation is enabled. This security setting must be enabled on all IM and Presence Service clusters to support XMPP Federation Group Chat over TLS.

## Generate a CSR

Use this procedure to generate a Certificate Signing Request (CSR). You will need the CSR to submit to the third-party CA so that they can provide you with a CA-signed certificate.

### Procedure

**Step 1** From Cisco Unified OS Administration, choose Security > Certificate Management.

**Step 2** Click the Generate CSR button. The Generate Certificate Signing Request popup displays.

**Step 3** From the Certificate Purpose drop-down, select the type of certificate that you are generating.

**Step 4** From the Distribution drop-down, select an IM and Presence server. For multi-server certificates, select Multi-server (SAN).

**Step 5** Enter the Key Length and Hash Algorithm.

**Step 6** Complete any remaining fields and click Generate.

**Step 7** Download the CSR to a local computer:

a) Click Download CSR.

b) Choose the certificate name from the Certificate Purpose drop-down list.
c) **Download CSR**

---

**What to do next**

Submit the CSR to the third-party Certificate Authority so that they can issue you a CA-signed certificate.

### CSR Key Usage Extensions

The following tables display key usage extensions for Certificate Signing Requests (CSRs) for both Unified Communications Manager and the IM and Presence Service CA certificates.

**Table 14: Cisco Unified Communications Manager CSR Key Usage Extensions**

<table>
<thead>
<tr>
<th>Multi server</th>
<th>Extended Key Usage</th>
<th>Key Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Server Authentication (1.3.6.1.5.5.7.3.1)</td>
<td>Client Authentication (1.3.6.1.5.5.7.3.2)</td>
</tr>
<tr>
<td>CallManager</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>CallManager-ECDSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAPF (publisher only)</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>ipsec</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>ipsec-ECDSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tomcat</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>tomcat-ECDSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TVS</td>
<td>N</td>
<td>Y</td>
</tr>
</tbody>
</table>

**Table 15: IM and Presence Service CSR Key Usage Extensions**

<table>
<thead>
<tr>
<th>Multi server</th>
<th>Extended Key Usage</th>
<th>Key Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Server Authentication (1.3.6.1.5.5.7.3.1)</td>
<td>Client Authentication (1.3.6.1.5.5.7.3.2)</td>
</tr>
<tr>
<td>cup</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>cup-ECDSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cup-xmpp</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>cup-xmpp-ECDSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cup-xmpp-s2s</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>cup-xmpp-s2s-ECDSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipsec</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>tomcat</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>tomcat-ECDSA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Generate a Self-Signed Certificate

Use this procedure to generate a self-signed certificate.

Procedure

Step 1 From Cisco Unified OS Administration, choose Security > Certificate Management.
Step 2 Click Generate Self-Signed. The Generate New Self-Signed Certificate popup displays.
Step 3 From the Certificate Purpose drop-down, select the type of certificate that you are generating.
Step 4 From the Distribution drop-down, enter the name of the server.
Step 5 Select the appropriate Key Length.
Step 6 From the Hash Algorithm, select the encryption algorithm. For example, SHA256.
Step 7 Click Generate.

Delete Self Signed Trust Certificates from IM and Presence Service

To support cross navigation for serviceability between nodes in the same cluster, the Cisco Tomcat service trust stores between the IM and Presence Service and Cisco Unified Communications Manager are synchronized automatically.

If you have replaced the original self-signed trust certificates with CA-signed certificates, the original self-signed trust certificates persist in the service trust store. You can use this procedure to delete the self-signed certificates on the IM and Presence Service and Cisco Unified Communications Manager nodes.

Before you begin

Important
If you added CA-signed certificates, make sure that you have 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 From Cisco Unified IM and Presence Operating System Administration, 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 and Tomcat-ECDSA — tomcat-trust
• Cup-xmpp and Cup-xmpp-ECDSA — cup-xmpp-trust
• Cup-xmpp-s2s and Cup-xmpp-s2s-ECDSA — cup-xmpp-trust
• Cup and Cup-ECDSA — 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 appears only if you have the authority to delete that certificate.

Step 5  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.

What to do next
If the service is Tomcat, you must check for the IM and Presence Service node's self signed tomcat-trust certificate on the Cisco Unified Communications Manager node. See, Delete Self-Signed Tomcat-Trust Certificates from Cisco Unified Communications Manager, on page 127.

Delete Self-Signed Tomcat-Trust Certificates from Cisco Unified Communications Manager

There is a self-signed tomcat-trust certificate in the Cisco Unified Communications Manager service trust store for each node in the cluster. These are the only certificates that you delete from the Cisco Unified Communications Manager node.

**Note**  The information in the following procedure also applies to -EC certificates.

Before you begin
Ensure that you have configured the cluster's IM and Presence Service nodes with CA-signed certificates, and you have waited for 30 minutes to allow the certificates to propagate to the Cisco Unified Communications Manager node.

Procedure

Step 1  In Cisco Unified Operating System Administration, choose Security > Certificate Management.

The Certificate List window appears.
Step 2  To filter the search results, choose Certificate and begins with from the drop-down lists and then enter tomcat-trust in the empty field. Click Find.

The Certificate List window expands with the tomcat-trust certificates listed.

Step 3  Identify the links that contain an IM and Presence Service node's hostname or FQDN in its name. These are self-signed certificates associated with this service and an IM and Presence Service node.

Step 4  Click the link to an IM and Presence Service node's self-signed tomcat-trust certificate.

A new window appears that shows the tomcat-trust certificate details.

Step 5  Confirm in the Certificate Details that this is a self-signed certificate by ensuring that the Issuer Name CN= and the Subject Name CN= values match.

Step 6  If you have confirmed that it is a self-signed certificate and you are certain that the CA-signed certificate has propagated to the Cisco Unified Communications Manager node, click Delete.

Note  The Delete button only appears for certificates that you have the authority to delete.

Step 7  Repeat steps 4, 5, and 6 for each IM and Presence Service node in the cluster.

---

**Certificate Monitoring Task Flow**

Complete these tasks to configure the system to monitor certificate status and expiration. You can configure the system to do the following automatically:

- Email you when certificates are approaching expiration.
- Revoke expired certificates.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Configure Certificate Monitor Notifications, on page 128</td>
<td>Configure automatic certificate monitoring. The system periodically checks certificate statuses and emails you when a certificate is approaching expiration.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Configure Certificate Revocation via OCSP, on page 129</td>
<td>Configure the Online Certificate Status Protocol (OCSP) so that the system revokes expired certificates automatically.</td>
</tr>
</tbody>
</table>

**Configure Certificate Monitor Notifications**

Configure automated certificate monitoring for Unified Communications Manager or the IM and Presence Service. The system periodically checks the status of certificates and emails you when a certificate is approaching expiration.
Note
The Cisco Certificate Expiry Monitor network service must be running. This service is enabled by default, but you can confirm the service is running in Cisco Unified Serviceability by choosing Tools > Control Center - Network Services and verifying that the Cisco Certificate Expiry Monitor Service status is Running.

Procedure

Step 1 Log into Cisco Unified OS Administration (for Unified Communications Manager certificate monitoring) or Cisco Unified IM and Presence Administration (for IM and Presence Service certificate monitoring).
Step 3 In the Notification Start Time field, enter a numeric value. This value represents the number of days before certificate expiration where the system starts to notify you of the upcoming expiration.
Step 4 In the Notification Frequency fields, enter the frequency of notifications.
Step 5 Optional. Check the Enable E-mail notification check box to have the system send email alerts of upcoming certificate expirations.
Step 6 Check the Enable LSC Monitoring check box to include LSC certificates in the certificate status checks.
Step 7 In the E-mail IDs field, enter the email addresses where you want the system to send notifications. You can enter multiple email addresses separated by a semicolon.
Step 8 Click Save.

What to do next
Configure the Online Certificate Status Protocol (OCSP) so that the system revokes expired certificates automatically. For details, see Configure Certificate Revocation via OCSP, on page 129

Configure Certificate Revocation via OCSP

Enable the Online Certificate Status Protocol (OCSP) to check certificate status regularly and to revoke expired certificates automatically.

Before you begin
Make sure that your system has the certificates that are required for OCSP checks. You can use Root or Intermediate CA certificates that are configured with the OCSP response attribute or you can use a designated OCSP signing certificate that has been uploaded to the tomcat-trust.

Procedure

Step 1 Log in to Cisco Unified OS Administration (for Unified Communications Manager certificate revocation) or Cisco Unified IM and Presence Administration (for IM and Presence Service certificate revocation).
Step 3 Check the Enable OCSP check box, and perform one of the following tasks:
If you want to specify an OCSP responder for OCSP checks, select the **Use configured OCSP URI** button and enter the URI of the responder in the **OCSP Configured URI** field.

If the certificate is configured with an OCSP responder URI, select the **Use OCSP URI from Certificate** button.

**Step 4**  
Check the **Enable Revocation Check** check box.

**Step 5**  
Complete the **Check Every** field with the interval period for revocation checks.

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

**Step 7**  
Optional. If you have CTI, IPsec or LDAP links, you must also complete these steps in addition to the above steps to enable OCSP revocation support for those long-lived connections:

a) From Cisco Unified CM Administration, choose **System > Enterprise Parameters**.

b) Under **Certificate Revocation and Expiry**, set the **Certificate Validity Check** parameter to **True**.

c) Configure a value for the **Validity Check Frequency** parameter.

**Note**  
The interval value of the **Enable Revocation Check** parameter in the **Certificate Revocation** window takes precedence over the value of the **Validity Check Frequency** enterprise parameter.

d) Click **Save**.
CHAPTER 12

Configure Security Settings

• Security Overview, on page 131
• Security Settings Configuration Task Flow, on page 131

Security Overview

This chapter contains procedures for configuring security settings on the IM and Presence Service. On the IM and Presence Service, you can configure secure TLS connections and enable enhanced security settings such as FIPS mode.

The IM and Presence Service shares a platform with Cisco Unified Communications Manager. For information on how to configure security in Cisco Unified Communications Manager, refer to the Security Guide for Cisco Unified Communications Manager.

Security Settings Configuration Task Flow

Complete these optional tasks to set up security with the IM and Presence Service.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create Login Banner, on page 132</td>
<td>Create a login banner that users must acknowledge when they log in to any IM and Presence Service interface.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure Secure XMPP Connections, on page 132</td>
<td>Complete these tasks to configure XMPP security.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure TLS Peer Subject, on page 133</td>
<td>Configure these tasks if you want to set up TLS peers.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure TLS Context, on page 134</td>
<td>Configure a TLS Context and TLS ciphers for your TLS peers.</td>
</tr>
<tr>
<td>Step 5</td>
<td>FIPS Mode, on page 134</td>
<td>If you want your deployment to be FIPS-compliant, you can enable FIPS mode.</td>
</tr>
</tbody>
</table>
Create Login Banner

You can create a banner that users acknowledge as part of their login to any IM and Presence Service interface. You create a .txt file using any text editor, include important notifications they want users to be made aware of, and upload it to the Cisco Unified IM and Presence OS Administration page.

This banner will then appear on all IM and Presence Service interfaces notifying users of important information before they login, including legal warnings and obligations. The following interfaces will display this banner before and after a user logs in: Cisco Unified CM IM and Presence Administration, Cisco Unified IM and Presence Operating System Administration, Cisco Unified IM and Presence Serviceability, Cisco Unified IM and Presence Reporting, and IM and Presence Disaster Recovery System.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Create a .txt file with the contents you want to display in the banner.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Sign in to Cisco Unified IM and Presence Operating System Administration.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose Software Upgrades &gt; Customized Logon Message.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Browse and locate the .txt file.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Upload File.</td>
</tr>
</tbody>
</table>

The banner will appear before and after login on most IM and Presence Service interfaces.

Note: The .txt file must be uploaded to each IMand Presence Service node separately.

Configure Secure XMPP Connections

Use this procedure to enable secure XMPP connections using TLS.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From Cisco Unified CM IM and Presence Administration, choose System &gt; Security &gt; Settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Check the appropriate check box to enable the following XMPP security settings:</td>
</tr>
</tbody>
</table>
Table 16: XMPP Security Settings for the IM and Presence Service

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable XMPP Client To IM/P Service Secure Mode</td>
<td>When enabled, the IM and Presence Service establishes a secure TLS connection with XMPP client applications in a cluster. This setting is enabled 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.</td>
</tr>
<tr>
<td>Enable XMPP Router-to-Router Secure Mode</td>
<td>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.</td>
</tr>
<tr>
<td>Enable Web Client to IM/P Service Secure Mode</td>
<td>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.</td>
</tr>
</tbody>
</table>

Step 3: Click Save.

What to do next

If you updated the Enable XMPP Client To IM/P Service Secure Mode setting, restart the Cisco XCP Connection Manager.

**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: In Cisco Unified CM IM and Presence Administration, choose 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.
**Configure TLS Context**

Use this procedure to assign a TLS context and TLS ciphers to your TLS peer subjects.

---

**Note**

When you import an IM and Presence Service certificate, the IM and Presence Service automatically attempts to add the TLS peer subject to the TLS peer subject list, and to the TLS context list.

---

**Before you begin**

Configure TLS Peer Subject, on page 133

**Procedure**

2. Click Find.
4. From the list of available TLS peer subjects, select the TLS peer subject that you configured.
5. Use the > arrow to move this TLS peer subject to Selected TLS Peer Subjects.
6. Configure the TLS Cipher Mapping options:
   a) Review the list of TLS ciphers that are available in the Available TLS Ciphers and Selected TLS Ciphers boxes.
   b) If you want to enable a TLS cipher that isn't currently selected, use the > arrow to move the cipher to Selected TLS Ciphers.
7. Click Save.
8. Restart the Cisco SIP Proxy service:
   a) From Cisco Unified IM and Presence Serviceability, choose Tools > Control Center - Feature Services.
   b) From the Server drop-down list box, select an IM and Presence Service cluster node and click Go.
   c) Select the Cisco SIP Proxy service and click Restart.

---

**FIPS Mode**

The IM and Presence Service contains a set of enhanced system security modes that allow your system to operate in a stricter set of security guidelines and risk management controls around items such as cryptography, data and signaling encryption, and audit logging.
• FIPS Mode—The IM and Presence Service can be configured to operate in FIPS mode, which allows your system to comply with FIPS or Federal Information Processing Standards, a US and Canadian government standard for cryptographic modules.

• Enhanced Security Mode—Enhanced Security Mode runs on a FIPS-enabled system and provides additional risk management controls such as data encryption requirements, a stricter credential policy, user authentication for contact searches, and stricter audit logging requirements.

• Common Criteria Mode—Common Criteria mode also runs on a FIPS-enabled system providing additional controls that allow your system to comply with Common Criteria guidelines such as TLS and the use of X.509 v3 certificates.

FIPS Mode
Intercluster Peers Overview

Intercluster peering provides the ability for users in one cluster to communicate and subscribe to the presence of users in a different cluster within the same domain. For large deployments you can use intercluster peering to connect your remote IM and Presence clusters.

Intercluster peering is configured on the database publisher node of both the local and the remote cluster.


Intercluster Peers Prerequisites

Before you configure IM and Presence Service intercluster peers in your network, note the following:

• Configure the system topology and assign your users as required for all clusters.

• 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
## Intercluster Peers Configuration Task Flow

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Check User Provisioning, on page 138</td>
<td>Verify that end users are correctly provisioned before you configure intercluster peers.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Enable the Cisco AXL Web Service, on page 139</td>
<td>The Cisco AXL Web Service must be active on all local and remote IM and Presence nodes. Use this procedure to verify the service is running.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enable the Sync Agent, on page 139</td>
<td>Enable the Sync Agent on the database publisher node of each intercluster peer.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure Intercluster Peers, on page 140</td>
<td>Complete this task on the database publisher node in each cluster to set up intercluster peers.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Verify the Intercluster Sync Agent is On, on page 141</td>
<td>The Intercluster Sync Agent must be running on all nodes in the IM and Presence Service cluster. Use this procedure to verify that the Intercluster Sync Agent parameter is running.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Verify Intercluster Peer Status, on page 141</td>
<td>Verify that the intercluster peer configuration works.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Update Intercluster Sync Agent Tomcat Trust Certificates, on page 142</td>
<td>If the tomcat certificate status for an intercluster peer is out-of-sync, update the Tomcat trust certificate.</td>
</tr>
</tbody>
</table>

### Check User Provisioning

Use this procedure to verify that end users are correctly provisioned before you configure intercluster peers.

#### Procedure

1. From Cisco Unified CM IM and Presence Administration, choose **Diagnostics > System Troubleshooter**. The System Troubleshooter runs.
2. In the **User Troubleshooter** section, verify that end users are correctly provisioned and that there are no duplicate or invalid users.

#### What to do next

Enable the Cisco AXL Web Service, on page 139
Enable the Cisco AXL Web Service

The Cisco AXL Web Service must be running on all local and remote IM and Presence cluster nodes. By default, this service is running. However, you can use this procedure to verify that the service is running.

When you enable the Cisco AXL Web Service, the system creates an intercluster application user with AXL permissions. You will need the username and password for the intercluster application user when you configure intercluster peers on the remote IM and Presence Service node.

Procedure

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

**Step 2**
From the **Server** list, choose the node on which you want to reactivate services and click **Go**.

**Step 3**
In the **Database and Admin Services** area, check the **Status** of the **Cisco AXL Web Service**.

- If the service is **Started**, no action is required.
- If the service is **Not Running**, select the service and click **Restart**.

**Step 4**
Repeat this procedure on all cluster nodes in the local and remote clusters.

What to do next

Enable the Sync Agent, on page 139

Enable the Sync Agent

The Cisco Sync Agent must be running on the database publisher node of each intercluster peer on the local and remote IM and Presence database publisher nodes.

Procedure

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

**Step 2**
From the **Server** drop-down list box, choose the IM and Presence database publisher node and click **Go**.

**Step 3**
Under **IM and Presence Services**, verify that the **Cisco Sync Agent** status is **Running**.

**Step 4**
If the service is not running, select the service and click **Restart**.

**Step 5**
Repeat this procedure in each cluster.

What to do next

After the Cisco Sync Agent completes the user sync from Cisco Unified Communications Manager, Configure Intercluster Peers, on page 140
Configure Intercluster Peers

Use this procedure on the database publisher node for both the local and remote cluster to set up an intercluster peer relationship.

**Before you begin**

- Confirm that the Sync Agent has completed the user synchronization from Cisco Unified Communications Manager on the local and remote cluster. If you configure the intercluster peer connection before the Sync Agent completes the user sync, the status of the intercluster peer connection displays as **Failed**.

- Make sure that you have the AXL username and password for the intercluster application user on the remote IM and Presence Service node.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In Cisco Unified CM IM and Presence Administration, choose <strong>Presence &gt; Inter-Clustering</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click <strong>Add New</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>Peer Address</strong> field, enter the node name of the remote cluster's database publisher node. This field may be an IP address, hostname or FQDN, but must match the actual node name that defines the server.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To verify the type of address the node name uses, log in to Cisco Unified CM IM and Presence Administration on the remote cluster and choose <strong>System &gt; Presence Topology</strong>. This window displays the node name and server details for each cluster node.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter the AXL credentials.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select the preferred <strong>Protocol</strong> for SIP communication.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Cisco recommends that you use <strong>TCP</strong> (the default setting) as the intercluster trunk transport for all IM and Presence Service clusters. You can change this setting if it suits your network configuration and security needs.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click <strong>Save</strong>.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Check your notifications in the top right of the GUI header. If a notification advises you to restart the <strong>Cisco XCP Router</strong>, then do the following. Otherwise, you can skip this step:</td>
</tr>
<tr>
<td>a) From Cisco Unified IM and Presence Serviceability, choose <strong>Tools &gt; Control Center - Network Services</strong>.</td>
<td></td>
</tr>
<tr>
<td>b) From the <strong>Server</strong> drop-down list box, choose an IM and Presence node and click <strong>Go</strong>.</td>
<td></td>
</tr>
<tr>
<td>c) Select <strong>Cisco XCP Router</strong> and click <strong>Restart</strong>.</td>
<td></td>
</tr>
<tr>
<td>d) Repeat these steps on all cluster nodes</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>Repeat this procedure on the database publisher node of each remote peer cluster.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>If you choose <strong>TLS</strong> as the intercluster transport protocol, the 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.</td>
</tr>
</tbody>
</table>
What to do next
Verify the Intercluster Sync Agent is On, on page 141

Restart the XCP Router Service

Restart the Cisco XCP Router service on all nodes in the local cluster, as well as all nodes in the remote cluster.

Before you begin
Configure Intercluster Peers, on page 140

Procedure

Step 1 From Cisco Unified IM and Presence Serviceability, choose Tools > Control Center - Network Services.
Step 2 From the Server list, choose the node on which you want to reactivate services and click Go.
Step 3 In the IM and Presence Services area, select Cisco XCP Router.
Step 4 Click Restart.

What to do next
Verify the Intercluster Sync Agent is On, on page 141

Verify the Intercluster Sync Agent is On

The Intercluster Sync Agent network service synchronizes user information between intercluster peers. Use this procedure to confirm that the service is running on all cluster nodes in each intercluster peer.

Procedure

Step 1 From Cisco Unified IM and Presence Serviceability, choose Tools > Control Center - Network Services.
Step 2 From the Server menu, choose an IM and Presence Service node and click Go.
Step 3 Confirm that the Cisco Intercluster Sync Agent displays a status of Running.
Step 4 If the service is not running, select the service and click Start.
Step 5 Repeat this procedure for all cluster nodes on each intercluster peer.

What to do next
Verify Intercluster Peer Status, on page 141

Verify Intercluster Peer Status

Use this procedure to confirm that your intercluster peer configurations are working properly.
Procedure

Step 1  In Cisco Unified CM IM and Presence Administration, choose Presence > Inter-Clustering.
Step 2  Choose the peer address from the search criteria menu.
Step 3  Click Find.
Step 4  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 chose 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 5  Run the System Troubleshooter:
   a) From Cisco Unified CM IM and Presence Administration, choose Diagnostics > System Troubleshooter.
   b) In the Inter-Clustering Troubleshooter section, verify that there are check marks beside the status of each of the intercluster peer connection entries.

What to do next
Update Intercluster Sync Agent Tomcat Trust Certificates, on page 142

Update Intercluster Sync Agent Tomcat Trust Certificates

If a connection error occurs on the local cluster, and the corrupt Tomcat trust certificates are associated with the remote cluster, use this procedure to update the Tomcat trust certificate.

If the tomcat certificate status for an intercluster peer is out-of-sync, you must update the Tomcat trust certificate. In an intercluster deployment, this error can occur if you reuse an existing intercluster peer configuration to point to a new remote cluster. This error can also occur in a fresh IM and Presence Service installation, if you change the IM and Presence Service host or domain name, or if you regenerate the Tomcat certificate.

Procedure

Step 1  In Cisco Unified CM IM and Presence Administration, choose 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. All certificates marked with an X are the missing certificates which you need to copy manually.

Intercluster Peering Interactions and Restrictions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Interactions and Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVA Requirements</td>
<td>If you are deploying Persistent Chat or Intercluster Peering, the minimum OVA size that you can deploy for these features is the 5000 user OVA. It’s recommended that you deploy at least the 15,000 user OVA. Centralized Deployments may require the 25,000 user OVA, depending on the size of the user base. For additional details on OVA options and user capacities, refer to the following site: <a href="https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html">https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html</a></td>
</tr>
</tbody>
</table>
Configure Push Notifications for Cisco Jabber on iPhone and iPad

- Push Notifications Overview, on page 145
- Push Notifications Configuration, on page 147

Push Notifications Overview

When your cluster is enabled for Push Notifications, Cisco Unified Communications Manager and the IM and Presence Service use Apple’s cloud-based Push Notification service to push notifications for voice and video calls, instant messages, and Cisco WebEx invitations to Cisco Jabber for iPhone and iPad clients that are running in suspended mode. Push Notifications allows your system to maintain a persistent communication with Cisco Jabber. Push Notifications is required both for Cisco Jabber for iPhone and iPad clients that connect from within the enterprise network, and for clients that register to an on-premise deployment via Expressway’s Mobile and Remote Access (MRA) feature.

Note

Push Notifications is required only for Cisco Jabber for iPhone and iPad clients. The feature is not supported for Android and is not applicable for Windows and Mac users.

How Push Notifications Works

At startup, Cisco Jabber clients that are installed on iPhone and iPad devices register to Cisco Unified Communications Manager, the IM and Presence Service and to the Apple cloud. With MRA deployments, the Cisco Jabber for iPhone or iPad client registers to the on-premises servers via Expressway. So long as the Jabber client remains in foreground mode, Cisco Unified Communications Manager and the IM and Presence Service can send calls and instant messages to the Jabber client directly.

However, once the Cisco Jabber client moves to suspended mode (for example, to maintain battery life), the standard communication channel is unavailable, preventing Cisco Unified Communications Manager and IM and Presence Service from communicating directly with the client. Push Notifications provides another channel to reach the Jabber client via the Cisco and Apple clouds.
Cisco Jabber is considered to be running in suspended mode if any of the following conditions are true:

- the Cisco Jabber application is running off-screen (i.e., in the background)
- the iPhone or iPad is locked
- the iPhone or iPad screen is turned off

The above diagram displays what happens when Cisco Jabber for iPhone and iPad clients run in the background or are stopped. The figure illustrates: (1) an MRA deployment where the Cisco Jabber client that connects with an on-premises Cisco Unified Communications Manager and IM and Presence Service deployment via Expressway, and (2) a Cisco Jabber for iPhone or iPad client that connects directly to the on-premises deployment from within the enterprise network.

For a detailed description of what happens with each use case, see the following table:
### Table 17: Message Flow for Cisco Jabber for iPhone and iPad when Push Notifications is Enabled

<table>
<thead>
<tr>
<th>Jabber client is running...</th>
<th>Cisco Unified Communications Manager and IM and Presence Service send push notification to...</th>
</tr>
</thead>
</table>
| Foreground Mode             | Standard communication channels are used for voice, video, IM and Presence:  
                               | • For on-premises mobile clients, Cisco Unified Communications Manager and IM and Presence Service send the call or instant message to the Jabber client directly.  
                               | • For MRA clients, the call or IM notification is sent to the Jabber client via Expressway.  
                               | **Note** For voice and video calls, the Push Notification is still sent via the Push Notification channel, but the Cisco Jabber client uses the standard channel. |
| Suspended Mode              | **Voice or Video Calls**  
                               | Standard communication channels are unavailable. Cisco Unified Communications Manager uses the Push Notifications channel.  
                               | Upon receiving the notification, the Jabber client re-enters foreground mode automatically, and the client rings.  
                               | **Instant Messaging**  
                               | Standard communication channels are unavailable. IM and Presence Service uses the Push Notifications channel to send IM notifications as follows:  
                               | 1. IM and Presence Service sends the IM notification to the Push REST service in the Cisco cloud, which forwards the notification to the Apple cloud.  
                               | 2. The Apple cloud pushes the IM notification to the Jabber client and a notification appears on the Jabber client.  
                               | 3. When the user clicks the notification, the Jabber client moves back the foreground. The Jabber client resumes the session with the IM and Presence Service and downloads the instant message.  
                               | **Note** While the Cisco Jabber client is in suspended mode, the user's Presence status displays as **Away**. |

---

**Push Notifications Configuration**

PART III

Configure Features

• Configure Availability and Instant Messaging, on page 151
• Configure Chat Rooms, on page 155
• Configure High Availability for Persistent Chat, on page 163
• Configure Managed File Transfer, on page 173
• Configure Multiple Device Messaging, on page 189
• Configure Enterprise Groups, on page 193
• Configure Advanced Features, on page 203
Availability and Instant Messaging Overview

IM and Presence Service allows your users to share their availability status with their contacts.

Point-to-point instant messaging 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 instant message clients to exchange point-to-point instant messages.

Instant messaging capabilities include:

**Instant Message Forking**

When a user sends an instant message to a contact who is signed into multiple instant message clients, IM and Presence Service delivers the instant message to each client. IM and Presence Service continues to fork instant messages to each client, until the contact replies. Once the contact replies, IM and Presence Service only delivers instant messages to the client on which the contact replied.

**Offline Instant Messaging**

When a user sends an instant message to a contact who is not signed in (offline), IM and Presence Service stores the instant message and delivers it after the offline contact signs back in to their instant message client.

**Broadcast Instant Messaging**

Allows a user to send an instant message to multiple contacts at the same time, for example, when a user wants to send a notification to a large group of contacts.

Please note that not all instant message clients support broadcasting.

**Maximum Contact List Size**

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.

The System Troubleshooter in Cisco Unified CM IM and Presence Administration indicates if there are users who have reached the contact list limit.

### Availability and Instant Messaging Prerequisites

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

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

For SIP to XMPP instant messaging, 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

### Availability and Instant Messaging Task Flow

Perform the following tasks to configure availability and instant messaging on IM and Presence Service.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Configure Presence Sharing, on page 153</td>
<td>Use this procedure to configure the cluster-wide setting for Presence and IM availability sharing. Presence sharing allow your users to be able to view each other’s IM availability status.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Enable Instant Messaging, on page 154</td>
<td>Configure the system to allow users to exchange instant messages.</td>
</tr>
</tbody>
</table>
Configure Presence Sharing

Use this procedure to configure the cluster-wide setting for Presence and IM availability sharing. Presence sharing allow your users to be able to view each other's IM availability status.

---

When availability sharing is turned off:

- Users can view their own availability status in the client application, but the status for other users is greyed out.
- When users enter a chat room, their availability status displays as **Unknown**.

---

**Procedure**

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

**Step 2**  
To enable cluster-wide Presence sharing, check the **Enable availability sharing** check box.

**Note**  
Individual Cisco Jabber users can enable or disable this setting for their own Jabber client, by reconfiguring the policy settings within their Cisco Jabber client.

**Step 3**  
If you want users to be able to view the Presence of other users without requiring the other user's approval, check the **Allow user to view the availability of other users without being prompted for approval** check box. Otherwise, all Presence requests must be authorized by the other user.

**Note**  
Individual end users can override this setting by reconfiguring the policy settings within their Cisco Jabber client.

**Step 4**  
Configure maximum values for the **Maximum Contact List Size** and **Maximum Watchers (per user)** settings. If you don't want to use maximums, check the **No Limit** check box for each.

**Step 5**  
Optional. If you want Cisco Jabber users to be able to temporarily subscribe the Presence status of other users whom are not on their contact list, check the **Enable ad-hoc presence subscriptions** check box and configure the additional ad-hoc presence settings.

**Step 6**  
Complete any additional settings in the **Presence Settings** window. Refer to the online help for help with the fields and their settings.

**Step 7**  
Click **Save**.

**Step 8**  
Restart the **Cisco XCP Router** and **Cisco Presence Engine** services:

a) Log in to Cisco Unified IM and Presence Serviceability and choose **Tools > Control Center - Feature Services**

b) Select the **Cisco Presence Engine** service and click **Restart**.

c) Choose **Tools > Control Center - Network Services**.

d) Select the **Cisco XCP Router** service and click **Restart**.
Note: Depending on which fields you edited, you may not need to restart services. Refer to the online help for information on the fields that you edited.

What to do next
Enable Instant Messaging, on page 154

Enable Instant Messaging
Configure the system to allow users to exchange instant messages.

Before you begin
Configure Presence Sharing, on page 153

Procedure

Step 1 In Cisco Unified CM IM and Presence Administration, choose Messaging > Settings.
Step 2 Check the Enable instant messaging check box.
Step 3 Check the check box options that meet your deployment needs. For field descriptions, refer to the online help:
   - Suppress offline instant messaging
   - Allow clients to log instant message history (on supported clients only)
   - Allow cut & paste in instant messages
Step 4 Click Save.

Availability and Instant Messaging Interactions and Restrictions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Restriction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability Sharing</td>
<td>If you turn off this setting, users can view only their own availability status. Availability information is not shared to other users in the cluster. In addition, availability information received from outside the cluster is not shared either.</td>
</tr>
</tbody>
</table>
Configure Chat Rooms

- Group Chat Rooms Overview, on page 155
- Group Chat Prerequisites, on page 156
- Group Chat and Persistent Chat Task Flow, on page 156
- Group Chat and Persistent Chat Interactions and Restrictions, on page 160
- Persistent Chat Examples (without HA), on page 161

Group Chat Rooms Overview

Group chat is an instant messaging session between more than two users. IM and Presence Service supports group chat in either ad hoc chat rooms or persistent chat rooms. Support for ad hoc chat rooms is enabled by default once you enable instant messaging, but you must configure the system to support persistent chat rooms.

Ad Hoc Chat Rooms

Ad hoc chat rooms are group chat sessions that remain in existence only as long as one person is still connected to the chat room. Ad hoc chat rooms are deleted from the system when the last user leaves the room. Records of the instant message conversation are not maintained permanently. Once instant messaging is enabled, ad hoc chat rooms are enabled by default.

Ad hoc chat rooms are, by default, public rooms. A user can join:

- By being invited
- If they have not been invited, users can find the room through service discovery, or room search on a third-party XMPP client.

Persistent Chat Rooms

Persistent chat rooms are group chat sessions that remain in existence even after all users have left the room. Users are expected to return to the same room over time to continue the discussion.

Persistent chat rooms are created so that users can collaborate and share knowledge on 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.

You must configure the system for Persistent Chat Rooms. In addition, persistent chat requires that you deploy an external database.
Group Chat Prerequisites

Ad Hoc Chat Prerequisites

If you are deploying ad hoc chat rooms, make sure that instant messaging is enabled. For details, see Enable Instant Messaging, on page 154.

Persistent Chat Prerequisites

If you are deploying persistent chat rooms:

- Make sure that instant messaging is enabled. For details, see Enable Instant Messaging, on page 154.
- Decide whether you are going to deploy High Availability for Persistent Chat. This deployment type adds redundancy and failover to your persistent chat rooms. However, the external database requirements are slightly different than if you deploy the feature without High Availability.

Group Chat and Persistent Chat Task Flow

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Configure Group Chat System Administrators, on page 157</td>
<td>Add system administrators to manage the persistent chat system.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure Chat Room Settings, on page 157</td>
<td>Configure basic chat room settings. Optionally, enable Persistent Chat.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Restart the Cisco XCP Text Conference Manager, on page 158</td>
<td>If you are deploying Persistent Chat, make sure that the Cisco XCP Text Conference Manager service is running.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Set up External Database for Persistent Chat, on page 159</td>
<td>For Persistent Chat, you must configure a unique external database instance for each node. Note: If you are deploying High Availability for Persistent Chat, you can skip the remaining tasks in this chapter as the database requirements are slightly different when HA is deployed.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Add External Database Connection, on page 159</td>
<td>In the IM and Presence Service, set up a connection to your external database.</td>
</tr>
</tbody>
</table>
Configure Group Chat System Administrators

Add system administrators to manage the persistent chat system.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Messaging &gt; Group Chat System Administrators.</strong></td>
</tr>
</tbody>
</table>
| Step 2 | Check **Enable Group Chat System Administrators.**  
  Restart the Cisco XCP Router when the setting is enabled or disabled. Once the System Administrator setting is enabled, you can add system administrators dynamically. |
| Step 3 | Click **Add New.** |
| Step 4 | Enter an IM address. |
| Example | The IM address must be in the format of name@domain. |
| Step 5 | Enter a **Nickname** and **Description.** |
| Step 6 | Click **Save.** |

What to do next

Configure Chat Room Settings, on page 157

Configure Chat Room Settings

Configure basic chat room settings such as Room Member and Occupancy settings, and the maximum number of users per room.

Optionally, you can enable Persistent Chat by checking the **Enable Persistent Chat** check box.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From Cisco Unified CM IM and Presence Administration, choose <strong>Messaging &gt; Group Chat and Persistent Chat</strong></td>
</tr>
</tbody>
</table>
| Step 2 | Configure whether you want the system to manage chat node aliases by checking or unchecking the **System automatically manages primary group chat server aliases** check box.  
  • Checked—The system assigns chat node aliases automatically. This is the default value.  
  • Unchecked—Administrators can assign their own chat node aliases. |
| Step 3 | Check the **Enable Persistent Chat** check box if you want your chat rooms to remain in existence after all participants have left the room. |
Note This is a cluster-wide setting. If persistent chat is enabled on any node in the cluster, clients in any cluster will be able to discover the Text Conference instance on the node and chat rooms hosted on that node.

Users from a remote cluster can discover Text Conference instances and chat rooms in the local cluster even if Persistent Chat is not enabled for the remote cluster.

**Step 4** If you have chosen to enabled Persistent Chat, configure values for each to the following fields:

- Maximum number of persistent chat rooms allowed
- Number of connections to the database
- Database connection heartbeat interval (seconds)
- Timeout value for persistent chat rooms (minutes)

**Note** Do not set the Database Connection Heartbeat Interval value to zero without contacting Cisco support. The heartbeat interval is typically used to keep connections open through firewalls.

**Step 5** Under Room Settings, assign a maximum number of rooms.

**Step 6** Complete the remaining settings in the Group Chat and Persistent Chat Settings window. For help with the fields and their settings, refer to the online help.

**Step 7** Click Save.

---

**What to do next**

Restart the Cisco XCP Text Conference Manager, on page 158

---

**Restart the Cisco XCP Text Conference Manager**

If you have edited your chat settings or added one or more aliases to a chat node, restart the Cisco XCP Text Conference Manager service.

**Procedure**

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

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

**Step 3** In the IM and Presence Service section, click the Cisco XCP Text Conference Manager radio button and click Start or Restart.

**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.

---

**What to do next**

If you are deploying High Availability for Persistent Chat, go to Configure High Availability for Persistent Chat, on page 163.

Otherwise, Set up External Database for Persistent Chat, on page 159.
Set up External Database for Persistent Chat

This topic covers Persistent Chat without High Availability. If you are deploying High Availability for Persistent Chat refer to that chapter instead for external database setup info.

If you are configuring persistent chat rooms, you must set up a separate external database instance for each node that hosts persistent chat rooms. In addition:

- 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 you use an external database for persistent chat logging, make sure that your database is large enough to handle the volume of information. Archiving all the messages in a chat room is optional, but will increase traffic on the node and consume disk space.

- Before you configure the number of connections to the external database, consider the number of IMs you are writing and the overall volume of traffic that results. The number of connections that you configure will allow the system to scale. While the system defaults suit most installations, you may want to adapt the parameters for your specific deployment.


**What to do next**

Add External Database Connection, on page 159

Add External Database Connection

Configure a connection to the Persistent Chat external database from the IM and Presence Service. A minimum of one unique logical external database instance (tablespace) is required for the entire IM and Presence Service intercluster.

**Procedure**

1. From Cisco Unified CM IM and Presence Administration, choose **Messaging > External Servers Setup > External Databases**.
2. Click **Add New**.
3. In the **Database Name** field, enter the name of external database instance.
4. From the **Database Type** drop-down, select the type of external database that you are deploying.
5. Enter the **User Name** and **Password information** for the database.
6. In the **Hostname** field, enter the hostname or IP address of the database.
7. Complete the remaining settings in the **External Database Settings** window. For help with the fields and their settings, refer to the online help.
8. Click **Save**.
Step 9
Repeat this procedure to create connections to each external database instance.

## Group Chat and Persistent Chat Interactions and Restrictions

### Table 18: Group Chat and Persistent Chat Interactions and Restrictions

<table>
<thead>
<tr>
<th>Feature Interaction</th>
<th>Restriction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archiving room joins</td>
<td>Archiving room joins and leaves is optional because it will increase traffic and consume space on the external database server.</td>
</tr>
<tr>
<td>Chat with anonymous rooms</td>
<td>If you are deploying chat via Cisco Jabber (either group chat or persistent chat), make sure that the <strong>Rooms are anonymous by default</strong> and <strong>Room owners can change whether or not rooms are anonymous</strong> options are not selected in the <strong>Group Chat and Persistent Chat Settings</strong> window. If either check box is checked, chat will fail</td>
</tr>
<tr>
<td>Database Connection Issues</td>
<td>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.</td>
</tr>
<tr>
<td>OVA Requirements</td>
<td>If you are deploying Persistent Chat or Intercluster Peering, the minimum OVA size that you can deploy for these features is the 5000 user OVA. It’s recommended that you deploy at least the 15,000 user OVA. Centralized Deployments may require the 25,000 user OVA, depending on the size of the user base. For additional details on OVA options and user capacities, refer to the following site: <a href="https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html">https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html</a></td>
</tr>
<tr>
<td>Persistent chat character limit with Microsoft SQL Server</td>
<td>Chat messages where the message body (includes HTML tags + text message) exceeds 4000 characters are not delivered. These messages are rejected and are not archived. This issue exists when Microsoft SQL Server is used as the external database for releases 11.5(1)SU3 onward. See CSCvd89705 for additional detail.</td>
</tr>
</tbody>
</table>
Persistent Chat Examples (without HA)

The following two examples illustrate the Persistent Chat feature along with intercluster peering where High Availability for Persistent Chat is not deployed.

Note Cisco recommends that if you are deploying Persistent Chat, you should display High Availability for Persistent Chat in order to add redundancy to your persistent chat rooms.

Persistent Chat (without HA) Enabled on all Intercluster Nodes

Persistent Chat (without HA) is enabled on all nodes in an intercluster network. All nodes have an external database associated for Persistent Chat, thereby allowing all nodes to host persistent chat rooms.

The Cisco Text Conferencing service is running on all nodes in either cluster, allowing all users in either cluster to join persistent chat rooms that are hosted on any node in either cluster.
Persistent Chat (without HA) Enabled in one Cluster of Intercluster Network

Only nodes in Cluster 1 are configured for Persistent Chat (without HA) and have external databases. External databases are not required in Cluster 2 as the nodes are not configured to host persistent chat rooms.

However, the Cisco Text Conference Manager service is running on all nodes in either cluster, thereby allowing all users in either cluster to join the persistent chat rooms that are hosted in Cluster 1.
High Availability for Persistent Chat Overview

High Availability (HA) for Persistent Chat is an optional feature that you can deploy if you are using Persistent Chat rooms and you have system redundancy configured with Presence Redundancy Groups.

High Availability for Persistent Chat adds redundancy and failover capability to your persistent chat rooms. In the event of an IM and Presence Service node failure or Text Conferencing (TC) service failure, all persistent chat rooms hosted by that service are automatically hosted by the backup node or TC service. After failover, Cisco Jabber clients can seamlessly continue to use the persistent chat rooms.

External Database

The main difference between the Persistent Chat (non-HA) and Persistent Chat HA setup is around the external database requirements:

- If Persistent Chat is deployed without HA, the external database connects to an individual chat node only. Each node that hosts persistent chat rooms requires a separate external database instance. If a chat node fails, persistent chat rooms that were hosted on that node become unavailable until the chat node comes back up.

- If High Availability for Persistent Chat is deployed, the external database instance connects to both nodes in a subcluster (Presence Redundancy Group). If a persistent chat node fails, the backup node in the subcluster takes over, allowing chat to continue uninterrupted.

High Availability for Persistent Chat - Intercluster Example

The following illustration displays an intercluster network where Persistent Chat High Availability is deployed in Cluster 1 only. With Persistent Chat High Availability, each subcluster hosts an external database. Cluster 2 does not have Persistent Chat High Availability enabled, so there is no external database requirement. However, because the Cisco Text Conference Manager service is running on all nodes, users in Cluster 2 can join persistent chat rooms that are hosted in Cluster 1.
In this example, only the chat rooms in Cluster 1 are configured to host persistent chat rooms. You can also add persistent chat support on the Cluster 2 nodes, along with external database instances. In this case, all users in either cluster would be able to join persistent chat rooms that are hosted on any node in either cluster.

**Comparison of Persistent Chat (non-HA) and Persistent Chat HA Requirements**

If you are deploying Persistent Chat Rooms, Cisco recommends that you deploy High Availability for Persistent Chat as well as this adds failover capability to your persistent chat rooms. However, it is not mandatory.

The following table discusses the differences between Persistent Chat deployed with and without High Availability.
Table 19: Comparison of Persistent Chat with and without High Availability

<table>
<thead>
<tr>
<th>Persistent Chat (without HA)</th>
<th>Persistent Chat HA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Database Requirements</strong></td>
<td><strong>Database Requirements</strong></td>
</tr>
<tr>
<td>You require a separate external database instance for each cluster node that hosts persistent chat rooms. These external database instances can be created on the same external database server.</td>
<td>You require a separate external database instance for each subcluster (Presence Redundancy Group) that hosts persistent chat rooms. These external database instances can be created on the same external database server.</td>
</tr>
<tr>
<td><strong>Recommended:</strong> For optimum performance and scalability, deploy a unique logical external database instance for each node or redundancy group an the IM and Presence cluster. However, this is not mandatory.</td>
<td><strong>Recommended:</strong> For optimum performance and scalability, deploy a separate external database instance for each subcluster within an IM and Presence cluster. However, this is not mandatory.</td>
</tr>
<tr>
<td><strong>Minimum Requirement:</strong> You must have at least one external database instance for Persistent Chat across an IM and Presence intercluster network. However, this deployment may be inadequate for high-use networks.</td>
<td><strong>Minimum Requirement:</strong> You require at least one external database instance for Persistent Chat HA across an IM and Presence intercluster network. However, this deployment may be inadequate for high-use networks.</td>
</tr>
<tr>
<td><strong>Supported Database Types</strong></td>
<td><strong>Supported Database Types</strong></td>
</tr>
<tr>
<td>• PostgreSQL</td>
<td>• PostgreSQL</td>
</tr>
<tr>
<td>• Oracle</td>
<td>• Oracle</td>
</tr>
<tr>
<td>• Microsoft SQL Server</td>
<td>• Microsoft SQL Server (as of 11.5(1)SU2)</td>
</tr>
</tbody>
</table>

**Behavior when persistent chat node fails**

Persistent chat rooms hosted on the failed node are inaccessible until the node comes back up.

Users homed on the failed node fail over to the backup node in the subcluster, provided cluster redundancy is configured. However, they cannot access persistent chat rooms from the failed node.

Persistent chat rooms failover to the backup node in the subcluster. Users can continue messaging with no interruption of services.

Any users homed on the failed node also fail over.

High Availability for Persistent Chat Prerequisites

Before you configure High Availability for Persistent Chat, make sure that:

- Persistent Chat rooms are enabled. For details, see Configure Chat Room Settings, on page 157.
- High availability is enabled in each Presence Redundancy Groups. For details, see Presence Redundancy Group Task Flow, on page 44.
• You have configured the external database. For database setup and support information, see the *Database Setup Guide for the IM and Presence Service*.

### High Availability for Persistent Chat Task Flow

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Set up External Database, on page 166</td>
<td>You require a separate external database instance for each subcluster where persistent chat rooms are hosted. These separate external database instances can be hosted on the same database server.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Add External Database Connection, on page 167</td>
<td>Configure a connection to the external database from the IM and Presence Service.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Verify High Availability for Persistent Chat Settings, on page 167</td>
<td>Confirm your system settings for Persistent Chat High Availability.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Start Cisco XCP Text Conference Manager Service, on page 168</td>
<td>If the Cisco XCP Text Conference Manager service was stopped on any nodes, use this procedure to start it.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Merge External Databases, on page 168</td>
<td>Optional. If you are upgrading from an earlier release where you had Persistent Chat configured with multiple external databases, use this procedure to merge your external databases into a single database.</td>
</tr>
</tbody>
</table>

### Set up External Database

To deploy High Availability for Persistent Chat, you require a separate external database instance for each subcluster where persistent chat rooms are hosted. These separate external database instances can be hosted on the same database server.

A subcluster is a redundant pair of IM and Presence nodes (Presence Redudancy Group). You can have a maximum of three subclusters in an IM and Presence cluster of 6 nodes. If HA for Persistent Chat is enabled in an IM and Presence cluster of 6 nodes, you will have three external database instances and three subcluster pairs.

You can use PostgreSQL, Oracle, or Microsoft SQL Server for the external database connection. For setup details, refer to the *Database Setup Guide for IM and Presence Service*.

**What to do next**

Add External Database Connection, on page 167
Add External Database Connection

Configure connections to the High Availability for Persistent Chat external database instances from the IM and Presence Service. Make sure that both nodes in the subcluster are assigned to the same unique logical external database instance.

Procedure

Step 1  From Cisco Unified CM IM and Presence Administration, choose Messaging > External Servers Setup > External Databases.
Step 2  Click Add New.
Step 3  In the Database Name field, enter the name of external database instance.
Step 4  From the Database Type drop-down, select the type of external database that you are deploying.
Step 5  Enter the User Name and Password information for the database.
Step 6  In the Hostname field, enter the hostname or IP address of the database.
Step 7  Complete the remaining settings in the External Database Settings window. For help with the fields and their settings, refer to the online help.
Step 8  Click Save.
Step 9  Repeat this procedure to create connections to each external database instance.

What to do next

Verify High Availability for Persistent Chat Settings, on page 167

Verify High Availability for Persistent Chat Settings

Use this procedure to confirm that your system is set up for High Availability for Persistent Chat.

Note

If you've already enabled High Availability for your Presence Redundancy Groups (subclusters) and your chat room configuration includes Persistent Chat then your High Availability for Persistent Chat may be completed.

Procedure

Step 1  Confirm that High Availability is enabled in each subcluster:
  a)  From Cisco Unified CM Administration, choose System > Presence Redundancy Groups.
  b)  Click Find and choose the Presence Redundancy Group that you want to check.
  c)  Verify that the Enable High Availability check box is checked. If the check box is unchecked, then check it.
  d)  Click Save.
  e)  Repeat these steps for each presence redundancy group in the cluster.
Step 2 Confirm that persistent chat is enabled:
   a) From Cisco Unified CM Administration, choose Messaging > Group Chat and Persistent Chat.
   b) Confirm that the Enable Persistent Chat check box is checked. If the check box is unchecked, then check it.
   c) Click Save.

Step 3 From Cisco Unified CM Administration, confirm that the Cisco XCP Text Conference Manager Service is running on all cluster nodes.
   a) Choose System > Presence Topology.
   b) For each cluster node, click view to view the node details.
   c) Under Node Status, verify that the Cisco XCP Text Conference Manager service is STARTED.
   d) In the left navigation bar, click Presence Topology to return to the cluster topology and and repeat the above steps until you've confirmed the status for all cluster nodes.

What to do next
If the Cisco XCP Text Conference Manager Service service needs to be enabled, Start Cisco XCP Text Conference Manager Service, on page 168.

Start Cisco XCP Text Conference Manager Service
Use this procedure to start the Cisco XCP Text Conference Manager service. This service must be running on all cluster nodes for users on those nodes to be able to join persistent chat rooms.

Procedure

Step 1 In Cisco Unified IM and Presence Serviceability, choose Tools > Control Center - Feature Services.
Step 2 From the Server drop-down list, choose the IM and Presence cluster node and click Go.
Step 3 Under IM and Presence Services, select Cisco XCP Text Conference Manager and click Start.
Step 4 Click OK.
Step 5 (Optional) Click Refresh if you want to verify that the service has fully restarted.

Merge External Databases
Optional. If you have upgraded from a release prior to 11.5(1), and multiple external databases were used to manage redundancy, use the External Database Merge Tool to merge your external databases into a single database.

Example
If you have upgraded from a release prior to 11.5(1), and you had persistent chat configured with each persistent chat node connecting to a separate external database instance, use this procedure to merge the two databases in a subcluster into a single database that connects to both nodes.
Before you begin

- Ensure that the two source destination databases are assigned correctly to each IM and Presence Service node in the presence redundancy group. This verifies that both of their schemas are valid.
- Back up the tablespace of the destination database.
- Ensure that there is enough space in the destination database for the new merged databases.
- Ensure that the database users, created for the source and destination databases, have the permissions to run these commands:
  - CREATE TABLE
  - CREATE PUBLIC DATABASE LINK
- If your database users do not have these permissions, you can use these commands to grant them:
  - GRANT CREATE TABLE TO <user_name>;
  - GRANT CREATE PUBLIC DATABASE LINK TO <user_name>;
- If you are using a PostgreSQL external database, make sure that the following access is configured in the pg_hba.conf file:
  - The IM and Presence publisher node must have full access to each external database.
  - The external PostgreSQL database must have full access to each database instance. For example, if the external database is configured on 192.168.10.1 then each database instance must be configured in the pg_hba.conf file as host dbName username 192.168.10.0/24 password.

Procedure

**Step 1**  Sign in to Cisco Unified CM IM and Presence Administration on the IM and Presence Service publisher node.

**Step 2**  Stop the Cisco XCP Text Conference Service on the System > Services window for each IM and Presence Service node in the presence redundancy group.

**Step 3**  Click Messaging > External Server Setup > External Database Jobs.

**Step 4**  Click Find if you want to see the list of merge jobs. Choose Add Merge Job to add a new job.

**Step 5**  On the Merging External Databases window, enter the following details:
  - Choose Oracle or Postgres from the Database Type drop-down list.
  - Choose the IP address and hostname of the two source databases and the destination database that will contain the merged data.

  If you chose Oracle as the Database Type enter the tablespace name and database name. If you chose Postgres as the Database Type you provide the database name.

**Step 6**  In the Feature Tables pane, the Text Conference(TC) check-box is checked by default. For the current release, the other options are not available.

**Step 7**  Click Validate Selected Tables.
If the Cisco XCP Text Conference service has not been stopped you receive an error message. Once the service has been stopped, validation will complete.

**Step 8** If there are no errors in the Validation Details pane, click Merge Selected Tables.

**Step 9** When merging has completed successfully, the Find And List External Database Jobs window is loaded. Click Find to refresh the window and view the new job.

**Step 10** Restart the Cisco XCP Router service.

**Step 11** Start the Cisco XCP Text Conference Service on both IM and Presence Service nodes.

**Step 12** You must reassign the newly merged external database (destination database) to the presence redundancy group.

---

### High Availability for Persistent Chat Use Cases

The following flows demonstrate the high availability for persistent chat flows for failover and failback. This example covers an IM and Presence cluster with two nodes. An IM and Presence cluster can have a maximum of 6 nodes, which allows for three subclusters. If persistent chat rooms are hosted on all nodes, you require three separate external database instances.

**Note** For this enhancement the Text Conferencing (TC) service has been made a critical service. As a result, the TC high availability failover flow remains the same even if the failover has been caused by the failure of another critical service on the node, such as the Cisco XCP Router service.
High Availability for Persistent Chat Failover Use Case

For this example, there are four users on four IM and Presence Service nodes with two High Availability (HA) pairs or subclusters. The users are assigned as follows:

<table>
<thead>
<tr>
<th>Subcluster 1</th>
<th>Subcluster 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Andy is on Node 1A—Node 1A hosts the chat room</td>
<td></td>
</tr>
<tr>
<td>• Bob is on Node 1B</td>
<td>• Catherine is on Node 2A</td>
</tr>
<tr>
<td></td>
<td>• Deborah is on Node 2B</td>
</tr>
</tbody>
</table>

1. All four users are chatting in the same chat room, which is hosted on Node 1A.
2. The Text Conferencing (TC) service fails on Node 1A.
3. After 90 seconds, the Server Recovery Manager (SRM) determines the failure of the TC critical service and starts an automatic failover.

4. Node 1B takes over the users from 1A and transitions to the Failed Over with Critical Services not Running state, before transitioning to the HA state Running in Backup Mode.

5. In line with the HA Failover Model, Andy is signed out from node 1A automatically and is signed in to the backup Node 1B.

6. The other users are not affected, but continue to post messages to the chat room, which is now hosted on Node 1B.

7. Andy enters the persistent chat room, and continues to read or post messages to the room.

High Availability Persistent Chat Fallback Use Case

For this example there are four users on four IM and Presence Service nodes with two High Availability (HA) pairs or subclusters. The users are assigned as follows:

<table>
<thead>
<tr>
<th>Subcluster 1</th>
<th>Subcluster 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Andy is on Node 1A—Node 1A hosts the chat room</td>
<td></td>
</tr>
<tr>
<td>• Bob is on Node 1B</td>
<td>• Catherine is on Node 2A</td>
</tr>
<tr>
<td></td>
<td>• Deborah is on Node 2B</td>
</tr>
</tbody>
</table>

1. All four users are chatting in the same chat room, which is hosted on Node 1A.

2. The Text Conferencing (TC) service fails on Node 1A.

3. Node 1B takes over the users from 1A and transitions to the Failed Over with Critical Services not Running, before transitioning to the HA state Running in Backup Mode.

4. In line with the HA Failover model, Andy is signed out automatically and is signed in to the backup Node 1B.

5. Bob, Catherine and Deborah are unaffected, but continue to post messages to the chat room, which is now hosted on Node 1B.

6. The IM and Presence Service administrator starts a manual fallback.

7. Node 1A transitions to Taking Back and Node 1B transitions to Falling Back.

8. Andy is signed out of Node 1B. Bob, Catherine, and Deborah continue to use the persistent chat room, and once Fallback has occurred, the room is moved back to Node 1A.

9. Node 1B moves from the HA state Falling Back to Normal and unloads its peer node rooms.

10. Node 1A moves from the HA state Taking Back to Normal and it reloads the chat room.

11. Andy enters the persistent chat room, and continues to read or post messages to the room.
CHAPTER 18

Configure Managed File Transfer

• Managed File Transfer Overview, on page 173
• Managed File Transfer Prerequisites, on page 174
• Managed File Transfer Task Flow, on page 177
• Troubleshooting External File Server Public and Private Keys, on page 187
• Administering Managed File Transfer, on page 188

Managed File Transfer Overview

Managed File Transfer (MFT) allows an IM and Presence Service client, such as Cisco Jabber, to transfer files to other users, ad hoc group chat rooms, and persistent chat rooms. The files are stored in a repository on an external file server and the transaction is logged to an external database.

To deploy the Managed File Transfer feature, you must also deploy the following servers:

• External database—All file transfers get logged to the external database.

• External File Server—A copy of each transferred file gets saved to the repository on the external file server.

Note

This configuration is specific to file transfers and has no impact on the message archiver feature for regulatory compliance.

For use cases, see Managed File Transfer Call Flow, on page 174

For information on administering the feature on an ongoing basis, see Managed File Transfer Administration, on page 219
Managed File Transfer Call Flow

1. The sender uploads the file to the IM and Presence Service server via HTTP, and the server responds with a URI for the file.

2. The IM and Presence Service server sends the file to the file server repository for storage.

3. IM and Presence Service writes an entry to the external database log table to record the upload.

4. The sender sends an IM to the recipient. The IM includes the URI of the file.

5. The recipient sends an HTTP request to IM and Presence Service for the file. IM and Presence Service reads the file from the repository (6), records the download in the log table (7) and sends the file to the recipient.

The flow for transferring a file to a group chat or persistent chat room is similar, except the sender sends the IM to the chat room, and each chat room participant sends a separate request to download the file.

---

**Note**

When a file upload occurs, the managed file transfer service is selected from all managed file transfer services available in the enterprise for the given domain. The file upload is logged to the external database and external file server associated with the node where this managed file transfer service is running. When a user downloads this file, the same managed file transfer service handles the request and logs it to the same external database and the same external file server, regardless of where this second user is homed.

---

**Managed File Transfer Prerequisites**

- You must also deploy an external database and external file server.

- Ensure that all clients can resolve the full FQDN of the IM and Presence Service node to which they are assigned. This is needed in order for Managed File Transfer to work.
External Database Prerequisites

If you are also deploying persistent chat and/or message archiver, you can assign the same external database and file server for all features. Make sure when determining server capacity to consider the potential IM traffic, number of files transferred, and the file size.

Tip

Install and configure an external database. For details, including supported databases, see Database Setup Guide for the IM and Presence Service.

In addition follow these guidelines:

• You require one unique logical external database instance for each IM and Presence Service node in an IM and Presence Service cluster.

• The external database is supported on both virtualized and non-virtualized platforms.

• For a full list of the logged metadata, see the AFT_LOG Table in the "External Database Tools" chapter of the Database Setup for IM and Presence Service on Cisco Unified Communications Manager.

• If you are connecting to the external database using IPv6, check Configure IPv6 Task Flow, on page 28 for details on setting up IPv6.

External File Server Requirements

Follow these guidelines when setting up your external file server:

• Subject to file server capacity, each IM and Presence Service node requires its own unique Cisco XCP File Transfer Manager file server directory, however, nodes can share the same physical file server installation.

• The file server must support an ext4 file system, SSHv2, and SSH tools.

• The file server must support OpenSSH 4.9 or later.

• The network throughput between IM and Presence Service and the external file server must be greater than 60 megabytes per second.

You can use the show fileserver transferspeed CLI command after you enable managed file transfer to determine your file server transfer speed. Be aware that if you run this command while the system is busy, it may impact the value returned by the command. For more information about this command, see the Command Line Interface Guide for Cisco Unified Communications Solutions at this link.

Partition Recommendations for External File Servers

Cisco recommends that you create one or more separate partitions that are dedicated to file transfer storage so that other applications that run on the server do not write to it. All file storage directories should be created on these partitions.

Consider the following:

• If you create partitions, be sure to consider that the IM and Presence Service default file size setting (0) allows files up to 4GB to be transferred. This setting can be lowered when you set up managed file transfer.
• Consider the number of uploads per day and the average file size.
• Ensure that the partition has sufficient disk space to hold the expected volume of files.
• For example, 12000 users transfer 2 files per hour with an average file size of 100KB = 19.2GB per 8 hour day.

Directory Structure for External File Servers

When the first file transfer occurs, timestamped subdirectories are automatically created, as described in this example:

• We create the path /opt/mftFileStore/node_1/ on an IM and Presence Service node.
• The directory /files/ is autogenerated.
• The three /chat_type/ directories (im, persistent, groupchat) are autogenerated.
• The date directory /YYYYMMDD/ is autogenerated.
• The hour directory /HH/ is autogenerated. If more than 1,000 files are transferred within an hour, additional roll-over directories /HH.n/ are created.
• The file is saved with an autogenerated encoded resource name, hereafter referred to as file_name.

In this example, our complete path to a file is:
/opt/mftFileStore/node_1/files/chat_type/YYYYMMDD/HH/file_name

Using our example path:

• Files transferred during one-to-one IM on August 11th 2014 between 15.00 and 15.59 UTC are in the following directory: /opt/mftFileStore/node_1/files/im/20140811/15/file_name

Files transferred during persistent group chat on August 11th 2014 between 16.00 and 16.59 UTC are in the following directory:
/opt/mftFileStore/node_1/files/persistent/20140811/16/file_name

• The 1001st file transferred during ad hoc chat on August 11th 2014 between 16.00 and 16.59 UTC is in the following directory:
/opt/mftFileStore/node_1/files/groupchat/20140811/16.1/file_name

• If no file transfers occur inside of an hour, there are no directories created for that period.

Note
The traffic between IM and Presence Service and the file server is encrypted using SSHFS, but the file contents are written to the file server in unencrypted form.

User Authentication for the External File Server

IM and Presence Service authenticates itself and the file server using SSH keys:

• IM and Presence Service public key is stored on the file server.
• During connection, SSHFS validates the IM and Presence Service private key. This ensures that the content of all files is encrypted.
The file server public key is stored on IM and Presence Service. This allows the IM and Presence Service to ensure that it is connecting to the configured file server and minimizes man-in-the-middle attacks.

The node public key is invalidated if the node's assignment is removed. If the node is reassigned, a new node public key is automatically generated and the key must be reconfigured on the external file server.

**Managed File Transfer Task Flow**

Complete these tasks to set up the Managed File Transfer feature on IM and Presence Service, and to set up your external file server.

**Before you begin**

Set up both an external database and an external file server for Managed File Transfer. For requirements, see

- External Database Prerequisites, on page 175
- External File Server Requirements, on page 175


**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Add External Database Connection, on page 178</td>
<td>Configure a connection to the external database from the IM and Presence Service.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Set up an External File Server, on page 178</td>
<td>Before setting up users, directories, ownership, permissions and other tasks on the file server, set up the external file server.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Create User for the External File Server, on page 179</td>
<td>Set up a user for the external file server.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Set up Directory for External File Server, on page 180</td>
<td>Set up the top level directory structure for the external file server.</td>
</tr>
<tr>
<td><strong>Step 5</strong> Obtain Public Key for the External File Server, on page 181</td>
<td>Obtain the external file server's public key.</td>
</tr>
<tr>
<td><strong>Step 6</strong> Provision External File Server on IM and Presence Service, on page 182</td>
<td>Obtain the following information for the external file server:</td>
</tr>
<tr>
<td><strong>Step 7</strong> Verify Cisco XCP File Transfer Manager Activation, on page 184</td>
<td>The Cisco XCP File Transfer Manager service must be active on each node where Managed File Transfer is enabled.</td>
</tr>
</tbody>
</table>
### Add External Database Connection

Configure a connection to the external database from the IM and Presence Service. With Managed File Transfer, you require a unique logical external database instance for each IM and Presence Service cluster node.

#### Before you begin

Set up each external database. For details, see the *External Database Setup Guide for the IM and Presence Service* at:


#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 8</td>
<td>Enable Managed File Transfer, on page 185</td>
<td>Enable Managed File Transfer on IM and Presence Service.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Verify External Server Status, on page 186</td>
<td>Verify that there are no problems with the external database setup and with the external file server setup.</td>
</tr>
</tbody>
</table>

#### Set up an External File Server

Before setting up users, directories, ownership, permissions and other tasks on the file server, set up the external file server.

#### Before you begin

Review the design recommendations for the external file server. For details, see External File Server Requirements, on page 175.
Procedure

**Step 1**  Install a supported version of Linux.

**Step 2**  Verify the file server supports SSHv2 and OpenSSH 4.9 or later by entering one of the following commands as root:

```
# telnet localhost 22
```

Trying ::1...

Connected to localhost.

Escape character is '^]'.

**SSH-2.0-OpenSSH_5.3**

Or

```
# ssh -v localhost
```

```
OpenSSH_5.3p1, OpenSSL 1.0.0-fips 29 Mar 2010
debug1: Reading configuration data /root/.ssh/config ... 
...debug1: Local version string SSH-2.0-OpenSSH_5.3 
... 
```

**Step 3**  To allow private/public key authentication, make sure that you have the following fields in the `/etc/ssh/sshd_config` file, set to `yes`.

- RSAAuthentication yes
- PubkeyAuthentication yes

If these are commented out in the file, the setting can be left alone.

**Tip**  To enhance security, you can also disable password log in for the file transfer user (mftuser in our example). This forces logging in only by SSH public/private key authentication.

**Step 4**  Cisco recommends that you create one or more separate partitions that are dedicated to file transfer storage so that other applications that run on the server do not write to it. All file storage directories should be created on these partitions.

What to do next

Create User for the External File Server, on page 179

Create User for the External File Server

Set up a user for the external file server.

**Before you begin**

Set up an External File Server, on page 178
Procedure

Step 1  On the file server as root, create a user for the managed file transfer feature. This user owns the file storage directory structure (our example uses mftuser) and force creation of the home directory (~mftuser).

```bash
# useradd -m mftuser
# passwd mftuser
```

Step 2  Switch to the managed file transfer user.

```bash
# su mftuser
```

Step 3  Create a .ssh directory under the ~mftuser home directory that is used as a key store.

```bash
$ mkdir ~mftuser/.ssh/
```

Step 4  Create an authorized_keys file under the .ssh directory that is used to hold the public key text for each managed file transfer enabled node.

```bash
$ touch ~mftuser/.ssh/authorized_keys
```

Step 5  Set the correct permissions for passwordless SSH to function.

```bash
$ chmod 700 ~mftuser (directory)
$ chmod 700 ~/.ssh (directory)
$ chmod 700 ~/.ssh/authorized_keys (file)
```

Note  On some Linux systems these permissions may vary, depending on your SSH configuration.

What to do next

Set up Directory for External File Server, on page 180

**Set up Directory for External File Server**

Set up the top level directory structure for the external file server.

You can create any directory structure that you want, with any directory names. Be certain to create a directory for each managed file transfer-enabled node. Later, when you enable Managed File Transfer on IM and Presence Service, you must assign each directory to a node.

**Important**

You must create a directory for each node that has managed file transfer enabled.

**Note**

A file server partition/directory is mounted in the IM and Presence Service directory that is used to store files.
Before you begin
Create User for the External File Server, on page 179

Procedure

**Step 1**
Switch back to the root user.

`$ exit`

**Step 2**
Create a top-level directory structure (our example uses `/opt/mftFileStore/`) to hold directories for all of the IM and Presence Service nodes that have Managed File Transfer enabled.

`# mkdir -p /opt/mftFileStore/`

**Step 3**
Give `mftuser` sole ownership of the `/opt/mftFileStore/` directory.

`# chown mftuser:mftuser /opt/mftFileStore/`

**Step 4**
Give the `mftuser` sole permissions to the `mftFileStore` directory.

`# chmod 700 /opt/mftFileStore/`

**Step 5**
Switch to the `mftuser`.

`# su mftuser`

**Step 6**
Create a subdirectory under `/opt/mftFileStore/` for each managed file transfer enabled node. (Later, when you enable managed file transfer, you assign each directory to a node.)

`$ mkdir /opt/mftFileStore/{node_1,node_2,node_3}`

**Note**
- These directories and paths will be used in the External File Server Dictionary field that you configure when you provision the file server in Cisco Unified CM IM and Presence Administration.
- If you have multiple IM and Presence Service nodes writing to this file server, you must define a target directory for each node, as we did in our example for three nodes `{node_1,node_2,node_3}`.
- Within each node's directory, the transfer type subdirectories (`im`, `groupchat`, and `persistent`) are automatically created by IM and Presence Service, as are all subsequent directories.

What to do next
Obtain Public Key for the External File Server, on page 181

**Obtain Public Key for the External File Server**

Obtain the external file server's public key.
Before you begin

Set up Directory for External File Server, on page 180

Procedure

**Step 1**

To retrieve the file server's public key, enter:

```
$ ssh-keyscan -t rsa host
```

Where *host* is the hostname, FQDN, or IP address of the file server.

**Warning**

- To avoid a man-in-the-middle attack, where the file server public key is spoofed, you must verify that the public key value that is returned by the `ssh-keyscan -t rsa host` command is the real public key of the file server.
- On the file server go to the location of the `ssh_host_rsa_key.pub` file (in our system it is under `/etc/ssh/`) and confirm the contents of the public key file, minus the host (the host is absent in the `ssh_host_rsa_key.pub` file on the file server), matches the public key value returned by the command `ssh-keyscan -t rsa host`.

**Step 2**

Copy the result of the `ssh-keyscan -t rsa host` command, not what is in the `ssh_host_rsa_key.pub` file. Be certain to copy the entire key value, from the server hostname, FQDN, or IP address to the end.

**Note**

In most cases the server key begins with the hostname or FQDN, although it may begin with an IP address.

For example, copy:

```
hostname ssh-rsa AAAQEAzRevlQCH1KFAxwhd5UvEFzJs...
...a7y49d+/Am6+Zxklc4ux5xZXueL3GSt4rQu3rp/sdug+/+N9MQ==
```

(ellipses added).

**Step 3**

Save the result of the `ssh-keyscan -t rsa host` command to a text file. It is needed when you configure the file server during the **Deploy an External File Server on IM and Presence Service** procedure.

**Step 4**

Open the `authorized_keys` file you created and leave it open. You will need it later, when you provision the file server on the IM and Presence Service.

**Note**

If you are unable to retrieve the public key, see Troubleshooting External File Server Public and Private Keys, on page 187 for further help.

What to do next

Provision External File Server on IM and Presence Service, on page 182

---

**Provision External File Server on IM and Presence Service**

You must configure one external file server instance for each node in your cluster that will have Managed File Transfer enabled.
The external file server instances do not need to be physical instances of the external file server. However, be aware that for a given hostname, you must specify a unique external file server directory path for each external file server instance. You can configure all the external file server instances from the same node.

**Before you begin**

*Obtain Public Key for the External File Server, on page 181*

Obtain the following information for the external file server:

- Hostname, FQDN, or IP address
- Public key
- Path to the file storage directory
- User name

**Procedure**

**Step 1** In Cisco Unified CM IM and Presence Administration, choose Messaging > External Server Setup > External File Servers.

**Step 2** Click Add New.

The **External File Servers** window appears.

**Step 3** Enter the server details. For help with the fields and their configuration options, see **External File Servers Fields**, on page 183.

**Step 4** Click Save.

**Step 5** Repeat this procedure until you have created a separate external file server instance for each cluster node where managed file transfer is enabled.

**What to do next**

*Verify Cisco XCP File Transfer Manager Activation, on page 184*

**External File Servers Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the file server. Ideally the server name should be descriptive enough to be instantly recognized. Maximum characters: 128. Allowed values are alphanumeric, dash, and underscore.</td>
</tr>
<tr>
<td>Host/IP Address</td>
<td>Enter the hostname or IP address of the file server.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>• The value entered for the Host/IP Address field must match the beginning of the key that is entered for the External File Server Public Key field (follows).</td>
</tr>
<tr>
<td></td>
<td>• If you change this setting, you must restart the Cisco XCP Router service.</td>
</tr>
</tbody>
</table>
Verify Cisco XCP File Transfer Manager Activation

The Cisco XCP File Transfer Manager service must be active on each node where Managed File Transfer is enabled.

This service can only starts if an external database and an external file server have been assigned, and if the service can connect to the database and mount the file server.

**Before you begin**

Provision External File Server on IM and Presence Service, on page 182

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>On any node in the cluster, log in to the <strong>Cisco Unified IM and Presence Serviceability</strong> user interface.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Choose <strong>Tools &gt; Service Activation</strong>.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>From the <strong>Server</strong> drop-down, choose a node where Managed File Transfer is enabled, and click <strong>Go</strong>.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Confirm that the <strong>Cisco XCP File Transfer Manager</strong> service's <strong>Activation Status</strong> reads <strong>Activated</strong>.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>If the service is deactivated, check the <strong>Cisco XCP File Transfer Manager</strong> check box and click <strong>Save</strong>.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Repeat this procedure for all cluster nodes where Managed File Transfer is enabled.</td>
</tr>
</tbody>
</table>
What to do next
Enable Managed File Transfer, on page 185

Enable Managed File Transfer

Enable Managed File Transfer on IM and Presence Service.

Procedure

Step 1
Sign into Cisco Unified CM IM and Presence Administration, choose Messaging > File Transfer. The File Transfer window opens.

Step 2
In the File Transfer Configuration area, choose either Managed File Transfer or Managed and Peer-to-Peer File Transfer depending on your deployment. See File Transfer Options, on page 186.

Step 3
Enter the Maximum File Size. If you enter 0, the maximum size (4GB) applies.

Note You must restart the Cisco XCP Router service for this change to take effect.

Step 4
In the Managed File Transfer Assignment area, assign the external database and the external file server for each node in the cluster.

a) External Database — From the drop-down list, choose the name of the external database.

b) External File Server — From the drop-down list, choose the name of the external file server.

Step 5
Click Save.

After clicking Save a Node Public Key link, for each assignment, appears.

Step 6
For each node in the cluster that has managed file transfer enabled, you must copy the node's entire public key to the external file server's authorized_keys file.

a) To display a node's public key, scroll down to the Managed File Transfer Assignment area and click the Node Public Key link. Copy the entire contents of the dialog box including the node's IP address, hostname, or FQDN.

Example:

    ssh-rsa yc2EAAAABIAwAAAQEAp2g+S2XDEzptN11S5h5nwV1eKBnfG2pdW6KiLfwz/saFLegioIIqA8jBguNY/... ...S+ttuBBucKcH5gFxwesFSO0AfFwvnnq1xmMmIS9W2rf0Qp+aG4MVpTkHg3onw== imp@imp_node (ellipses added).

    Warning • If the managed file transfer feature is configured and the File Transfer Type is changed to either Disabled or Peer-to-Peer, all managed file transfer settings are deleted.

    • A node’s keys are invalidated if the node is unassigned from the external database and file server.

    b) On the external file server, if it was not left open, open the ~mftuser/.ssh/authorized_keys file that you created under the mftuser's home directory and (on a new line) append each node's public key.

    Note The authorized_keys file must contain a public key for each managed file transfer enabled IM and Presence Service node that is assigned to the file server.
c) Save and close the `authorized_keys` file.

**Step 7**  
(Optional) Configure the managed file transfer service parameters to define the threshold at which an RTMT alarm is generated for the external file server disk space. See Set Service Parameter Thresholds, on page 222.

**Step 8**  
Restart the Cisco XCP Router service on all nodes where Managed File Transfer is enabled. See Restart Cisco XCP Router service.

---

**What to do next**

Verify External Server Status, on page 186

---

## File Transfer Options

You can configure one of the following file transfer options on the File Transfer window:

<table>
<thead>
<tr>
<th>File Transfer Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>File transfer is disabled for the cluster.</td>
</tr>
<tr>
<td>Peer-to-Peer</td>
<td>One-to-one file transfers are allowed, but files are not archived or stored on a server. Group chat file transfer is not supported.</td>
</tr>
<tr>
<td>Managed File Transfer</td>
<td>One-to-one and group file transfers are allowed. File transfers are logged to a database and the transferred files are stored on a server. The client must also support managed file transfer, otherwise no file transfers are allowed.</td>
</tr>
<tr>
<td>Managed and Peer-to-Peer File Transfer</td>
<td>One-to-one and group file transfers are allowed. File transfers are logged to a database and the transferred files are stored on a server only if the client supports managed file transfer. If the client does not support managed file transfer, this option is equivalent to the Peer-to-Peer option.</td>
</tr>
</tbody>
</table>

---

**Note**

If managed file transfer is configured on a node and you change the File Transfer Type to **Disabled** or **Peer-to-Peer**, be aware that the mapped settings to the external database and to the external file server for that node are deleted. The database and file server remain configured but you must reassign them if you re-enable managed file transfer for the node.

Depending on your pre-upgrade setting, after an upgrade to IM and Presence Service Release 10.5(2) or later, either **Disabled** or **Peer-to-Peer** is selected.

---

## Verify External Server Status

Verify that there are no problems with the external database setup and with the external file server setup.
Before you begin
Enable Managed File Transfer, on page 185

Procedure

Step 1 To verify the status of the external database:
   a) In Cisco Unified CM IM and Presence Administration, choose Messaging > External Server Setup > 
      External Databases. 
   b) Check the information provided in the External Database Status area.

Step 2 On the IM and Presence Service node where you need to verify that the external file server is assigned:
   a) In Cisco Unified CM IM and Presence Administration, choose Messaging > External Server Setup > 
      External File Servers. 
   b) Check the information provided in the External File Server Status area to verify that the connection is 
      trouble free.

Troubleshooting External File Server Public and Private Keys

When a server private/public key pair is generated the private key is usually written to
/ect/ssh/ssh_host_rsa_key
The public key is written to /ect/ssh/ssh_host_rsa_key.pub
If these files do not exist, complete the following procedure:

Procedure

Step 1 Enter the following command:
   $ ssh-keygen -t rsa -b 2048

Step 2 Copy the file server's public key.
   You must copy the entire string of text for the public key from the hostname, FQDN, or the IP address (for 
   example, hostname ssh-rsa AAAAB3NzaC1yc...). In most Linux deployments the key contains the server's 
   hostname or FQDN.
   Tip If the output from the $ ssh-keygen -t rsa -b 2048 command doesn't contain a hostname, then 
   use the output from the following command instead: $ ssh-keyscan hostname

Step 3 For each IM and Presence Service node that is configured to use this file server, paste the public key into the 
   External File Server Public Key field on the External File Server Configuration window.
   Important Passwordless SSH must be configured for the managed file transfer feature. See the SSHD man 
   page for full configuration instructions for passwordless SSH.
While checking the status from the publisher node to the subscriber node, and vice versa the information message "The diagnostics tests for this External File Server may be run from here," is displayed.

In the logs we see "pingable": ":-7", which means we are viewing the status of other node where the external file server is not configured.

We configure external file server on the publisher node and the publisher nodes public key is shared in the external file server's "Authorized_key" file.

---

**Administering Managed File Transfer**

After you configure Managed File Transfer, you will need to administer the feature on an ongoing basis. For example, you will need to put a system in place for managing file server and database growth. For information on ongoing administration for this feature, see *Managed File Transfer Administration Overview, on page 219.*
Configure Multiple Device Messaging

- Multiple Device Messaging Overview, on page 189
- Multiple Device Messaging Prerequisites, on page 189
- Configure Multiple Device Messaging, on page 189
- Multiple Device Messaging Flow Use Case, on page 190
- Multiple Device Messaging Quiet Mode Use Case, on page 191
- Multiple Device Messaging Interactions and Restrictions, on page 191
- Counters for Multiple Device Messaging, on page 192

Multiple Device Messaging Overview

With Multiple Device Messaging (MDM), you can have one-to-one instant message (IM) conversations tracked across all devices on which you are currently signed in. If you are using a desktop client and a mobile device, both of which are MDM-enabled, messages are sent, or carbon copied, to both devices. Read notifications are also synchronized on both devices as you participate in a conversation.

MDM lets you maintain an IM conversation while moving between any of your devices. For example, if you start an IM conversation on your desktop computer, but you have to leave your desk for a meeting, you can you can continue the IM conversation on your mobile device. Clients must be signed-in to be MDM-enabled. Signed-out clients do not display sent or received IMs or notifications.

MDM supports quiet mode, which helps to conserve battery power on your mobile devices. The Jabber client turns quiet mode on automatically when the mobile client is not being used. Quiet mode is turned off when the client becomes active again.

Multiple Device Messaging Prerequisites

Instant messaging must be enabled. For details, see Group Chat and Persistent Chat Task Flow, on page 156

Configure Multiple Device Messaging

Multiple Device Messaging is enabled by default. You can use this procedure to disable the feature, or to turn it back on after it has been disabled.
Procedure

Step 1  In Cisco Unified CM IM and Presence Administration, choose System > Service Parameters.

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

Step 3  From the Service drop-down list, choose Cisco XCP Router (Active).

Step 4  From the Enable Multi-Device Messaging drop-down list, select either Enabled (the default value) or Disabled.

Step 5  Click Save.

Step 6  Restart the Cisco XCP Router service:
   a) Log in to Cisco Unified IM and Presence Serviceability and choose Tools > Control Center - Network Services.
   b) From the Server drop-down list box, select the IM and Presence publisher node.
   c) Under IM and Presence Services, select Cisco XCP Router and click Restart.

Multiple Device Messaging Flow Use Case

This flow describes how messages and notifications are handled when a user, Alice, has MDM enabled on her laptop and mobile device.

1. Alice has a Jabber client open on her laptop, and is also using Jabber on her mobile device.

2. Alice receives an instant message (IM) from Bob.
   Her laptop receives a notification and displays a new message indicator. Her mobile device receives a new message with no notification.

Note

IMs are always sent to all MDM-enabled clients. Notifications are displayed either on the active Jabber client only or, if no Jabber client is active, notifications are sent to all Jabber clients.

3. Alice chats with Bob for 20 minutes.
   Alice uses her laptop as normal to do this, while on her mobile device new messages are received and are marked as read. No notifications are sent to her mobile device.

4. When Alice receives three chat messages from a third user, Colin, Alice's devices behave as they did in step 2.

5. Alice does not respond, and closes the lid on her laptop. While on the bus home Alice receives another message from Bob.
   In this case, both her laptop and mobile device receive a new message with notifications.

6. Alice opens her mobile device, where she finds the new messages sent from Bob and Colin. These messages have also been sent to her laptop.

7. Alice reads through her messages on her mobile device, and as she does so, messages are marked as read on both her laptop and on her mobile device.
Multiple Device Messaging Quiet Mode Use Case

This flow describes the steps Multiple Device Messaging uses to enable quiet mode on a mobile device.

1. Alice is using Jabber on her laptop and also on her mobile device. She reads a message from Bob and sends a response message using Jabber on her laptop.

2. Alice starts using another application on her mobile device. Jabber on her mobile device continues working in the background.

3. Because Jabber on her mobile device is now running in the background, quiet mode is automatically enabled.

4. Bob sends another message to Alice. Because Alice's Jabber on her mobile device in quiet mode, messages are not delivered. Bob's response message to Alice is buffered.

5. Message buffering continues until one of these triggering events occur:
   - An \(<iq>\) stanza is received.
   - A \(<message>\) stanza is received when Alice has no other active clients currently operating on any other device.

   Note: An active client is the last client that sent either an Available presence status or an instant message in the previous five minutes.

   - The buffering limit is reached.

6. When Alice returns to Jabber on her mobile device, it becomes active again. Bob's message, which had been buffered is delivered, and Alice is able to view it.

Multiple Device Messaging Interactions and Restrictions

The following table summarizes feature interactions and restrictions with the Multiple Device Messaging (MDM) feature.

Table 20: Multiple Device Messaging Interactions and Restrictions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Interaction or Restriction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Jabber Clients</td>
<td>MDM is supported by all Jabber clients from version 11.7 and higher.</td>
</tr>
<tr>
<td>Group Chat</td>
<td>Group chat is only available on the device which joined the chat room.</td>
</tr>
<tr>
<td>Message Archiver</td>
<td>MDM is compatible with the Message Archiver feature.</td>
</tr>
<tr>
<td>Managed File Transfer</td>
<td>File transfer is only available on the active device.</td>
</tr>
<tr>
<td>Feature</td>
<td>Interaction or Restriction</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MRA via Expressway</td>
<td>For MRA clients that connect to IM and Presence Service via Cisco Expressway, you must be running at least Expressway X8.8 minimum to use MDM.</td>
</tr>
<tr>
<td>Server Recovery Manager</td>
<td>The Multiple Device Messaging feature causes a delay with server recovery on the IM and Presence Service if failover occurs. If server failover occurs on a system where Multiple Device Messaging is configured, the failover times generally are twice as long as the times specified with the Cisco Server Recovery Manager service parameters.</td>
</tr>
<tr>
<td>Third-Party Clients</td>
<td>MDM is compatible with third-party clients that do not support the feature.</td>
</tr>
</tbody>
</table>

## Counters for Multiple Device Messaging

Multiple Device Messaging (MDM) uses the following counters from the Cisco XCP MDM Counters Group:

<table>
<thead>
<tr>
<th>Counter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDMSessions</td>
<td>The current number of MDM enabled sessions.</td>
</tr>
<tr>
<td>MDMSilentModeSessions</td>
<td>The current number of sessions in silent mode.</td>
</tr>
<tr>
<td>MDMQuietModeSessions</td>
<td>The current number of sessions in quiet mode.</td>
</tr>
<tr>
<td>MDMBufferFlushes</td>
<td>The total number of MDM buffer flushes.</td>
</tr>
<tr>
<td>MDMBufferFlushesLimitReached</td>
<td>The total number of MDM buffer flushes due to reaching the overall buffer size limit.</td>
</tr>
<tr>
<td>MDMBufferFlushPacketCount</td>
<td>The number of packets flushed in the last timeslice.</td>
</tr>
<tr>
<td>MDMBufferAvgQueuedTime</td>
<td>The average time in seconds before the MDM buffer is flushed.</td>
</tr>
</tbody>
</table>
Configure Enterprise Groups

- Enterprise Groups Overview, on page 193
- Enterprise Groups Deployment Models, on page 194
- Enterprise Groups Prerequisites, on page 196
- Enterprise Groups Configuration Task Flow, on page 196
- Enterprise Groups Limitations, on page 201

Enterprise Groups Overview

Cisco Jabber users can search for enterprise groups and security groups in Microsoft Active Directory and add them to their contact lists. If a group that is already added to the contact list is updated, the contact list is automatically updated. Cisco Unified Communications Manager synchronizes its database with Microsoft Active Directory groups at specified intervals. The interval at which Cisco Unified Communications Manager synchronizes the groups is determined by LDAP Directory Synchronization Schedule parameters in the LDAP Directory Configuration window.

Currently, the Enterprise Groups feature is supported only on the Microsoft Active Directory server. It is not supported on Active Directory Lightweight Directory Services (AD LDS) and other corporate directories.

If a Cisco Jabber user wants to add a group to the contact list while the Enterprise Groups feature is enabled, the Cisco Jabber client sends a group request to the IM and Presence Service node. The IM and Presence Service node provides the following information for each group member:

- Display Name
- User ID
- Title
- Phone number
- Mail ID

Note

Only the group members that are assigned to the IM and Presence Service nodes can be added to the contact list. Other group members are discarded.
If you disable the Enterprise Groups feature, Cisco Jabber users cannot search Microsoft Active Directory groups or see the groups that they already added to their contact lists. If a user is already logged in when you disable the Enterprise Groups feature, the group will be visible until the user logs out. When the user logs in again, the group will not be visible.

**Maximum Allowed Entries**

The maximum number of entries that are allowed in a contact list is the sum of the number of entries in the contact list and the number of entries in groups that are already added to the contact list.

Maximum entries in contact list = (number of entries in contact list) + (number of entries in groups)

When the Enterprise Groups feature is enabled, Cisco Jabber users can add the groups to the contact list if the number of entries in the contact list is less than the maximum allowed entries. If the maximum allowed entries is exceeded while the feature is disabled, the users are not restricted until the feature is enabled. If the user continues to be logged in after the feature is enabled, no error message is displayed. When the user logs out and logs in again, an error message is displayed that asks the users to clear the excess entries.

**Security Groups**

In addition to enterprise groups, Cisco Jabber users can also search for, and add, security groups to their contact list. To set up this feature, administrators must configure a customized LDAP filter and apply it to the configured LDAP directory sync.

**Related Topics**

View User Groups

---

**Enterprise Groups Deployment Models**

The Enterprise Groups feature offers two deployment options for Active Directory.

---

**Important**

Ensure that Cluster 1 and Cluster 2 have a unique set of UserGroup, UserGroupMember, and UserGroupWatcherList records before synchronizing data through the Cisco Intercluster Sync Agent service. If both the clusters have unique sets of records, both the clusters will have a super set of all the records after synchronization.

**Enterprise Groups Deployment Model 1**

In this deployment model, Cluster 1 and Cluster 2 synchronize different subsets of users and groups from Microsoft Active Directory. The Cisco Intercluster Sync Agent service replicates the data from Cluster 2 into Cluster 1 to build the complete database of users and groups.
Enterprise Groups Deployment Model 1

In this deployment model, Cluster 1 synchronizes all the users and groups from Microsoft Active Directory. Cluster 2 synchronizes only users from Microsoft Active Directory. The Cisco Intercluster Sync Agent service replicates group information from Cluster 1 into Cluster 2.

Caution

If you are using this deployment model, ensure that you synchronize the groups data in only one cluster. The Enterprise Groups feature will not work as expected if you fail to do so.

You can verify your configuration on the Cisco Unified CM IM and Presence Administration > Presence > Inter-Clustering window.

Check the status of the Enterprise Groups LDAP Configuration parameter in the Inter-cluster peer table. No conflict found means there are no misconfigurations between peers. If there are conflicts found, click the Enterprise GroupConflicts link, and click the details button which appears. This opens a Reporting window for a detailed report.
Enterprise Groups Prerequisites

This feature assumes that you already have an LDAP Directory sync schedule configured with the below conditions. For details on how to configure an LDAP Directory sync, see the "Import Users from LDAP Directory" chapter of the System Configuration Guide for Cisco Unified Communications Manager.

- The Cisco DirSync service must be activated
- The LDAP Directory sync must include both users and groups
- Regular LDAP Directory syncs, as configured with the LDAP Directory Synchronization Schedule must be scheduled.

Supported LDAP Directories

Only Microsoft Active Directory is supported with enterprise groups.

Enterprise Groups Configuration Task Flow

Complete these tasks to configure the Enterprise Groups feature.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 <strong>Enable Enterprise Groups</strong>, on page 197</td>
<td>Complete this task to enable Cisco Jabber users to search for enterprise groups in Microsoft Active Directory and add them to their contact lists.</td>
</tr>
</tbody>
</table>
### Start Directory Sync Service

Before you can sync Enterprise Groups, the Cisco DirSync service must be running.

**Procedure**

1. Log in to Cisco Unified Serviceability and choose **Tools > Service Activation**.
2. Under **Directory Services**, check the **Cisco DirSync** check box.
3. Click **Save**.

**What to do next**

[Enable Enterprise Groups, on page 197](#)

### Enable Enterprise Groups

The enterprise parameter **Directory Group Operations on Cisco IM and Presence** in the **Enterprise Parameter Configuration** window allows you to enable or disable the Enterprise Groups feature. Follow these steps to enable the Enterprise Groups feature.

**Before you begin**

The Cisco DirSync feature service must be running.

**Procedure**

1. From Cisco Unified CM Administration, choose **System > Enterprise Parameters**. The **Enterprise Parameters Configuration** window appears.
2. In the **User Management Parameters** section, from the **Directory Group Operations on Cisco IM and Presence** drop-down list, select **Enabled**.
3. (Optional) From the **Syncing Mode for Enterprise Groups** drop-down list, choose one of the following:
   - **None**—If you choose this option, the Cisco Intercluster Sync Agent service does not synchronize the enterprise groups and the group membership records between IM and Presence Service clusters.
**Enable Security Groups**

If you want to allow Cisco Jabber users to be able to add a security group to their contact list, complete these optional tasks to include security groups in an LDAP Directory sync.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create Security Group Filter, on page 199</td>
<td>Create an LDAP filter that filters both directory groups and security groups.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure Cisco Jabber for Security Groups, on page 200</td>
<td>Update existing service profiles to give Cisco Jabber users whom are associated to that service profile access to search and add security groups.</td>
</tr>
</tbody>
</table>
Create Security Group Filter

Create an LDAP filter that filters security groups.

Procedure

Step 1  In Cisco Unified CM Administration, choose System > LDAP > LDAP Filter.
Step 2  Click Add New.
Step 3  Enter a unique Filter Name. For example, syncSecurityGroups.
Step 4  Enter the following Filter: (&(objectClass=group)(CN=*)).
Step 5  Click Save.

What to do next

Synchronize Security Groups from LDAP Directory, on page 199

Synchronize Security Groups from LDAP Directory

Add your Security Group filter to an LDAP Directory sync and complete a sync.

Note

You cannot add new configurations into an existing LDAP Directory configuration in Cisco Unified Communications Manager if the initial LDAP sync has already occurred.

Note

For detailed information on how to set up a new LDAP Directory sync, see the "Configure End Users" part of the System Configuration Guide for Cisco Unified Communications Manager.

Before you begin

Create Security Group Filter, on page 199

Procedure

Step 1  In Cisco Unified CM Administration, choose System > LDAP > LDAP Directory.
Step 2  Do one of the following:
   • Click Add New to create a new LDAP Directory.
   • Click Find and select the LDAP Directory from which the security groups will be synchronized.
Step 3  From the LDAP Custom Filter for Groups drop-down list box, select the security group filter that you created.
Step 4  Click Save.
Configure Cisco Jabber for Security Groups

Update existing service profiles to allow Cisco Jabber users whom are associated to that service profile to add security groups from an LDAP directory to their contact lists.

**Note**

For information on how to set up new service profiles and assign them to Cisco Jabber users, see the "Configure Service Profiles" chapter of the *System Configuration Guide for Cisco Unified Communications Manager*.

**Before you begin**

*Synchronize Security Groups from LDAP Directory, on page 199*

**Procedure**

**Step 1**
Complete any remaining fields in the **Service Profile Configuration** window. For help with the fields and their settings, refer to the online help.

**Step 2**
Click **Find** and select the service profile that your Jabber users use.

**Step 3**
Under **Directory Profile**, check the **Allow Jabber to Search and Add Security Groups** check box.

**Step 4**
Click **Save**. Cisco Jabber users who are associated to this service profile can now search and add security groups.

**Step 5**
Repeat this procedure for all service profiles that your Cisco Jabber users use.

**View User Groups**

You can view the Active Directory user groups that are synchronized with the Cisco Unified Communications Manager database using the following steps.

**Procedure**

**Step 1**
From Cisco Unified CM Administration, choose **User Management > User Settings > User Group**. The **Find and List User Groups** window appears.

**Step 2**
Enter search criteria and click **Find**. A list of user groups that match the search criteria is displayed.
Step 3  
To view a list of users that belong to a user group, click on the required user group. The User Group Configuration window appears.

Step 4  
Enter search criteria and click Find. A list of users that match the search criteria is displayed.

If you click on a user in the list, the End User Configuration window appears.

What to do next  
(Optional) Enable Security Groups, on page 198

## Enterprise Groups Limitations

### Table 21: Enterprise Groups Limitations

<table>
<thead>
<tr>
<th>Limitation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intercluster peering with a 10.x cluster</td>
<td>Enterprise Groups is supported for releases 11.0(1) and higher. If the synced group includes group members from a 10.x intercluster peer, users on the higher cluster cannot view the presence of synced members from the 10.x cluster. This is due to database updates that were introduced in 11.0(1) for the Enterprise Groups sync. These updates are not a part of the 10.x releases. To guarantee that users homed on the higher cluster can view the presence of group members homed on the 10.x cluster, users on the higher cluster should manually add the 10.x users to their contact lists. There are no presence issues for manually added users.</td>
</tr>
<tr>
<td>Multilevel grouping</td>
<td>Multilevel grouping is not allowed for the group sync.</td>
</tr>
<tr>
<td>Group-only synchronization</td>
<td>When a user group and users are present in the same search base, group-only synchronization is not allowed. Instead, the user group as well as the users are synchronized.</td>
</tr>
<tr>
<td>Maximum number of user groups</td>
<td>You can synchronize a maximum of 15000 user groups from Microsoft Active Directory server to the Unified Communications Manager database. Each user group can contain from 1 to 200 users. You can configure the exact amount on the Cisco Unified CM IM and Presence Administration &gt; System &gt; Service Parameters window. The maximum number of user accounts in the database cannot exceed 160,000.</td>
</tr>
<tr>
<td>User group migration</td>
<td>If a user group is moved from one organization unit to another, you must perform a full sync on the original unit followed by a full sync on the new unit.</td>
</tr>
<tr>
<td>Local groups</td>
<td>Local groups are not supported. Only groups synchronized from Microsoft Active Directory are supported.</td>
</tr>
<tr>
<td>Limitation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Group members not assigned to IM and Presence Service nodes</td>
<td>Group members that are not assigned to IM and Presence Service nodes display in the contact list with the presence bubble greyed out. However, these members are considered when calculating a maximum numbers of users allowed in the contact list.</td>
</tr>
<tr>
<td>Migration from Microsoft Office Communication Server</td>
<td>During migration from Microsoft Office Communication Server, the Enterprise Groups feature is not supported until users are fully migrated to the IM and Presence Service node.</td>
</tr>
<tr>
<td>LDAP synchronization</td>
<td>If you change the synchronization option in the <strong>LDAP Directory Configuration window</strong> while the synchronization is in progress, the existing synchronization remains unaffected. For example, if you change the synchronization option from <strong>Users and Groups</strong> to <strong>Users Only</strong> when the synchronization is in progress, the users and groups synchronization still continues.</td>
</tr>
<tr>
<td>Group search functionality over the Edge</td>
<td>Group search functionality over the Edge is offered in this release, but has not been fully tested. As a result, full support for group searches over the Edge cannot be guaranteed. Full support is expected to be offered in a future release.</td>
</tr>
<tr>
<td>Cisco Intercluster Sync Agent service periodic synchronization</td>
<td>If a group name or a group member name is updated in the external LDAP directory, it gets updated on the Cisco Jabber contact list only after the periodic Cisco Intercluster Sync Agent service synchronization. Typically, the Cisco Intercluster Sync Agent service synchronization occurs every 30 minutes.</td>
</tr>
<tr>
<td>Synchronization of users and user groups through different synchronization agreements in LDAP configuration</td>
<td>If users and user groups are synchronized into the Cisco Unified Communications Manager database as part of the same synchronization agreement, the user and group association gets updated as expected in Cisco Unified Communications Manager database after synchronization. However, if a user and user group are synchronized as part of different synchronization agreements, the user and the group may not get associated in the database after the first synchronization. The user and group association in the database depends on the sequence in which the synchronization agreements are processed. If the users are synchronized ahead of the groups, then the groups may not be available in the database for association. In such cases, you must ensure that the synchronization agreement with groups is scheduled ahead of the synchronization agreement with the users. Otherwise, after the groups synchronize into the database, the users will get associated with the groups after the next manual or periodic sync.</td>
</tr>
</tbody>
</table>
CHAPTER 21

Configure Advanced Features

- Calendar Integration with Microsoft Outlook, on page 203
- Federation, on page 203
- Message Archiver, on page 204
- Remote Call Control, on page 204

Calendar Integration with Microsoft Outlook

This feature allows users to incorporate their calendar and meeting status from Microsoft Outlook into their Presence status on the IM and Presence Service server. If a user is in a meeting, that status will display as a part of the user’s Presence status. This feature can be configured by connecting the IM and Presence Service to an on-premises Microsoft Exchange server or to a hosted Office 365 server.


Federation

On IM and Presence Service, you can create federated networks from within any domain that IM and Presence Service manages. There are two main types of Federation deployments:

- Interdomain Federation—This integration enables users from within any domain that IM and Presence Service manages to exchange availability information and Instant Messaging (IM) with users in external domains. The external domain may be managed by a Microsoft, Google, IBM, or AOL server. IM and Presence Service can use a variety of protocols to communicate with the server in the external domain.

- Partitioned Intradomain Federation—With this integration, IM and Presence Service and the Microsoft server (for example, Microsoft Lync) host a common domain or set of domains. The integration allows IM and Presence Service client users and Microsoft Lync users within a single enterprise to exchange instant messaging and availability.

Message Archiver

Many industries require that instant messages adhere to the same regulatory compliance guidelines as for all other business records. To comply with these regulations, your system must log and archive all business records, and the archived records must be retrievable.

The IM and Presence Service supports instant messaging (IM) compliance by collecting data for the following IM activities in single cluster, intercluster, or federated network configurations:

- Point-to-point messages.
- Group chat - This includes ad-hoc, or temporary chat messages, and permanent chat messages.
- IM Compliance Components
- Sample Topologies and Message Flow for IM Compliance


Remote Call Control

Microsoft Remote Call Control (RCC) allows enterprise users to control their Cisco Unified IP Phone or Cisco IP Communicator Phone through Microsoft Lync, a third-party desktop instant-messaging (IM) application. When a user signs in to the Microsoft Lync client, the Lync server sends instructions, through the IM and Presence Service node, to the Cisco Unified Communications Manager to set up, tear down and maintain calling features based on a user's action at the Lync client.

PART IV

Administer the System

- Manage Chat, on page 207
- Managed File Transfer Administration, on page 219
- Manage End Users, on page 227
- Migrate Users, on page 239
- Manage Locales, on page 251
- Manage the Server, on page 257
- Backup the System, on page 263
- Restore the System, on page 273
- Bulk Administration of Contact Lists, on page 289
- Troubleshoot the System, on page 299
Manage Chat Overview

IM and Presence Service provides you with settings you can use to manage your chat rooms and to control who has access to them. This includes the ability to:

- Create new rooms, manage members and the configurations of the rooms they create.
- Control access to persistent chat rooms so that only members of that room have access.
- Assign Administrators to a chat room.
- Invite other users to a room.
- 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.

IM and Presence Service also lets you manage chat node aliases. Chat node aliases make it possible for your users to search for specific chat rooms on specific nodes, and to join those chat rooms.

In addition, the IM and Presence Service also stores transcripts and makes this chat room history available to room members, including members who have just joined the chat room. You can configure how much of the existing archive you want to make available to new and old members.

Chat Node Alias Overview

Each chat node in a system must have a unique alias. Chat node aliases are unique addresses 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. Chat node aliases form a part of the unique ID for each chat room that is created on that node. For example, the alias conference-3-mycup.cisco.com gets used to name the chat room roomjid@conference-3-mycup.cisco.com that is created on that node.

There are two modes for assigning chat node aliases:
• System-generated—The system automatically assigns a unique alias to each chat node. By default, the system auto-generates one alias per chat node by 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
  - clusterid is the configured enterprise parameter
  - domain is the configured domain

For example, the system might assign: conference-3-mycup.cisco.com

• Manual—You must disable system-generated aliases to be able to assign chat node aliases manually. With manually-assigned aliases, you have complete flexibility to name chat nodes using aliases that suit your specific requirements. For example, you might do this if the conference-x-clusterid.domain naming convention does not suit your deployment needs.

Assigning Multiple Aliases per Node

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 functionality applies to both system-generated aliases and aliases that are created manually.

Manage Chat Prerequisites

Ensure that you have persistent chat enabled. See Configure Chat Rooms, on page 155.

Manage Chat Task Flow

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Enable Chat Room Owners to Edit Chat Room Settings, on page 209</td>
<td>Configure whether you want to allow chat room owners to be able to edit chat room settings. Otherwise, only administrators will be able to edit chat room settings.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Allow Clients to Log Instant Message History, on page 210</td>
<td>Configure whether you want to allow users to log instant message history locally on their computer.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Edit chat room settings. Complete any of the following tasks, in any order, to update chat room settings:</td>
<td>Note If you update any of the Persistent Chat settings, on Cisco Unified IM and Presence Serviceability, choose Tools &gt; Control Center - Feature Services to restart the Cisco XCP Text Conference Manager service.</td>
</tr>
<tr>
<td></td>
<td>• Set Number of Chat Rooms, on page 210</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Configure Chat Room Member Settings, on page 210</td>
<td></td>
</tr>
</tbody>
</table>
Enable Chat Room Owners to Edit Chat Room Settings

Use this procedure if you want to allow chat room owners to be able to edit chat room settings.

Procedure

Step 1
In Cisco Unified CM IM and Presence Administration, choose Messaging > Group Chat and Persistent Chat.

Step 2
Configure a value for the Room owners can change whether or not rooms are for members only check box.

- Checked—Chat room owners have administrative ability to edit chat room settings.
- Unchecked—Only an administrator can edit chat room settings.

Step 3
Click Save.

Step 4
In Cisco Unified IM and Presence Serviceability, choose Tools > Control Center - Feature Services.

Step 5
Restart the Cisco XCP Text Conference Manager service.
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** In Cisco Unified CM IM and Presence Administration, choose 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.

Configure Chat Room Settings

**Set Number of Chat Rooms**

Use room settings to limit the number of rooms that users can create. Limiting the number of chat rooms helps the performance of the system and allows it to scale. Limiting the number of rooms also helps to mitigate any possible service-level attacks.

**Procedure**

**Step 1** In Cisco Unified CM IM and Presence Administration, choose Messaging > Group Chat and Persistent Chat.

**Step 2** To change the maximum number of chat rooms that are allowed, enter a value in the field for *Maximum number of rooms allowed*. The default is set to 5500.

**Step 3** Click Save.

Configure Chat Room Member Settings

Member settings allow control over the membership in chat rooms. Such a control is useful for users to mitigate service-level attacks that can be prevented by restricting membership. Configure the member settings as required.

**Procedure**

**Step 1** In Cisco Unified CM IM and Presence Administration, choose Messaging > Group Chat and Persistent Chat.
### Step 2
Configure the room member settings as described in Room Member Settings.

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

### Step 4
In **Cisco Unified IM and Presence Serviceability**, choose **Tools > Control Center - Feature Services**.

### Step 5
Restart the Cisco XCP Text Conference Manager service.

---

**Room Member Settings**

*Table 22:*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rooms are for members only by default</td>
<td>Check this check box if you want rooms to be created as members-only rooms by default. Members-only rooms are accessible only by users on an allowed list configured by the room owner or administrator. The check box is unchecked by default.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The allowed list contains the list of members who are allowed in the room. It is created by the owner or administrator of the members-only room.</td>
</tr>
<tr>
<td>Only moderators can invite people to members-only rooms</td>
<td>Check this check box if you want to configure the room so that only moderators are allowed to invite users to the room. If this check box is unchecked, members can invite other users to join the room. The check box is checked by default.</td>
</tr>
<tr>
<td>Room owners can change whether or not rooms are for members only</td>
<td>Check this check box if you want to configure the room so that room owners are allowed to change whether or not rooms are for members only. The check box is checked by default.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>A room owner is the user who creates the room or a user who has been designated by the room creator or owner as someone with owner status (if allowed). A room owner is allowed to change the room configuration and destroy the room, in addition to all other administrator abilities.</td>
</tr>
<tr>
<td>Room owners can change whether or not only moderators can invite people to members-only rooms</td>
<td>Check this check box if you want to configure the room so that room owners can allow members to invite other users to the room. The check box is checked by default.</td>
</tr>
<tr>
<td>Users can add themselves to rooms as members</td>
<td>Check this check box if you want to configure the room so that any user can request to join the room at any time. If this check box is checked, the room has an open membership. The check box is unchecked by default.</td>
</tr>
<tr>
<td>Room owners can change whether users can add themselves to rooms as members</td>
<td>Check this check box if you want to configure the room so that room owners have the ability to change the setting that is listed in Step 5 at any time. The check box is unchecked by default.</td>
</tr>
</tbody>
</table>
Configure Availability Settings

Availability settings determine the visibility of a user within a room.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In Cisco Unified CM IM and Presence Administration, choose Messaging &gt; Group Chat and Persistent Chat.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure the availability member settings as described in Availability Settings.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Save.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In Cisco Unified IM and Presence Serviceability, choose Tools &gt; Control Center - Feature Services.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Restart the Cisco XCP Text Conference Manager service.</td>
</tr>
</tbody>
</table>

Availability Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Members and administrators who are not in a room are still visible in the room</td>
<td>Check this check box if you want to keep users on the room roster even if they are currently offline. The check box is checked by default.</td>
</tr>
<tr>
<td>Room owners can change whether members and administrators who are not in a room are still visible in the room</td>
<td>Check this check box if you want to allow room owners the ability to change the visibility of a member or administrator. The check box is checked by default.</td>
</tr>
<tr>
<td>Rooms are backwards-compatible with older clients</td>
<td>Check this check box if you want the service to function well with older Group Chat 1.0 clients. The check box is unchecked by default.</td>
</tr>
<tr>
<td>Room owners can change whether rooms are backwards-compatible with older clients</td>
<td>Check this check box if you want to allow room owners the ability to control backward compatibility of the chat rooms. The check box is unchecked by default.</td>
</tr>
<tr>
<td>Rooms are anonymous by default</td>
<td>Check this check box if you want the room to display the user nickname but keep the Jabber ID private. The check box is unchecked by default.</td>
</tr>
<tr>
<td>Room owners can change whether or not rooms are anonymous</td>
<td>Check this check box if you want to allow room owners to control the anonymity level of the user Jabber ID. The check box is unchecked by default.</td>
</tr>
</tbody>
</table>

Configure Occupancy Settings

Occupancy settings determine how many users can be in a chat room at a given time.
**Procedure**

**Step 1**  
To change the system maximum number of users that are allowed in a room, enter a value in the field for **How many users can be in a room at one time**. The default value is set to 1000.

**Note**  
The total number of users in a room should not exceed the value that you set. The total number of users in a room includes both normal users and hidden users.

**Step 2**  
To change the number of hidden users that are allowed in a room, enter a value in the field for **How many hidden users can be in a room at one time**. Hidden users are not visible to others, cannot send a message to the room, and do not send presence updates. Hidden users can see all messages in the room and receive presence updates from others. The default value is 1000.

**Step 3**  
To change the default maximum number of users that are allowed in a room, enter a value in the field for **Default maximum occupancy for a room**. The default value is set to 50 and cannot be any higher than the value that is set in Step 1.

**Step 4**  
Check **Room owners can change default maximum occupancy for a room** if you want to allow room owners to change the default maximum room occupancy. The check box is checked by default.

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

---

**Configure Chat Message Settings**

Use Chat Message settings to give privileges to users based on their role. For the most part, roles exist in a visitor-to-moderator hierarchy. For example, a participant can do anything a visitor can do, and a moderator can do anything a participant can do.

The check box is checked by default.

**Procedure**

**Step 1**  
From the drop-down list for **Lowest participation level a user can have to send a private message from within the room**, choose one:

- **Visitor** allows visitors, participants, and moderators to send a private message to other users in the room. This is the default setting.
- **Participant** allows participants and moderators to send a private message to other users in the room.
- **Moderator** allows only moderators to send a private message to other users in the room.

**Step 2**  
Check **Room owners can change the lowest participation level a user can have to send a private message from within the room** if you want to allow room owners to change the minimum participation level for private messages. The check box is checked by default.

**Step 3**  
From the drop-down list for **Lowest participation level a user can have to change a room's subject**, choose one:

a) **Participant** allows participants and moderators to change the room's subject. This is the default setting.
b) **Moderator** allows only moderators to change the room's subject.

Visitors are not permitted to change the room subject.
Configure Moderated Room Settings

Moderated rooms provide the ability for moderators to grant and revoke the voice privilege within a room (in the context of Group Chat, voice refers to the ability to send chat messages to the room). Visitors cannot send instant messages in moderated rooms.

Procedure

Step 1 Check **Rooms are moderated by default** if you want to enforce the role of moderator in a room. The check box is unchecked by default.

Step 2 Check **Room owners can change whether rooms are moderated by default** if you want to allow room owners the ability to change whether rooms are moderated. The check box is checked by default.

Step 3 Click **Save**.

Configure History Settings

Use History settings to set the default and maximum values of messages that are retrieved and displayed in the rooms, and to control the number of messages that can be retrieved through a history query. When a user joins a room, the user is sent the message history of the room. History settings determine the number of previous messages that the user receives.

Procedure

Step 1 To change the maximum number of messages that users can retrieve from the archive, enter a value in the field for **Maximum number of messages that can be retrieved from the archive**. The default value is set to 100. It serves as a limit for the next setting.

Step 2 To change the number of previous messages displayed when a user joins a chat room, enter a value in the field for **Number of messages in chat history displayed by default**. The default value is set to 15 and cannot be any higher than the value that is set in Step 1.

Step 3 Check **Room owners can change the number of messages displayed in chat history** if you want to allow room owners to change the number of previous messages displayed when a user joins a chat room. The check box is unchecked by default.

Step 4 Click **Save**.
Reset Chat Rooms to System Defaults

Use this procedure if you want to reset your group chat settings for both ad hoc and persistent chat rooms to the system defaults.

Ad hoc chat is enabled by default, but persistent chat is disabled by default. Completing this task will disable persistent chat.

Procedure

Step 1
In Cisco Unified CM IM and Presence Administration, choose Messaging > Settings.

Step 2
Click Set to Default.

Step 3
Click Save.

Chat Node Alias Management

Manage Chat Node Aliases

Complete these tasks to manage chat node aliases for your cluster. You can have the system manage aliases automatically, or you can update them yourself.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Assign Mode for Managing Chat Aliases, on page 215</td>
<td>Assign whether you want the system to manage chat node aliases or whether you want to do it manually.</td>
</tr>
<tr>
<td>Step 2 Add Chat Node Alias Manually, on page 216</td>
<td>Add, edit, or delete chat node aliases for your cluster.</td>
</tr>
</tbody>
</table>

Assign Mode for Managing Chat Aliases

Configure whether you want the system to assign chat node aliases automatically using the conference-x-clusterid.domain naming convention, or whether you want to assign them manually.

Before you begin

For information on chat node aliases, see Chat Node Alias Overview, on page 207.
Procedure

**Step 1**  
In **Cisco Unified CM IM and Presence Administration**, choose **Messaging > Group Chat and Persistent Chat**.

**Step 2**  
Enable or disable system-generated aliases:

- If you want the system to assign chat node aliases automatically, 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.

- If you want to assign chat node aliases manually, uncheck **System Automatically Manages Primary Group Chat Server Aliases**.

**What to do next**

- Even if you configure a system-generated alias for a chat node, you can associate more than one alias with the node if required.

- If you are federating with external domains, you may want to inform federated parties that the aliases have changed and new aliases are available. To advertise all aliases externally, configure DNS and publish the aliases as DNS records.

- If you update any of the system-generated alias configuration, perform one of these actions: Restart the Cisco XCP Text Conference Manager. See Restart the Cisco XCP Text Conference Manager, on page 158.

  - To add, edit, or delete a chat node alias, Add Chat Node Alias Manually, on page 216.

**Add Chat Node Alias Manually**

Use this procedure to 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 that are 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 **Cisco Unified CM IM and Presence Administration > Presence Settings > Advanced Settings** to see the domain.
Before you begin

Assign Mode for Managing Chat Aliases, on page 215

Procedure

Step 1
In Cisco Unified CM IM and Presence Administration, choose Messaging > Group Chat Server Alias Mapping.

Step 2
Click Find.

The Group Chat Server Alias window displays the existing node aliases.

Step 3
To add a new alias:
   a) Click Add New.
   b) In the Group Chat Server Alias field, enter a new alias.
   c) From the Server Name drop-down list box, select the server to which you want to assign the alias.
   d) Click Save.

Step 4
To edit an existing alias:
   a) Select the alias.
   b) Enter your updates and click Save.

Step 5
To delete an alias, select the alias and click Delete Selected.

What to do next

• Turn on the Cisco XCP Text Conference Manager. See Restart the Cisco XCP Text Conference Manager, on page 158.

Chat Node Alias 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.

Manage Chat Interactions

Changing chat node aliases can make the chat rooms in the database unaddressable and prevent your users from finding existing chat rooms.

Note these results before you change the constituent parts of aliases or other node dependencies:
• Cluster ID - This value is part of the fully qualified cluster name (FQDN). Changing the Cluster ID (choose System > Presence Topology: Settings) causes the FQDN to incorporate the new value and the system-managed alias to automatically change across the cluster. For manually-managed aliases, it is the responsibility of the Administrator to manually update the alias list if the Cluster ID changes.

• Domain - This value is part of the FQDN. Changing the Domain (choose Presence > Presence Settings) causes the FQDN to incorporate the new value and the system-managed alias to automatically change across the cluster. For manually-managed aliases, it is the responsibility of the Administrator to manually update the alias list if the Domain changes.

• Connection between the chat node and external database - The chat node will not start if persistent chat is enabled and you do not maintain the correct connection with the external database.

• Deletion of a chat node — If you delete a node associated with an existing alias from the Presence Topology, chat rooms created using the old alias may not be addressable unless you take further action.

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.
Managed File Transfer Administration Overview

As the IM and Presence Service administrator, you are responsible for managing file storage and disk usage for the Managed File Transfer feature. Use this chapter to monitor the levels of file storage and disk usage and to set counters and alerts to let you know when the levels exceed your defined thresholds.

Managing External File Server and Database Server

When managing external database size, you can combine queries with shell scripting so that files get purged from the database automatically, according to your specifications. To create your queries use file transfer metadata. This includes transfer type, file type, timestamp, absolute path on the file server to the file, and other information.

When choosing how to handle file transfers within IM and group chat, consider that one-to-one IM and group chat are probably transient so transferred files may be deleted promptly. However, keep in mind that:

- IMs delivered to offline users may trigger a delayed request for a file.
- Persistent chat transfers may need to be longer lived.
Managed File Transfer Administration Prerequisites

Configure the Managed File Transfer feature. For details, see Configure Managed File Transfer, on page 173.

Managed File Transfer Administration Task Flow

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>AFT_LOG Table Example Query and Output, on page 220</td>
<td>The following procedure provides an example of a query that you can run on the AFT_LOG table and how to use the output to purge unwanted files from the file server.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Set Service Parameter Thresholds, on page 222</td>
<td>Configure the Managed File Transfer service parameters to define the threshold at which an RTMT alarm is generated for the external file server disk space.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure XCP File Transfer Manager Alarms, on page 223</td>
<td>Configure alarms for Managed File Transfer to let you know when defined thresholds have been reached.</td>
</tr>
</tbody>
</table>

AFT_LOG Table Example Query and Output

The following procedure provides an example of a query that you can run on the AFT_LOG table and how to use the output to purge unwanted files from the file server.

This query returns records for every uploaded file after the specified date.
**Procedure**

**Step 1**

In the IM and Presence Service Command Line Interface (CLI), enter the following command:

```sql
SELECT file_path
FROM aft_log
WHERE method='Post' AND timestampvalue > '2014-12-18 11:58:39';
```

The command generates the following output:

```
/opt/mftFileStore/node_1/files/im/20140811/15/file_name1
/opt/mftFileStore/node_1/files/im/20140811/15/file_name2
/opt/mftFileStore/node_1/files/im/20140811/15/file_name3
/opt/mftFileStore/node_1/files/im/20140811/15/file_name4
...
/opt/mftFileStore/node_1/files/im/20140811/15/file_name99
/opt/mftFileStore/node_1/files/im/20140811/15/file_name100
```

**Step 2**

Write a script that uses the `rm` command and this output to purge the above files from the external file server. For sample SQL queries, see *Database Setup for IM and Presence Service on Cisco Unified Communications Manager*.

**Note**

Files that have not been purged from the external file server can still be accessed or downloaded even if records relating to those files have been purged from the external database.

**What to do next**

*Set Service Parameter Thresholds, on page 222*

**External Database Disk Usage**

You must ensure that the disks or tablespaces do not become full, otherwise the managed file transfer feature may stop working. Following are sample SQL commands that you can use to purge records from the external database. For additional queries, see the *Database Setup for IM and Presence Service on Cisco Unified Communications Manager*.

**Note**

Files that have not been purged from the external file server can still be accessed or downloaded even if records relating to those files have been purged from the external database.
### Sample Command

<table>
<thead>
<tr>
<th>Action</th>
<th>Sample Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove all records of files that were uploaded.</td>
<td>DELETE FROM aft_log WHERE method = 'Post';</td>
</tr>
<tr>
<td>Remove records of all files that were downloaded by a specific user.</td>
<td>DELETE FROM aft_log WHERE jid LIKE '&lt;userid&gt;@&lt;domain&gt;%' AND method = 'Get';</td>
</tr>
<tr>
<td>Remove records of all files that were uploaded after a specific time.</td>
<td>DELETE FROM aft_log WHERE method = 'Post' AND timestampvalue &gt; '2014-12-18 11:58:39';</td>
</tr>
</tbody>
</table>

In addition, there are counters and alarms that can help you manage database disk usage. For details, see [Alarms and Counters for Managed File Transfer, on page 223](#).

### Set Service Parameter Thresholds

Configure the Managed File Transfer service parameters to define the threshold at which an RTMT alarm is generated for the external file server disk space.

#### Procedure

1. **Step 1** In Cisco Unified CM IM and Presence Administration, choose System > Service Parameters.
2. **Step 2** Choose the Cisco XCP File Transfer Manager service for the node.
3. **Step 3** Enter values for the following service parameters.
   - **External File Server Available Space Lower Threshold** — If the percentage of available space on the external file server partition is at or below this value, the XcpMFTExtFsFreeSpaceWarn alarm is raised. The default value is 10%.
   - **External File Server Available Space Upper Threshold** — If the percentage of available space on the external file server partition reaches or exceeds this value, the XcpMFTExtFsFreeSpaceWarn alarm is cleared. The default value is 15%.

   **Note** Do not configure the lower threshold value to be greater than the upper threshold value. Otherwise the Cisco XCP File Transfer Manager service will not start after you restart the Cisco XCP Router service.

4. **Step 4** Click Save.
5. **Step 5** Restart the Cisco XCP Router service:
   a) From Cisco Unified IM and Presence Serviceability, choose Tools > Control Center - Network Services.
   b) From the Server drop-down select the IM and Presence publisher and click Go.
c) Under **IM and Presence Services**, select **Cisco XCP Router**, and click **Restart**.

---

**What to do next**

[Configure XCP File Transfer Manager Alarms, on page 223](#)

## Configure XCP File Transfer Manager Alarms

Configure alarms for Managed File Transfer to let you know when defined thresholds have been reached.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sign in to <strong>Cisco Unified IM and Presence Serviceability</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Choose <strong>Alarm &gt; Configuration</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>From the <strong>Server</strong> drop-down, choose the server (node), and click <strong>Go</strong>.</td>
</tr>
<tr>
<td>4</td>
<td>From the <strong>Service Group</strong> drop-down list, choose <strong>IM and Presence Services</strong> and click <strong>Go</strong>.</td>
</tr>
<tr>
<td>5</td>
<td>From the <strong>Service</strong> drop-down list, choose <strong>Cisco XCP File Transfer Manager (Active)</strong> and click <strong>Go</strong>.</td>
</tr>
<tr>
<td>6</td>
<td>Configure the preferred alarm settings. For help with the fields and their settings, refer to the online help.</td>
</tr>
<tr>
<td>7</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

**What to do next**

For more information on the available alarms and counters, see [Alarms and Counters for Managed File Transfer, on page 223](#)

### Alarms and Counters for Managed File Transfer

With Managed File Transfers, the transferred files get delivered to users only after they are successfully archived to the external file server, and after the file metadata is logged to the external database. If an IM and Presence Service node loses its connection to the external file server or external database, IM and Presence Service does not deliver the file to the recipient.

**Alarms for Managed File Transfer**

To ensure that you are notified if a connection is lost, verify that the following alarms are properly configured in the Real-Time Monitoring Tool.

---

**Note**

Any files that were uploaded before the connection to the external file server was lost and which were in the process of being downloaded to the recipient, fail to be downloaded. However, there is a record of the failed transfer in the external database. To identify these files, the external database fields file_size and bytes_transferred do not match.
**Table 23: Alarms for Managed File Transfers**

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>XcpMFTExtFsMountError</td>
<td>Cisco XCP File Transfer Manager has lost its connection to the external file server.</td>
<td>Check the External File Server Troubleshooter for more information. Check that the external file server is running correctly. Check if there is any problem with the network connectivity to the external file server.</td>
</tr>
<tr>
<td>XcpMFTExtFsFreeSpaceWarn</td>
<td>Cisco XCP File Transfer Manager has detected that the available disk space on the external file server is low.</td>
<td>Free up space on the external file server by deleting unwanted files from the partition used for file transfer.</td>
</tr>
<tr>
<td>XcpMFTDBConnectError</td>
<td>Cisco XCP data access layer was unable to connect to the database.</td>
<td>Check the System Troubleshooter for more information. Check that the external database is running healthy and if there is any problem with the network connectivity to the external database server.</td>
</tr>
<tr>
<td>XcpMFTDBFullError</td>
<td>Cisco XCP File Transfer Manager cannot insert or modify data in the external database because either the disk or tablespace is full.</td>
<td>Check the database and assess if you can free up or recover any disk space. Consider adding additional database capacity.</td>
</tr>
</tbody>
</table>

**Counters for Managed File Transfer**

To help you administer managed file transfer, you can monitor the following counters via the Real-Time Monitoring Tool. These counters are saved in the Cisco XCP MFT Counters folder.

**Table 24: Counters for Managed File Transfers**

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MFTBytesDownloadedLastTimeslice</td>
<td>This counter represents the number of bytes downloaded during the last reporting interval (typically 60 seconds).</td>
</tr>
<tr>
<td>MFTBytesUploadedLastTimeslice</td>
<td>This counter represents the number of bytes uploaded during the last reporting interval (typically 60 seconds).</td>
</tr>
<tr>
<td>MFTFilesDownloaded</td>
<td>This counter represents the total number of files downloaded.</td>
</tr>
<tr>
<td>MFTFilesDownloadedLastTimeslice</td>
<td>This counter represents the number of files downloaded during the last reporting interval (typically 60 seconds).</td>
</tr>
<tr>
<td>MFTFilesUploaded</td>
<td>This counter represents the total number of files uploaded.</td>
</tr>
<tr>
<td>Counter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MFTFilesUploadedLastTimeslice</td>
<td>This counter represents the number of files uploaded during the last reporting interval (typically 60 seconds).</td>
</tr>
</tbody>
</table>
Alarms and Counters for Managed File Transfer
CHAPTER 24

Manage End Users

• Manage End Users Overview, on page 227
• Manage End Users Task Flow, on page 229
• Presence Authorization Interactions and Restrictions, on page 238

Manage End Users Overview

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

As part of your administrative tasks for managing end users, you may have to manage the following tasks:

• Configure a default policy for authorizing presence requests
• Configure a scheduled system check for duplicate or invalid user IDs and directory URIs
• Fix user ID and directory URI issues as they arise

For information on how to import and set up end users, see the "Configure End Users" section of the System Configuration Guide for Cisco Unified Communications Manager.

For information on completing bulk user contact list imports and exports, see Bulk Administration of Contact Lists, on page 289.

Presence Authorization Overview

You must assign a system authorization policy for Presence Subscription requests. The Presence Authorization Policy determines, at a system level, whether end users on the system can view other end users' presence status without requiring the authorization of the end user whose presence is requested. This setting is configured via the Allow users to view the availability of other users without being prompted for approval check box in the Presence Settings configuration window. The available settings depends partially on which protocol is being deployed:

• For SIP-based clients, you must configure the IM and Presence Service to authorize automatically all presence subscription requests or Presence will not function correctly (this is the default setting). When this option is configured, the IM and Presence Service authorizes all requests automatically with one exception: if the user whose presence is being requested has a blocked list configured in their Cisco Jabber client that includes the user making the request. In this case, the user will be prompted to approve the Presence request.
• For XMPP-based clients, you can configure whether or not you want the IM and Presence Service to prompt users to authorize presence requests from other users, or whether those presence requests should be authorized automatically.

Note

The authorization system settings can be overridden by the User Policy configuration that end users can configure within their Cisco Jabber clients.

User Policy Settings in Jabber

When authorizing a presence request, the IM and Presence Service also refers to the user policy that users configure within their Cisco Jabber clients. End users can add other users to a blocked list, which prevents those other users from viewing presence status without authorization, or they can add those users to an allowed list, which authorizes those users to view their presence status. These settings override the system default settings:

End users can configure the following within their Cisco Jabber clients:

• Blocked list—Users can add other users (both local and external users) to a blocked list. If any users of the blocked users view that user's presence, they will always see the availability status of the user as unavailable regardless of the true status of the user. Users can also block a whole federated domain.

• Allowed list—Users can allow other local and external users to always be able to view their availability. The user can also allow a whole external (federated) domain.

• Default policy—The default policy settings for that user. The user can set the policy to block all users, or allow all users.

Validating User IDs and Directory URIs

For single cluster deployments, duplicate user IDs and directory URIs are not an issue as it is not possible to assign duplicates within the same cluster. However, with intercluster deployments, you can unintentionally assign the same user ID or directory URI value to different users on different clusters.

The IM and Presence Service provides the following validation tools to check for duplicate user IDs and duplicate directory URIs:

• Cisco IM and Presence Data Monitor service—You can configure ongoing system checks with this service. The Cisco IM and Presence Data Monitor service checks the active directory entries for duplicate user IDs and duplicate, or empty, directory URIs for all IM and Presence Service intercluster nodes. Administrators are notified via an alarm or alert. You can use the Cisco Unified Real-Time Monitoring Tool to monitor alarms and to set up email alerts for Duplicate UserID and DuplicateDirectoryURI errors.

• System Troubleshooter—Use the System Troubleshooter if you want to run an ad hoc check the system for errors, including duplicate directory URIs and user IDs. The Troubleshooter provides details for up to 10 users only. The System Troubleshooter can be accessed from the Cisco Unified CM IM and Presence Administration interface (Diagnostics > System Troubleshooter).

• Command Line Interface—To obtain a complete and detailed report of duplicate URIs and User IDs, run the `util users validate all` CLI command.
## Manage End Users Task Flow

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Assign a Presence Authorization Policy, on page 229</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configure Data Monitor Checks for User Data, on page 230</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Validate User Data via the System Troubleshooter, on page 232</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Validate User IDs and Directory URIs via CLI, on page 233</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>View Presence Settings for User, on page 236</td>
</tr>
</tbody>
</table>

### Assign a Presence Authorization Policy

Assign a system authorization policy for Presence Subscription requests.

#### Note

On their Cisco Jabber client, end users can configure whether they want to allow other users to be able to view their presence status. This user policy overrides the system authorization settings.

#### Procedure

**Step 1**

In Cisco Unified CM IM and Presence Administration, choose **Presence > Settings**.

**Step 2**

Check or uncheck the **Allow users to view the availability of other users without being prompted for approval** check box.

- Checked—IM and Presence automatically authorizes all Presence subscription requests received within the local enterprise.
- Unchecked—IM and Presence refers all presence subscription requests to the client whose presence is requested. The user can accept or reject the request.

**Note**

If you are deploying SIP-based clients, you must check this check box. If leave the check box unchecked, your deployment supports XMPP clients only.

**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.

Configure Data Monitor Checks for User Data

Complete these tasks to configure the Cisco IM and Presence Data Monitor to validate directory URIs and user IDs at scheduled intervals. Any errors are communicated via an alarm or alert with the Cisco Unified Real-Time Monitoring Tool.

Note
Duplicate directory URI and duplicate user ID errors are only an issue for intercluster deployments.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Set Schedule for User ID and Directory URI Validation Check, on page 230</td>
<td>Configure the scheduled interval for the Cisco IM and Presence Data Monitor check. The service checks the active directory entries for errors, including duplicate directory URIs and user IDs.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Set up Email Server for Email Alerts, on page 231</td>
<td>Optional. If you want to receive email alerts whenever the Data Monitor service finds a duplicate directory URI or user ID, you must set up an email server with the Real-Time Monitoring Tool.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Enable Email Alerts, on page 231</td>
<td>Optional. Complete this procedure to enable email alerts for the DuplicateDirectoryURI and DuplicateUserID alarm. When the Cisco IM and Presence Data Monitor service returns one of these alarms, an email will be sent to the administrator.</td>
</tr>
</tbody>
</table>

Set Schedule for User ID and Directory URI Validation Check

Set the scheduled interval for the Cisco IM and Presence Data Monitor service. This service checks the system at scheduled intervals for data errors, including duplicate directory URIs and user IDs. The service raises an alarm or alert that can be viewed via the Real-Time Monitoring Tool whenever an error is found.

Before you begin
The Cisco IM and Presence Data Monitor network service must be running. By default, the service is running. You can confirm that the service is running from the Control Center - Network Services window in the Cisco Unified IM and Presence Serviceability interface.
**Procedure**

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

**Step 2** In the **Service** drop-down, choose **Cisco IM and Presence Data Monitor**.

**Step 3** In the **User Check Interval** field, enter the time interval, in minutes. You can enter an integer from 5 through 1440 (minutes). The default value is 30 minutes.

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

**What to do next**

Optional. If you want to set up email alerting whenever a DuplicateDirectoryURI or DuplicateUserID alarm is raised, [Set up Email Server for Email Alerts, on page 231](#).

**Set up Email Server for Email Alerts**

It may help to have an administrator receive an email alert whenever the Data Monitor validation check finds duplicate directory URI and user ID errors. If so, use this optional procedure to set up an email server for email alerts.

**Procedure**

**Step 1** In the Real-Time Monitoring Tool's System window, click **Alert Central**.

**Step 2** Choose **System > Tools > Alert > Config Email Server**.

**Step 3** In the **Mail Server Configuration** popup, enter the details for the mail server.

**Step 4** Click **OK**.

**What to do next**

[Enable Email Alerts, on page 231](#)

**Enable Email Alerts**

Use this procedure to set up the Real-Time Monitoring Tool to email an administrator whenever a DuplicateUserID or DuplicateDirectoryURI system alert is raised.

**Before you begin**

[Set up Email Server for Email Alerts, on page 231](#)

**Procedure**

**Step 1** In the Real-Time Monitoring Tool **System** area, click **Alert Central**.

**Step 2** Click the **IM and Presence** tab.
Step 3  Click on the alert for which you want to add an email alert. For example, the DuplicateDirectoryURI or DuplicateUserid system alerts.

Step 4  Choose Tools > Alert > Config Alert Action.

Step 5  In the Alert Action popup, select Default and click Edit.

Step 6  In the Alert Action popup, Add a recipient.

Step 7  In the popup window, enter the address where you want to send email alerts, and click OK.

Step 8  In the Alert Action popup, make sure that the address appears under Recipients and that the Enable check box is checked.

Step 9  Click OK.

Step 10  Repeat this procedure for each system alert for which you want to enable email alerting.

---

Validate User Data via the System Troubleshooter

Use the System Troubleshooter in the Cisco Unified CM IM and Presence Administration GUI to check your deployment for duplicate user IDs and duplicate or invalid directory URIs. The troubleshooter checks all nodes and clusters in the deployment.

Procedure

Step 1  In Cisco Unified CM IM and Presence Administration, choose Diagnostics > System Troubleshooter.

Step 2  Monitor the status of user IDs and Directory URIs in the User Troubleshooter area. The Problem column is populated if the system check detects any issues.

- Verify that all users have a unique User ID configured.
- Verify that all users have a Directory URI configured.
- Verify that all users have a unique Directory URI configured.
- Verify that all users have a valid Directory URI configured.
- Verify that all users have a unique Mail ID configured.

Note  Duplicate mail IDs impact both Email Address for Federation and Exchange Calendar integration features.

Step 3  If an issue appears, click the fix link in the Solution column to be redirected to the End User Configuration window in Cisco Unified Communications Manager where you can reconfigure user settings.

Note  The user ID and directory URI fields in the user profile may be mapped to the LDAP Directory. In that case, apply the fix in the LDAP Directory server.

---

What to do next

If any issues arise, edit the user settings in the End User Configuration window of Cisco Unified Communications Manager. If the user is synchronized from an LDAP directory, you will need to make your edits in the LDAP directory.

If you need a more detailed report, Validate User IDs and Directory URIs via CLI, on page 233.
Validate User IDs and Directory URIs via CLI

Use the Command Line Interface to run a detailed check of your deployment for duplicate user IDs and duplicate directory URIs.

**Procedure**

**Step 1**
Login to the Command Line Interface.

**Step 2**
Run one of the following commands:

- `utils users validate all`— Checks the system for both duplicate user IDs and duplicate directory URIs.
- `utils users validate userid`— Checks the system for duplicate user IDs.
- `utils users validate uri`— Checks the system for duplicate directory URIs.

The CLI returns a report of duplicate directory URIs and/or user IDs. For a sample report, see User ID and Directory URI CLI Validation Examples, on page 233.

**What to do next**
If any issues arise, edit the user settings in the End User Configuration window of Cisco Unified Communications Manager. If the user is synchronized from an LDAP directory, you will need to make your edits in the LDAP directory.

**User ID and Directory URI CLI Validation Examples**

The CLI command to validate IM and Presence Service users to identify users that have duplicate user IDs and duplicate or invalid Directory URIs is `utils users validate {all | userid | uri}`. For more information about using the CLI and command descriptions, see the Command Line Interface Guide for Cisco Unified Communications Solutions.

**CLI Example Output Showing User ID Errors**

```
Users with Duplicate User IDs
---------------------------------------------
User ID: user3
Node Name
cucm-imp-1
cucm-imp-2
```

**CLI Example Output Showing Directory URI Errors**

```
Users with No Directory URI Configured
---------------------------------------------
Node Name: cucm-imp-2
User ID
user4

Users with Invalid Directory URI Configured
---------------------------------------------
```
User ID and Directory URI Errors

The Cisco IM and Presence Data Monitor service checks the Active directory entries for duplicate user IDs and empty or duplicate directory URIs for all IM and Presence Service intercluster nodes. Duplicate user IDs or directory URIs are not possible within a cluster; however, it is possible to unintentionally assign the same user ID or directory URI value to users on different clusters in an intercluster deployment.

The following list displays possible errors that may be found. You can view these errors in the Real-Time Monitoring Tool, which will raise an alarm or alert for each of these:

**DuplicateDirectoryURI**

This alert indicates that there are multiple users within the intercluster deployment that are assigned the same directory URI value when the Directory URI IM Address scheme is configured.

**DuplicateDirectoryURIWarning**

This warning indicates that there are multiple users within the intercluster deployment that are assigned the same directory URI value when the `userID@Default_Domain` IM Address scheme is configured.

**DuplicateUserId**

This alert indicates there are duplicate user IDs assigned to one or more users on different clusters within the intercluster deployment.

**InvalidDirectoryURI**

This alert indicates that one or more users within the intercluster deployment are assigned an empty or invalid directory URI value when the Directory URI IM Address scheme is configured.

**InvalidDirectoryURIWarning**

This warning indicates that one or more users within the intercluster deployment are assigned an empty or invalid directory URI value when the `userID@Default_Domain` IM Address scheme is configured.

To gather specific information about which users have these alarm conditions, use the Command Line Interface for a complete listing. System alarms do not provide details about the affected users and the System Troubleshooter displays details for only up to 10 users. Use the Command Line Interface and validate users to gather information about which users caused an alarm. For more information, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

**Caution**

Take the appropriate action to fix duplicate user IDs and duplicate or invalid Directory URIs to avoid communications disruptions for the affected users. To modify user contact information, see the *Cisco Unified Communications Manager Administration Guide*.
## Errors and Suggested Action

The following table describes userID and directory URI error conditions that can occur when a system check for duplicate user IDs and duplicate or invalid directory URIs is performed on an intercluster deployment. The alarms that are raised are listed, as well as suggested actions to take to correct the error.

### Table 25: User ID and Directory URI Error Conditions and Suggested Action

<table>
<thead>
<tr>
<th>Error Condition</th>
<th>Description</th>
<th>Suggested Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duplicate user IDs</td>
<td>Duplicate user IDs are assigned to one or more users on different clusters within the intercluster deployment. The affected users may be homed on an intercluster peer.</td>
<td>If the DuplicateUserID alert is raised, take immediate action to correct the issue. Each user within the intercluster deployment must have a unique userID.</td>
</tr>
<tr>
<td></td>
<td><strong>Related alarms:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DuplicateUserID</td>
<td></td>
</tr>
<tr>
<td>Duplicate directory URIs</td>
<td>Multiple users within the intercluster deployment are assigned the same directory URI value. The affected users may be homed on an intercluster peer.</td>
<td>If your system is configured to use the Directory URI IM address scheme and the DuplicateDirectoryURI alert is raised, take immediate action to correct the issue. Each user must be assigned a unique directory URI. If your system is configured to use the userID@Default_Domain IM address scheme and duplicate directory URIs are detected, the DuplicateDirectoryURIWarning warning is raised and no immediate action is required; however, Cisco recommends that you resolve the issue.</td>
</tr>
<tr>
<td></td>
<td><strong>Related alarms:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DuplicateDirectoryURI</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DuplicateDirectoryURIWarning</td>
<td></td>
</tr>
<tr>
<td>Invalid directory URIs</td>
<td>One or more users within the deployment are assigned an invalid or empty directory URI value. A URI that is not in the userID@domain format is an invalid Directory URI. The affected users may be homed on an intercluster peer.</td>
<td>If your system is configured to use the Directory URI IM address scheme and the following alert is raised, take immediate action to correct the issue: InvalidDirectoryURI. If your system is configured to use the userID@Default_Domain IM address scheme and invalid directory URIs are detected, the InvalidDirectoryURIWarning warning is raised and no immediate action is required; however, Cisco recommends that you resolve the issue.</td>
</tr>
<tr>
<td></td>
<td><strong>Related alarms:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>InvalidDirectoryURI</td>
<td></td>
</tr>
<tr>
<td></td>
<td>InvalidDirectoryURIWarning</td>
<td></td>
</tr>
</tbody>
</table>
View Presence Settings for User

Use the Presence Viewer to get a summarized view of presence settings for an IM and Presence-enabled end user. The Presence Viewer provides information such as Presence server assignments, contacts and watchers.

Before you begin

The Cisco AXL Web Service, Cisco SIP Proxy service, and Cisco Presence Engine service must all be running in Cisco Unified Serviceability.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From Cisco Unified CM Administration, choose <strong>User Management &gt; End Users</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click <strong>Find</strong> and select the end user for whom you want to view presence settings.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Under <strong>Service Settings</strong>, click <strong>Presence Viewer for User</strong> to open the Presence Viewer. Refer to the following table if you want to customize the view.</td>
</tr>
</tbody>
</table>

**Table 26: End User Presence Viewer Fields**

<table>
<thead>
<tr>
<th>Presence Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| User Status      | Identifies the availability state of the user, including:  
• Available  
• Away  
• Do Not Disturb  
• Unavailable  
• Custom |
| User ID          | Identifies the selected user ID. A user photo is displayed if one is available for that user.  
You can click **Submit** to choose a different User ID. |
| View From Perspective of | Specifies a user to see the availability status from the perspective of the user. This allows you to determine how the availability status of a specified user appears to another user, known as a watcher. This functionality is useful in debugging scenarios, for example, where a user has configured privacy policies.  
A maximum of 128 characters is allowed. |
## Presence Setting Description

### Contacts
Displays the number of contacts in the contact list for this user.

Click the arrow beside the Contacts heading in the Contacts and Watchers list area to view the availability status of a specific user contact. Click the arrow beside the group name to expand the list of contacts within that group.

Contacts that are not part of a group (groupless contacts) display below the contact group list. A contact may belong to multiple groups, but will only count once against the contact list size for that user.

A warning message appears if the maximum number of contacts configured for end users is exceeded. For more information about IM and Presence Service configuration and the maximum contacts setting, see the *IM and Presence Administration Online Help*.

### Watchers
Displays a list of users, known as watchers, who have subscribed to see the availability status of this user in their contact list.

Click the arrow beside the Watchers heading in the Contacts and Watchers list area to view the availability status of a specific watcher. Click the arrow beside the group name to expand the list of watchers within that group.

A watcher may belong to multiple groups but will only count once against the watcher list size for that user.

A warning message appears if the maximum number of watchers configured for end users is exceeded. For more information about IM and Presence Service configuration and the maximum watchers setting, see the *IM and Presence Administration Online Help*.

### Presence Server Assignment
Identifies the IM and Presence Service server to which the user is assigned. Hyperlinks allow you to go directly to the server configuration page for details.

### Enable accessible presence icons
Select this check box to enable presence accessibility icons for this end user.

### Submit
Select to run the Presence Viewer.

The user must be assigned to an IM and Presence node for valid presence information to be available. The AXL, Presence Engine and Proxy Service must all be running on the IM and Presence server for this action to be functional.
## Presence Authorization Interactions and Restrictions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Restriction</th>
</tr>
</thead>
</table>
| Turning off automatic presence authorization                  | If you turn off automatic authorization of presence requests, IM and Presence Service still automatically authorizes subscription requests for users that are on the contact list of the other user. This applies to users in the same domain, and users in different domains (federated users). For example:  
  - User A wishes to subscribe the view the availability status of User B. Automatic authorization is off on IM and Presence Service, and User B is not in the Allowed or Blocked list for the User A  
  - IM and Presence Service sends the presence subscription request to the client application of User B, and the client application prompts User B to accept or reject the subscription.  
  - User B accepts the presence subscription request, and User B is added to the contact list of User A.  
  - User A is then automatically added to the contact list for User B without being prompted to authorize the presence subscription. This occurs even if the policy for User B blocks the external domain, or User B has "ask me" configured in the user profile. |
| Interdomain Federation—Presence requests received from the external domain | IM and Presence will rely solely on the user policy settings of the user whose presence status is requested. If the user has selected "ask me" in their user policy, and has not added an Allowed or Blocked list for the external contact or domain, then IM and Presence sends the Presence request to the end user to authorize. |
CHAPTER 25

Migrate Users

• Migrate Users Overview, on page 239
• Migrate Users Prerequisites, on page 239
• Migrate Users Task Flow, on page 239

Migrate Users Overview

This section describes how to migrate users between IM and Presence Service clusters.

Migrate Users Prerequisites

• Run full backups of both the current and destination cluster. For details, see Backup Task Flow, on page 264.

• Ensure that the users to be migrated are licensed for the IM and Presence Service or Cisco Jabber on their current home cluster only. If these users are licensed on any cluster other than the premigration cluster, they must be fully unlicensed before proceeding with the migration tasks.

Migrate Users Task Flow

Complete these task to migrate IM and Presence users to a new cluster.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Start Essential Services for Migration, on page 241</td>
<td>Before migrating, confirm the following services are running:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco AXL Web Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Sync Agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Intercluster Sync Agent</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> Check for Intercluster Sync Errors, on page 241</td>
<td>Run the System Troubleshooter and confirm that there are no intercluster sync issues.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> Configure Standard Presence for Migration, on page 240</td>
<td>Before migrating users, configure these standard Presence settings.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> Export User Contact Lists, on page 242</td>
<td>Complete this procedure to export the contact lists of the migrating users from their current cluster.</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 5** Complete one of these mini-task flows to move users to the new cluster:  
  - Migrate Users via LDAP, on page 242  
  - Move Users to New Cluster Manually, on page 244  
  - Migrate Users via Bulk Administration, on page 246 | Move users to the new cluster. You can use LDAP to provision users in the new cluster, move users manually, or use Bulk Administration to migrate users to the new cluster. |
| **Step 6** Import Contact Lists on Home Cluster, on page 249 | After you have migrated users to the new cluster, import the contact lists to restore contact data for the migrated users. |
| **Step 7** Update Users in Old Cluster, on page 250 | You may not want to remove users from the old cluster until after you confirm that everything is working fine in the new cluster. Use this procedure to use Bulk Administration's Update Users feature to remove IM and Presence functionality from the old cluster. |

## Configure Standard Presence for Migration

Before migrating users, configure these Presence settings.

**Procedure**

| Step 1 | From Cisco Unified CM IM and Presence Administration, choose Presence > Settings > Standard Configuration. |
| Step 2 | Check the Allow users to view the availability of other users without being prompted for approval check box. |
| Step 3 | For the Maximum Contact List Size (per user) setting, check the No Limit check box. |
| Step 4 | For the Maximum Watchers (per user) setting, check the No Limit check box |
| Step 5 | Click Save. |
Check for Intercluster Sync Errors

Before migrating, confirm that there are no intercluster sync errors.

Procedure

Step 1
From Cisco Unified CM IM and Presence Administration, choose Diagnostics > System Troubleshooter.

Step 2
Confirm that there are no intercluster sync errors. If there are errors, fix them before proceeding.

Start Essential Services for Migration

In Cisco Unified IM and Presence Serviceability, confirm that the following essential services for the migration are running:

- Cisco AXL Web Service
- Cisco Sync Agent
- Cisco Intercluster Sync Agent

Procedure

Step 1
From Cisco Unified IM and Presence Serviceability, choose Tools > Control Center - Feature Services.

Step 2
From the Server drop-down select your IM and Presence node and click Go.

Step 3
Under Database and Admin Services, confirm that the Cisco AXL Web Service is Started. If the service is not running (the default setting is not running), select the service and click Start.

Step 4
Choose Tools > Control Center - Network Services.

Step 5
From the Server drop-down select your IM and Presence node and click Go.

Step 6
Under IM and Presence Services, confirm that both the Cisco Sync Agent and Cisco Intercluster Sync Agent services are running. If they are not running, Start them.

What to do next

Export User Contact Lists, on page 242
Export User Contact Lists

Complete this procedure to export the contact lists of the migrating users from their current cluster.

Procedure

**Step 1**
Export the contact lists of the migrating users from the current home cluster.

a) In Cisco Unified CM IM and Presence Administration, choose 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) In Cisco Unified CM IM and Presence Administration, choose 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. A time stamp is appended to the filename.

e) From the Job Results section, choose the log file to see a summary of what was uploaded. The log file includes the start and end time and result summary for the job.

**Step 3**
Download the contact list export file and store it for use later when the user migration is complete.

a) In Cisco Unified CM IM and Presence Administration, choose 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

Go to one of the following task flows to assign users in the new cluster:

- Migrate Users via LDAP, on page 242
- Move Users to New Cluster Manually, on page 244

Migrate Users via LDAP

Complete these tasks if your users are synced with an LDAP Directory and you want to migrate to a new cluster.
You must add your LDAP Directory configuration into the new cluster. This includes any service profiles, user profiles, and feature group templates. Make sure that your feature group template configuration has the Enable Users for Unified CM IM and Presence check box checked.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Update External LDAP Directory, on page 243</td>
<td>You may need to update your external LDAP directory if your deployment uses a separate LDAP structure for each cluster and where users are synchronized only to their home cluster.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure LDAP in New Cluster, on page 244</td>
<td>If LDAP is enabled on Cisco Unified Communications Manager, import users to your new cluster by synchronizing your new cluster with the updated LDAP directory.</td>
</tr>
</tbody>
</table>

### What to do next

Import Contact Lists on Home Cluster, on page 249

### Update External LDAP Directory

You may need to update your external LDAP directory if your deployment uses a separate LDAP structure for each cluster and where users are synchronized only 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.

**Note**

Depending on how you have your LDAP Directory sync configured in the old and new cluster, moving your users within the external LDAP Directory may automatically migrate those users to the new IM and Presence Service cluster when the next sync occurs.

### Procedure

**Step 1**
Update users in your external LDAP directory.

**Step 2**
After you move the users, delete the LDAP entries from the old LDAP cluster.
Configure LDAP in New Cluster

Before you begin

Provision the LDAP directory in your new cluster. If your LDAP directory sync includes universal line and device templates, and feature group templates, you must configure these templates in your new cluster. Make sure that your feature group template has the following options checked:

- Home Cluster
- Enable Users for Unified CM IM and Presence

For details on how to configure an LDAP directory sync, refer to the "Configure End Users" section of the System Configuration Guide for Cisco Unified Communications Manager.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From Cisco Unified CM Administration, choose System &gt; LDAP &gt; LDAP Directory.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click Find and select the LDAP Directory that you've configured.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Perform Full Sync Now.</td>
</tr>
</tbody>
</table>

Move Users to New Cluster Manually

Complete these tasks to move a user to the new cluster manually.

Note

If you have a large number of users, you may want to use the Bulk Administration Tool in Cisco Unified Communications Manager to update a large number of users via a csv file. For details, see the Bulk Administration Guide for Cisco Unified Communications Manager.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Disable IM and Presence For User Manually, on page 245</td>
<td>Disable a migrating user for IM and Presence Service and Cisco Jabber on their current home cluster.</td>
</tr>
<tr>
<td>Step 2 Import Users Manually, on page 245</td>
<td>If LDAP synchronization is not configured in the new cluster, provision users manually to</td>
</tr>
</tbody>
</table>
Disable IM and Presence For User Manually

The following procedure describes how to disable a migrating user for IM and Presence Service and Cisco Jabber on their current home cluster.

Procedure

Step 1 In **Cisco Unified CM Administration**, choose > **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**.

What to do next

Import Users Manually, on page 245

Import Users Manually

If LDAP synchronization is not configured in the new cluster, import users manually to your new Cisco Unified Communications Manager cluster.

For details, see **Configure User Settings**, on page 59.
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**

1. In **Cisco Unified CM Administration**, choose **User Management > End User**.
2. Use the filters to find the user that you want to enable for IM and Presence Service.
3. In the **End User Configuration** screen, check **Enable User for Unified CM IM and Presence**.
4. Click **Save**.
5. Provision the users on Cisco Unified Communications Manager for Phone and CSF. See the *Administration Guide for Cisco Unified Communications Manager* for more information.

Migrate Users via Bulk Administration

Move the users to a new cluster via the Bulk Administration Tool (for example, migrating from cluster 1 to cluster 2).

**Before you begin**

The **Cisco Bulk Provisioning Service** must be running in both clusters.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Export Users to CSV File, on page 247</td>
<td>In the original cluster (cluster 1) export the migrating users to a CSV file.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Download CSV Export File, on page 247</td>
<td>Download the CSV export file.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Upload CSV Export File to New Cluster, on page 247</td>
<td>Upload the CSV file to the destination cluster (cluster 2).</td>
</tr>
<tr>
<td><strong>Step 4</strong> Configure User Template, on page 248</td>
<td>In the destination cluster, configure a User Template with the user settings.</td>
</tr>
<tr>
<td><strong>Step 5</strong> Import Users to New Cluster, on page 248</td>
<td>Use the Insert Users menu in Bulk Administration to import users from the CSV file.</td>
</tr>
</tbody>
</table>
Export Users to CSV File

In the original cluster, use the Bulk Administration Tool to export the users whom you want to migrate to a CSV file.

Note: After the job runs, you can go to the Job Scheduler to check the status of the job and confirm that the file was created. If you selected Run Later, you can use the Job Scheduler to set the time for the job to run.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Bulk Administration > Users > Export Users**.
Step 2 Use the **Filter** tools to search for and select the users whom you want to migrate and click **Find**.
Step 3 Click **Next**.
Step 4 Enter a **File Name** for the file. The tool appends the `.txt` extension to the end of your file. For example, `<csvfilename>.txt`.
Step 5 From the **File Format** drop-down, select the format of the export file.
Step 6 To run the job right away, select **Run Immediately** and click **Submit**.

What to do next

After the job runs, you can go to the **Job Scheduler** to check the status of the job and confirm that the file was created. If you selected **Run Later**, you can use the Job Scheduler to set the time for the job to run.

Once you have confirmed that the file was created, **Download CSV Export File**, on page 247.

Download CSV Export File

Once you have confirmed that the export file was created, download the file.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Bulk Administration > Upload/Download Files**.
Step 2 Click **Find**.
Step 3 Select the file that was created and click **Download Selected**.
Step 4 Download the file.

What to do next

**Upload CSV Export File to New Cluster**, on page 247

Upload CSV Export File to New Cluster

In the destination cluster (cluster 2), upload the csv file that you exported from cluster 1.
**Configure User Template**

In the destination cluster, configure a user template with the settings that you want to apply to imported users.

**Procedure**

**Step 1** From Cisco Unified CM Administration choose **Bulk Administration > Users > User Templates**.

**Step 2** Do either of the following:
- Click **Find** and select an existing template.
- Click **Add New** to create a new template.

**Step 3** Configure the user settings that you want to apply to your imported users. For example, make sure that the following fields are checked
  - **Home Cluster**
  - **Enable User for Unified CM IM and Presence**

**Step 4** If you want users to be enabled for calendar integration with Microsoft Outlook, check the **Include meeting information in Presence** check box.

**Step 5** Configure any remaining fields.

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

**What to do next**

Import Users to New Cluster, on page 248

---

**Import Users to New Cluster**

Use Bulk Administration's Insert Users menu to import the exported users into the new Cluster.
Import Contact Lists on Home Cluster

After you have migrated users to the new cluster, import the contact lists to restore contact data for the migrated users.

Procedure

Step 1 Upload the previously exported contact list CSV file.
   a) In Cisco Unified CM IM and Presence Administration, choose 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.
   h) Click Save to upload the file.

Step 2 Run the import contact list job.
   a) In Cisco Unified CM IM and Presence Administration, choose 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) In Cisco Unified CM IM and Presence Administration, choose Bulk Administration > Contact List > 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 time and end time of the job is listed and a result summary is also displayed.

---

**Update Users in Old Cluster**

You may not want to remove users from the old cluster until after you confirm that everything is working fine in the new cluster. Use this procedure to use Bulk Administration's Update Users feature to remove IM and Presence functionality from the old cluster.

**Procedure**

**Step 1**
From Cisco Unified CM Administration, choose **Bulk Administration > Users > Update Users > Query**.

**Step 2**
Use the Filter tools to search for the migrating users. For example, you can search for all users whom meet this condition: **Has IM and Presence Enabled**.

**Step 3**
Click **Next**.

**Step 4**
For each of the following two fields, check the far left box and leave the adjacent box on the right unchecked. The left box indicates that you want to update the field and the right box indicates the new setting: unchecked.

- **Home Cluster**
- **Enable User for Unified CM IM and Presence**

**Step 5**
Under **Job Information**, select **Run Immediately**.

**Step 6**
Click **Submit**.

**What to do next**
Once you are confident that the migration worked, and that all users are configured properly in the new cluster, you can delete migrated users in the old cluster.
CHAPTER 26

Manage Locales

- Manage Locales Overview, on page 251
- Manage Locales Prerequisites, on page 252
- Install Locale Installer on IM and Presence Service, on page 252

Manage Locales Overview

You can configure Cisco Unified Communications Manager and IM and Presence Service to support multiple languages. There is no limit to the number of supported languages you can install.

Cisco provides locale-specific versions of the Cisco Unified Communications Manager Locale Installer and the IM and Presence Service Locale Installer on www.cisco.com. Installed by the system administrator, the locale installer allows the user to view/receive the chosen translated text or tones, if applicable, when a user works with supported interfaces.

After you upgrade Cisco Unified Communications Manager or the IM & Presence Service, you must reinstall all the locales. Install the latest version of the locales that match the major.minor version number of your Cisco Unified Communications Manager node or IM and Presence Service node.

Install locales after you have installed Cisco Unified Communications Manager on every node in the cluster and have set up the database. If you want to install specific locales on IM and Presence Service nodes, you must first install the Cisco Unified Communications Manager locale file for the same country on the Cisco Unified Communications Manager cluster.

Use the information in the following sections to install locales on Cisco Unified Communications Manager nodes and on IM and Presence Service nodes after you complete the software upgrade.

User Locales

User locale files contain language information for a specific language and country. They provide translated text and voice prompts, if available, for phone displays, user applications, and user web pages in the locale that the user chooses. These files use the following naming convention:

- cm-locale-language-country-version.cop (Cisco Unified Communications Manager)
- ps-locale-language_country-version.cop (IM and Presence Service)

If your system requires user locales only, install them after you have installed the CUCM locale.
Network Locales

Network locale files provide country-specific files for various network items, including phone tones, annunciators, and gateway tones. The combined network locale file uses the following naming convention:

- cm-locale-combinednetworklocale-version.cop (Cisco Unified Communications Manager)

Cisco may combine multiple network locales in a single locale installer.

Note

Cisco Unified Communications Manager and IM and Presence Service on Cisco-approved, customer-provided servers can support multiple locales. Installing multiple locale installers ensures that the user can choose from a multitude of locales.

You can install locale files from either a local or a remote source by using the same process for installing software upgrades. You can install more than one locale file on each node in the cluster. Changes do not take effect until you reboot every node in the cluster. Cisco strongly recommends that you do not reboot the nodes until you have installed all locales on all nodes in the cluster. Minimize call-processing interruptions by rebooting the nodes after regular business hours.

Manage Locales Prerequisites

Locale Installation Considerations

- Install all of the Cisco Unified Communications Manager and IM and Presence Service cluster nodes and set up the database before you install locales.

- If you want to install specific locales on IM and Presence Service nodes, you must first install the Cisco Unified Communications Manager locale file for the same country on the Cisco Unified Communications Manager cluster.

- You can install more than one locale file on each node in the cluster. To activate the new locale, you must restart each node in the cluster after installation.

- You can install locale files from either a local or a remote source by using the same process for installing software upgrades. See the Upgrade Guide for Cisco Unified Communications Manager for more information about upgrading from a local or a remote source.

Install Locale Installer on IM and Presence Service

- Install the Locale Installer on Cisco Unified Communications Manager before you install locales for IM and Presence Service. If you want to use a locale other than English, you must install the appropriate language installers on both Cisco Unified Communications Manager and on IM and Presence Service.

- If your IM and Presence Service cluster has more than one node, make sure that the locale installer is installed on every node in the cluster (install on the IM and Presence database publisher node before the subscriber nodes).
• User locales should not be set until all appropriate locale installers are loaded on both systems. Users may experience problems if they inadvertently set their user locale after the locale installer is loaded on Cisco Unified Communications Manager but before the locale installer is loaded on IM and Presence Service. If issues are reported, we recommend that you notify each user to sign into the Cisco Unified Communications Self Care Portal and change their locale from the current setting to English and then back again to the appropriate language. You can also use the BAT tool to synchronize user locales to the appropriate language.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Navigate to <a href="http://software.cisco.com/download/navigator.html?mdfid=285971059">cisco.com</a> and choose the locale installer for your version of IM and Presence Service.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the version of the IM and Presence Locale Installer that is appropriate for your working environment.</td>
</tr>
<tr>
<td>Step 3</td>
<td>After downloading the file, save the file to the hard drive and note the location of the saved file.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Copy this file to a server that supports SFTP.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Sign into Cisco Unified IM and Presence Operating System Administration using the administrator account and password.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Choose <strong>Software Upgrades &gt; Install/Upgrade</strong>.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Choose Remote File System as the software location source.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Enter the file location, for example <code>/tmp</code>, in the Directory field.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Enter the IM and Presence Service server name in the Server field.</td>
</tr>
<tr>
<td>Step 10</td>
<td>Enter your username and password credentials in the User Name and User Password fields.</td>
</tr>
<tr>
<td>Step 11</td>
<td>Choose SFTP for the Transfer Protocol.</td>
</tr>
<tr>
<td>Step 12</td>
<td>Click Next.</td>
</tr>
<tr>
<td>Step 13</td>
<td>Choose the IM and Presence Service locale installer from the list of search results.</td>
</tr>
<tr>
<td>Step 14</td>
<td>Click Next to load the installer file and validate it.</td>
</tr>
<tr>
<td>Step 15</td>
<td>After you complete the locale installation, restart each server in the cluster.</td>
</tr>
<tr>
<td>Step 16</td>
<td>The default setting for installed locales is &quot;English, United States&quot;. 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.</td>
</tr>
<tr>
<td>Step 17</td>
<td>Verify that your users can choose the locales for supported products.</td>
</tr>
</tbody>
</table>

**Tip** Make sure that you install the same components on every server in the cluster.

---

**Error Messages Locales Reference**

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>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[LOCALE] File not found: <code>&lt;language&gt;_&lt;country&gt;_user_locale.csv</code>, the user locale has not been added to the database.</td>
<td>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.</td>
</tr>
<tr>
<td>[LOCALE] File not found: <code>&lt;country&gt;_network_locale.csv</code>, the network locale has not been added to the database.</td>
<td>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.</td>
</tr>
<tr>
<td>[LOCALE] CSV file installer installdb is not present or not executable</td>
<td>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.</td>
</tr>
<tr>
<td>[LOCALE] Could not create `/usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maDialogs_&lt;ll&gt;_&lt;CC&gt;.properties.Checksum.</td>
<td>These errors could occur when the system fails to create a checksum file, which an absent Java executable, <code>/usr/local/thirdparty/java/j2sdk/jre/bin/java</code>, an absent or damaged Java archive file, <code>/usr/local/cm/jar/cmutil.jar</code>, or an absent or damaged Java class, <code>com.cisco.ccm.util.Zipper</code>, causes. Even if these errors occur, the locale will continue to work correctly, with the exception of Cisco Unified Communications Manager Assistant, which cannot detect a change in localized Cisco Unified Communications Manager Assistant files.</td>
</tr>
<tr>
<td>[LOCALE] Could not find <code>/usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt</code> in order to update Unified CM Assistant locale information.</td>
<td>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.</td>
</tr>
<tr>
<td>[LOCALE] Addition of <code>&lt;locale-installer-file-name&gt;</code> to the database has failed!</td>
<td>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.</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>[LOCALE] Could not locate <code>&lt;locale-installer-file-name&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td>[LOCALE] Could not copy <code>&lt;locale-installer-file-name&gt;</code> to migratory path. This locale will not be migrated during an upgrade!</td>
<td>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.</td>
</tr>
<tr>
<td>[LOCALE] DRS unregistration failed</td>
<td>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.</td>
</tr>
<tr>
<td>[LOCALE] Backup failed!</td>
<td>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. <strong>Note</strong> Manually reinstalling locales after a system restore achieves the same goal.</td>
</tr>
<tr>
<td>[LOCALE] No COP files found in restored tarball!</td>
<td>Corruption of backup files may prevent successful extraction of locale installer files. <strong>Note</strong> Manual reapplication of the locale installer will restore the locale fully.</td>
</tr>
<tr>
<td>[LOCALE] Failed to successfully reinstall COP files!</td>
<td>Corruption of backup files may damage locale installer files. <strong>Note</strong> Manual reapplication of the locale installer will restore the locale fully.</td>
</tr>
<tr>
<td>[LOCALE] Failed to build script to reinstall COP files!</td>
<td>The platform could not dynamically create the script used to reinstall locales. <strong>Note</strong> Manual reapplication of the locale installer will restore the locale fully. Record the installation log and contact TAC.</td>
</tr>
</tbody>
</table>
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 28: List of Localized Applications and Supported Languages

<table>
<thead>
<tr>
<th>Interface</th>
<th>Supported Languages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Applications</td>
<td></td>
</tr>
<tr>
<td>Cisco Unified CM IM and Presence Administration</td>
<td>Chinese (China), English, Japanese (Japan), Korean (Korean Republic)</td>
</tr>
<tr>
<td>Cisco Unified IM and Presence Operating System</td>
<td>Chinese (China), English, Japanese (Japan), Korean (Korean Republic)</td>
</tr>
</tbody>
</table>


## Manage the Server

- Manage the Server Overview, on page 257
- Changing the Server Address, on page 257
- Remove Node From Cluster, on page 258
- Add Deleted Server Back in to Cluster, on page 258
- Add Node to Cluster Before Install, on page 259
- View Presence Server Status, on page 260
- Restarting Services with High Availability, on page 260
- Hostname Configuration, on page 261

### Manage the Server Overview

This chapter contains information on how to edit server details for a deployed system. This includes assigning a new node to a cluster, removing a node from a cluster, viewing the presence status and changing server address details.

### Changing the Server Address

If you have an up and running system, and you need to make any of the following changes to the server addressing, refer to the procedures in the document Changing the IP Address and Hostname for Cisco Unified Communications Manager and the IM and Presence Service at [https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html](https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html).

This applies to the following types of address changes:

- Changing the server IP Address
- Changing the server hostname
- Changing the node name (for example, if you are using an IP address to define the node name and you want to use a hostname instead).
- Changing the default domain for the IM and Presence Service
Remove Node From Cluster

Follow this procedure if you need to safely remove an IM and Presence Service node from its presence redundancy group.

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

Procedure

Step 1
On the Cisco Unified CM Administration > System > Presence Redundancy Groups page, disable High Availability if it is enabled.

Step 2
On the Cisco Unified CM Administration > User Management > Assign Presence Users page, unassign or move all the users off the node that you want to remove.

Step 3
To remove the node from its presence redundancy group, choose Not-Selected from the Presence Server drop down list on the presence redundancy group's Presence Redundancy Group Configuration page. Select OK when a warning dialog box indicates that services in the presence redundancy group will be restarted as a result of unassigning the node.

Step 4
Delete the unassigned node from the Cisco Unified CM Administration > System > Server page. Select OK when a warning dialog box indicates that this action cannot be undone.

Step 5
Shut down the host VM or server for the node you have unassigned.

Add Deleted Server Back in to Cluster

If you delete a subsequent node (subscriber) from Cisco Unified Communications Manager Administration and you want to add it back to the cluster, perform the following procedure.

Procedure

Step 1
In Cisco Unified Communications Manager Administration, add the server by choosing System > Server.

Step 2
After you add the subsequent node to Cisco Unified Communications Manager Administration, perform an installation on the server by using the disk that Cisco provided in the software kit for your version.

Tip
Make sure that the version that you install matches the version that runs on the publisher node. If the version that is running on the publisher does not match your installation file, choose the Upgrade During Install option during the installation process. For details, see the Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service.

Step 3
After you install Cisco Unified CM, configure the subsequent node, as described in the installation documentation that supports your version of Cisco Unified CM.
Step 4  Access the Cisco Unified Reporting, RTMT, or the CLI to verify that database replication is occurring between existing nodes; if necessary, repair database replication between the nodes.

---

**Add Node to Cluster Before Install**

Use Cisco Unified Communications Manager Administration to add a new node to a cluster before installing the node. The server type you select when adding the node must match the server type you install.

You must configure a new node on the first node using Cisco Unified Communications Manager Administration before you install the new node. To install a node on a cluster, see the *Cisco Unified Communications Manager Installation Guide*.

For Cisco Unified Communications Manager Video/Voice servers, the first server you add during an initial installation of the Cisco Unified Communications Manager software is designated the publisher node. All subsequent server installations or additions are designated as subscriber nodes. The first Cisco Unified Communications Manager IM and Presence node you add to the cluster is designated the IM and Presence Service database publisher node.

**Note**

You cannot use Cisco Unified Communications Manager Administration to change the server type after the server has been added. You must delete the existing server instance, and then add the new server again and choose the correct server type setting.

---

**Procedure**

**Step 1**  Select System > Server.

The **Find and List Servers** window displays.

**Step 2**  Click Add New.

The **Server Configuration - Add a Server** window displays.

**Step 3**  From the **Server Type** drop-down list box, choose the server type that you want to add, and then click **Next**.

- CUCM Video/Voice
- CUCM IM and Presence

**Step 4**  In the **Server Configuration** window, enter the appropriate server settings.

For server configuration field descriptions, see **Server Settings**.

**Step 5**  Click **Save**.
View Presence Server Status

Use Cisco Unified Communications Manager Administration to view the status of critical services and self-diagnostic test results for the IM and Presence Service node.

Procedure

Step 1  Select System > Server.
The Find and List Servers window appears.

Step 2  Select the server search parameters, and then click Find.
Matching records appear.

Step 3  Select the IM and Presence server that is listed in the Find and List Servers window.
The Server Configuration window appears.

Step 4  Click on the Presence Server Status link in the IM and Presence Server Information section of the Server Configuration window.
The Node Details window for the server appears.

Restarting Services with High Availability

If you make any system configuration changes, or system upgrades, that require you to disable High Availability and then restart either the Cisco XCP router, Cisco Presence Engine, or the server itself, you must allow sufficient time for Cisco Jabber sessions to be recreated before you enable High Availability. Otherwise, Presence won't work for Jabber clients whose sessions aren't created.

Make sure to follow this process:

Procedure

Step 1  Before you make any changes, check the Presence Topology window in Cisco Unified CM IM and Presence Administration window (System > Presence Topology). Take a record of the number of assigned users to each node in each Presence Redundancy Group.

Step 2  Disable High Availability in each Presence Redundancy Group and wait at least two minutes for the new HA settings to synchronize.

Step 3  Do whichever of the following is required for your update:

• Restart the Cisco XCP Router
• Restart the Cisco Presence Engine
• Restart the server

Step 4  After the restart, monitor the number of active sessions on all nodes.
Step 5  For each node, run the `show perf query counter "Cisco Presence Engine" ActiveJsmSessions` CLI command on each node to confirm the number of active sessions on each node. The number of active sessions should match the number that you recorded in step 1 for assigned users. It should take no more than 15 minutes for all sessions to resume.

Step 6  Once all of your sessions are created, you can enable High Availability within the Presence Redundancy Group.

**Note**  If 30 minutes passes and the active sessions haven't yet been created, restart the Cisco Presence Engine. If that doesn't work, there is a larger system issue for you to fix.

**Note**  It is not recommended to do back-to-back restarts of the Cisco XCP Router and/or Cisco Presence Engine. However, if you do need to do a restart: restart the first service, wait for all of the JSM sessions to be recreated. After all of the JSM sessions are created, then do the second restart.

### Hostname Configuration

The following table lists the locations where you can configure a host name for the Unified Communications Manager server, the allowed number of characters for the host name, and the recommended first and last characters for the host name. Be aware that, if you do not configure the host name correctly, some components in Unified Communications Manager, such as the operating system, database, installation, and so on, may not work as expected.

![Caution](image)

**Caution**  Before you change the host name or IP address for any locations that are listed in the following table, see the document *Changing the IP Address and Host Name for Cisco Unified Communications Manager*. Failing to update the host name or IP address correctly after it is configured may cause problems for Unified Communications Manager.

**Table 29: Host Name Configuration in Cisco Unified Communications Manager**

<table>
<thead>
<tr>
<th>Host Name Location</th>
<th>Allowed Configuration</th>
<th>Allowed Number of Characters</th>
<th>Recommended First Character for Host Name</th>
<th>Recommended Last Character for Host Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name/ IP Address field</td>
<td>You can add or change the host name for a server in the cluster.</td>
<td>2-63</td>
<td>alphabetic</td>
<td>alphanumeric</td>
</tr>
<tr>
<td>System &gt; Server in Cisco Unified Communications Manager Administration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hostname field Cisco Unified Communications Manager installation wizard</td>
<td>You can add the host name for a server in the cluster.</td>
<td>1-63</td>
<td>alphabetic</td>
<td>alphanumeric</td>
</tr>
</tbody>
</table>
### Host Name Location

<table>
<thead>
<tr>
<th>Hostname field Settings &gt; IP &gt; Ethernet in Cisco Unified Communications Operating System</th>
<th>Host Name Configuration</th>
<th>Allowed Number of Characters</th>
<th>Recommended First Character for Host Name</th>
<th>Recommended Last Character for Host Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname field Settings &gt; IP &gt; Ethernet in Cisco Unified Communications Operating System</td>
<td>You can change, not add, the host name for a server in the cluster.</td>
<td>1-63</td>
<td>alphabetic</td>
<td>alphanumeric</td>
</tr>
<tr>
<td>set network hostname hostname Command Line Interface</td>
<td>You can change, not add, the host name for a server in the cluster.</td>
<td>1-63</td>
<td>alphabetic</td>
<td>alphanumeric</td>
</tr>
</tbody>
</table>

#### Tip

The host name must follow the rules for ARPANET host names. Between the first and last character of the host name, you can enter alphanumeric characters and hyphens.

Before you configure the host name in any location, review the following information:

- The Host Name/IP Address field in the Server Configuration window, which supports device-to-server, application-to-server, and server-to-server communication, allows you to enter an IPv4 address in dotted decimal format or a host name.

After you install the Unified Communications Manager publisher node, the host name for the publisher automatically displays in this field. Before you install a Unified Communications Manager subscriber node, enter either the IP address or the host name for the subscriber node in this field on the Unified Communications Manager publisher node.

In this field, configure a host name only if Unified Communications Manager can access the DNS server to resolve host names to IP addresses; make sure that you configure the Cisco Unified Communications Manager name and address information on the DNS server.

#### Tip

In addition to configuring Unified Communications Manager information on the DNS server, you enter DNS information during the Cisco Unified Communications Manager installation.

- During the installation of the Unified Communications Manager publisher node, you enter the host name, which is mandatory, and IP address of the publisher node to configure network information; that is, if you want to use static networking.

During the installation of a Unified Communications Manager subscriber node, you enter the hostname and IP address of the Unified Communications Manager publisher node, so that Unified Communications Manager can verify network connectivity and publisher-subscriber validation. Additionally, you must enter the host name and the IP address for the subscriber node. When the Unified Communications Manager installation prompts you for the host name of the subscriber server, enter the value that displays in the Server Configuration window in Cisco Unified Communications Manager Administration; that is, if you configured a host name for the subscriber server in the Host Name/IP Address field.
Backup the System

- Backup Overview, on page 263
- Backup Prerequisites, on page 263
- Backup Task Flow, on page 264
- Backup Interactions and Restrictions, on page 269

Backup Overview

Cisco recommends performing regular backups. You can use the Disaster Recovery System (DRS) to do a full data backup for all servers in a cluster. You can set up automatic backups or invoke a backup at any time.

The Disaster Recovery System performs a cluster-level backup, which means that it collects backups for all servers in a Cisco Unified Communications Manager cluster to a central location and archives the backup data to physical storage device. Backup files are encrypted and can be opened only by the system software.

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

When you perform a system data restoration, you can choose which nodes in the cluster you want to restore.

The Disaster Recovery System includes the following capabilities:

- A user interface for performing backup and restore tasks.
- A distributed system architecture for performing backup functions.
- Scheduled backups or manual (user-invoked) backups.
- It archives backups to a remote sftp server.

Backup Prerequisites

- Make sure that you meet the version requirements:
  - All Cisco Unified Communications Manager cluster nodes must be running the same version of the Cisco Unified Communications Manager application.
• All IM and Presence Service cluster nodes must be running the same version of the IM and Presence Service application.

• The software version saved in the backup file must match the version that is running on the cluster nodes.

The entire version string must match. For example, if the IM and Presence database publisher node is at version 11.5.1.10000-1, then all IM and Presence subscriber nodes must be 11.5.1.10000-1, and the backup file must also be must be 11.5.1.10000-1. If you try to restore the system from a backup file that does not match the current version, the restore will fail. Ensure that you backup the system whenever you upgrade the software version so that the version saved in the backup file matches the version that is running on the cluster nodes.

• Be aware the DRS encryption depends on the cluster security password. When running the backup, DRS generates a random password for encryption and then encrypts the random password with the cluster security password. If the cluster security password ever gets changed between the backup and this restore, you will need to know what the password was at the time of the backup in order to use that backup file to restore your system or take a backup immediately after the security password change/reset.

• If you want to back up to a remote device, make sure that you have an SFTP server set up. For more information on the available SFTP servers, see SFTP Servers for Remote Backups, on page 270

Backup Task Flow

Complete these tasks to configure and run a backup. Do not perform any OS Administration tasks while a backup is running. This is because Disaster Recovery System blocks all OS Administration requests by locking platform API. However, Disaster Recovery System does not block most CLI commands, because only the CLI-based upgrade commands use the Platform API locking package.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Configure Backup Devices, on page 265</td>
<td>Specify the devices on which to back up data.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Estimate Size of Backup File, on page 266</td>
<td>Estimate size of backup file created on the SFTP device.</td>
</tr>
</tbody>
</table>
| **Step 3** Choose one of the following options:  
  • Configure a Scheduled Backup, on page 266  
  • Start a Manual Backup, on page 267 | Create a backup schedule to back up data on a schedule. Optionally, run a manual backup. |
| **Step 4** View Current Backup Status, on page 268 | Optional. Check the Status of the Backup. While a backup is running, you can check the status of the current backup job. |
| **Step 5** View Backup History, on page 269 | Optional. View Backup History |
Configure Backup Devices

You can configure up to 10 backup devices. Perform the following steps to configure the location where you want to store backup files.

Before you begin

- Ensure you have write access to the directory path in the SFTP server to store the backup file.
- Ensure that the username, password, server name, and directory path are valid as the DRS Master Agent validates the configuration of the backup device.

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

Procedure

Step 1
From Disaster Recovery System, select Backup > Backup Device.

Step 2
In the Backup Device List window, do either of the following:
- To configure a new device, click Add New.
- To edit an existing backup device, enter the search criteria, click Find, and Edit Selected.
- To delete a backup device, select it in the Backup Device list and click Delete Selected.

You cannot delete a backup device that is configured as the backup device in a backup schedule.

Step 3
Enter a backup name in the Backup Device Name field.

The backup device name contains only alphanumeric characters, spaces ( ), dashes (-) and underscores (_). Do not use any other characters.

Step 4
In the Select Destination area, under Network Directory perform the following:
- In the Host name/IP Address field, enter the hostname or IP address for the network server.
- In the Path name field, enter the directory path where you want to store the backup file.
- In the User name field, enter a valid username.
- In the Password field, enter a valid password.
- From the Number of backups to store on Network Directory drop-down list, choose the required number of backups.

Step 5
Click Save.

What to do next

Estimate Size of Backup File, on page 266
Estimate Size of Backup File

Cisco Unified Communications Manager will estimate the size of the backup tar, only if a backup history exists for one or more selected features.

The calculated size is not an exact value but an estimated size of the backup tar. Size is calculated based on the actual backup size of a previous successful backup and may vary if the configuration changed since the last backup.

You can use this procedure only when the previous backups exist and not when you back up the system for the first time.

Follow this procedure to estimate the size of the backup tar that is saved to a SFTP device.

**Procedure**

**Step 1** From the Disaster Recovery System, select **Backup > Manual Backup**.

**Step 2** In the **Select Features** area, select the features to back up.

**Step 3** Click **Estimate Size** to view the estimated size of backup for the selected features.

**What to do next**

Perform one of the following procedures to backup your system:

- Configure a Scheduled Backup, on page 266
- Start a Manual Backup, on page 267

Configure a Scheduled Backup

You can create up to 10 backup schedules. Each backup schedule has its own set of properties, including a schedule for automatic backups, the set of features to back up, and a storage location.

Be aware that your backup .tar files are encrypted by a randomly generated password. This password is then encrypted by using the cluster security password and gets saved along with the backup .tar files. You must remember this security password or take a backup immediately after the security password change or reset.

**Caution**

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

**Before you begin**

Configure Backup Devices, on page 265

**Procedure**

**Step 1** From the Disaster Recovery System, choose **Backup Scheduler**.

**Step 2** In the **Schedule List** window, do one of the following steps to add a new schedule or edit an existing schedule.
To create a new schedule, click **Add New**.
To configure an existing schedule, click the name in the Schedule List column.

**Step 3**

In the **scheduler** window, enter a schedule name in the **Schedule Name** field.

**Note**
You cannot change the name of the default schedule.

**Step 4**

Select the backup device in the **Select Backup Device** area.

**Step 5**

Select the features to back up in the **Select Features** area. You must choose at least one feature.

**Step 6**

Choose the date and time when you want the backup to begin in the **Start Backup at** area.

**Step 7**

Choose the frequency at which you want the backup to occur in the **Frequency** area. The frequency can be set to Once Daily, Weekly, and Monthly. If you choose **Weekly**, you can also choose the days of the week when the backup will occur.

**Tip**
To set the backup frequency to **Weekly**, occurring Tuesday through Saturday, click **Set Default**.

**Step 8**

To update these settings, click **Save**.

**Step 9**

Choose one of the following options:

- To enable the selected schedules, click **Enable Selected Schedules**.
- To disable the selected schedules, click **Disable Selected Schedules**.
- To delete the selected schedules, click **Delete Selected**.

**Step 10**

To enable the schedule, click **Enable Schedule**.

The next backup occurs automatically at the time that you set.

**Note**
Ensure that all servers in the cluster are running the same version of Cisco Unified Communications Manager or Cisco IM and Presence Service and are reachable through the network. Servers that are not reachable at the time of the scheduled backup will not get backed up.

**What to do next**

Perform the following procedures:

- **Estimate Size of Backup File**, on page 266
- (Optional) **View Current Backup Status**, on page 268

**Start a Manual Backup**

**Before you begin**

- Ensure that you use a network device as the storage location for the backup files. Virtualized deployments of Unified Communications Manager do not support the use of tape drives to store backup files.
- Ensure that all cluster nodes have the same installed version of Cisco Unified Communications Manager or IM and Presence Service.
The backup process can fail due to non availability of space on a remote server or due to interruptions in the network connectivity. You need to start a fresh backup after addressing the issues that caused the backup to fail.

- Ensure that there are no network interruptions.

- **Configure Backup Devices, on page 265**

- **Estimate Size of Backup File, on page 266**

- Make sure that you have a record of the cluster security password. If the cluster security password changes after you complete this backup, you will need to know the password or you will not be able to use the backup file to restore your system.

Note

While a backup is running, you cannot perform any tasks in Cisco Unified OS Administration or Cisco Unified IM and Presence OS Administration because Disaster Recovery System locks the platform API to block all requests. However, Disaster Recovery System does not block most CLI commands because only the CLI-based upgrade commands use the Platform API locking package.

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the Disaster Recovery System, select <strong>Backup &gt; Manual Backup</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the <strong>Manual Backup</strong> window, select a backup device from the <strong>Backup Device Name</strong> area.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose a feature from the <strong>Select Features</strong> area.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Start Backup</strong>.</td>
</tr>
</tbody>
</table>

### What to do next

(Optional) **View Current Backup Status, on page 268**

### View Current Backup Status

Perform the following steps to check the status of the current backup job.

Caution

Be aware that if the backup to the remote server is not completed within 20 hours, the backup session times out and you must begin a fresh backup.

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the Disaster Recovery System, select <strong>Backup &gt; Current Status</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>To view the backup log file, click the log filename link.</td>
</tr>
<tr>
<td>Step 3</td>
<td>To cancel the current backup, click <strong>Cancel Backup</strong>.</td>
</tr>
</tbody>
</table>
The backup cancels after the current component completes its backup operation.

What to do next
View Backup History, on page 269

View Backup History

Perform the following steps to view the backup history.

Procedure

Step 1 From the Disaster Recovery System, select Backup > History.
Step 2 From the Backup History window, you can view the backups that you have performed, including filename, backup device, completion date, result, version, features that are backed up, and failed features.

Note The Backup History window displays only the last 20 backup jobs.

Backup Interactions and Restrictions

- Backup Restrictions, on page 269

Backup Restrictions

The following restrictions apply to backups:

Table 30: Backup Restrictions

<table>
<thead>
<tr>
<th>Restriction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Security Password</td>
<td>We recommend that you run a backup whenever you change the cluster security password. Backup encryption uses the cluster security password to encrypt data on the backup file. If you edit the cluster security password after a backup file is created, you will not be able to use that backup file to restore data unless you remember the old password.</td>
</tr>
</tbody>
</table>
The Disaster Recovery System (DRS) uses an SSL-based communication between the Master Agent and the Local Agent for authentication and encryption of data between the Cisco Unified Communications Manager cluster nodes. DRS makes use of the IPsec certificates for its Public/Private Key encryption. Be aware that if you delete the IPSEC truststore(hostname.pem) file from the Certificate Management pages, then DRS will not work as expected. If you delete the IPSEC-trust file manually, you must ensure that you upload the IPSEC certificate to the IPSEC-trust. For more details, see the “Certificate management” section in the Security Guide for Cisco Unified Communications Manager at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

<table>
<thead>
<tr>
<th>Restriction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Management</td>
<td>The Disaster Recovery System (DRS) uses an SSL-based communication between the Master Agent and the Local Agent for authentication and encryption of data between the Cisco Unified Communications Manager cluster nodes. DRS makes use of the IPsec certificates for its Public/Private Key encryption. Be aware that if you delete the IPSEC truststore(hostname.pem) file from the Certificate Management pages, then DRS will not work as expected. If you delete the IPSEC-trust file manually, you must ensure that you upload the IPSEC certificate to the IPSEC-trust. For more details, see the “Certificate management” section in the Security Guide for Cisco Unified Communications Manager at <a href="http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html">http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html</a>.</td>
</tr>
</tbody>
</table>

SFTP Servers for Remote Backups

To back up data to a remote device on the network, you must have an SFTP server that is configured. For internal testing, Cisco uses the SFTP Server on Cisco Prime Collaboration Deployment (PCD) which is provided by Cisco, and which is supported by Cisco TAC. Refer to the following table for a summary of the SFTP server options:

Use the information in the following table to determine which SFTP server solution to use in your system.

**Table 31: SFTP Server Information**

<table>
<thead>
<tr>
<th>SFTP Server</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFTP Server on Cisco Prime Collaboration Deployment</td>
<td>This server is the only SFTP server that is provided and tested by Cisco, and fully supported by Cisco TAC. Version compatibility depends on your version of Unified Communications Manager and Cisco Prime Collaboration Deployment. See the Cisco Prime Collaboration Deployment Administration Guide before you upgrade its version (SFTP) or Unified Communications Manager to ensure that the versions are compatible.</td>
</tr>
<tr>
<td>SFTP Server from a Technology Partner</td>
<td>These servers are third party provided and third party tested. Version compatibility depends on the third party test. See the Technology Partner page if you upgrade their SFTP product and/or upgrade Unified Communications Manager for which versions are compatible: <a href="https://marketplace.cisco.com">https://marketplace.cisco.com</a></td>
</tr>
</tbody>
</table>
SFTP Server | Information
---|---
SFTP Server from another Third Party | These servers are third party provided and are not officially supported by Cisco TAC.

Version compatibility is on a best effort basis to establish compatible SFTP versions and Unified Communications Manager versions.

**Note** These products have not been tested by Cisco and we cannot guarantee functionality. Cisco TAC does not support these products. For a fully tested and supported SFTP solution, use Cisco Prime Collaboration Deployment or a Technology Partner.

**Cipher Support**

For Unified Communications Manager 11.5 and earlier versions, Unified Communications Manager advertises the following CBC ciphers for SFTP connections:

- aes128-cbc
- 3des-cbc
- blowfish-cbc

**Note** Make sure that the backup SFTP Server supports one of these CBC ciphers to communicate with Unified Communications Manager.

From Unified Communications Manager 12.0 release onwards, CBC ciphers are not supported. Unified Communications Manager supports and advertises only the following CTR ciphers:

- aes256-ctr
- aes128-ctr
- aes192-ctr

**Note** Make sure that the backup SFTP Server supports one of these CTR ciphers to communicate with Unified Communications Manager.
Restore the System

- Restore Overview, on page 273
- Restore Prerequisites, on page 274
- Restore Task Flow, on page 274
- Data Authentication, on page 282
- Alarms and Messages, on page 284
- Restore Interactions and Restrictions, on page 287
- Troubleshooting, on page 288

Restore Overview

The Disaster Recovery System (DRS) provides a wizard to walk you through the process of restoring your system.

The backup files are encrypted and only the DRS system can open them to restore the data. The Disaster Recovery System includes the following capabilities:

- A user interface for performing restore tasks.
- A distributed system architecture for performing restore functions.

Master Agent

The system automatically starts the Master Agent service on each node of the cluster, but the Master Agent is functional only on the publisher node. The Master Agents on the subscriber nodes do not perform any functions.

Local Agents

The server has a Local Agent to perform backup and restore functions.

Each node in a Cisco Unified Communications Manager cluster, including the node that contains the Master Agent, must have its own Local Agent to perform backup and restore functions.
By default, a Local Agent automatically gets started on each node of the cluster, including IM and Presence nodes.

### Restore Prerequisites

- Make sure that you meet the version requirements:
  - All Cisco Unified Communications Manager cluster nodes must be running the same version of the Cisco Unified Communications Manager application.
  - All IM and Presence Service cluster nodes must be running the same version of the IM and Presence Service application.
  - The version saved in the backup file must match the version that is running on the cluster nodes.

The entire version string must match. For example, if the IM and Presence database publisher node is at version 11.5.1.10000-1, then all IM and Presence subscriber nodes must be 11.5.1.10000-1, and the backup file must also be must be 11.5.1.10000-1. If you try to restore the system from a backup file that does not match the current version, the restore will fail.

- Make sure that the IP address, hostname, DNS configuration and deployment type for the server matches the IP address, hostname, DNS configuration and deployment type that are stored on the backup file.
- If you have changed the cluster security password since the backup was run, make sure that you have a record of the old password, or the restore will fail.

### Restore Task Flow

During the restore process, do not perform any tasks with Cisco Unified Communications Manager OS Administration or Cisco Unified IM and Presence OS Administration.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>Restore the First Node Only, on page 275</strong></td>
<td>(Optional) Use this procedure only to restore the first publisher node in the cluster.</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>Restore Subsequent Cluster Node, on page 276</strong></td>
<td>(Optional) Use this procedure to restore the subscriber nodes in a cluster.</td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>Restore Cluster in One Step After Publisher Rebuilds, on page 278</strong></td>
<td>(Optional) Follow this procedure to restore the entire cluster in one step if the publisher has already been rebuilt.</td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>Restore Entire Cluster, on page 279</strong></td>
<td>(Optional) Use this procedure to restore all nodes in the cluster, including the publisher node. If a major hard drive failure or upgrade</td>
</tr>
</tbody>
</table>
Restore the First Node Only

If you are restoring the first node after a rebuild, you must configure the backup device.

This procedure is applicable to the Cisco Unified Communications Manager First Node, also known as the publisher node. The other Cisco Unified Communications Manager nodes and all the IM and Presence Service nodes are considered as secondary nodes or subscribers.

Before you begin

If there is an IM and Presence Service node in the cluster, ensure that it is running and accessible when you restore the first node. This is required so that a valid backup file can be found during the procedure.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>Restore Node Or Cluster to Last Known Good Configuration, on page 280</td>
<td>(Optional) Use this procedure only if you are restoring a node to a last known good configuration. Do not use this after a hard drive failure or other hardware failure.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Restart a Node, on page 281</td>
<td>Use this procedure to restart a node.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Check Restore Job Status, on page 282</td>
<td>(Optional) Use this procedure to check the restore job status.</td>
</tr>
<tr>
<td>Step 8</td>
<td>View Restore History, on page 282</td>
<td>(Optional) Use this procedure to view the restore history.</td>
</tr>
</tbody>
</table>

Restore the First Node Only

If you are restoring the first node after a rebuild, you must configure the backup device.

This procedure is applicable to the Cisco Unified Communications Manager First Node, also known as the publisher node. The other Cisco Unified Communications Manager nodes and all the IM and Presence Service nodes are considered as secondary nodes or subscribers.

Before you begin

If there is an IM and Presence Service node in the cluster, ensure that it is running and accessible when you restore the first node. This is required so that a valid backup file can be found during the procedure.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the Disaster Recovery System, choose Restore &gt; Restore Wizard.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Restore Wizard Step 1 window, Select Backup Device area, select the appropriate backup device to restore.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Next.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Restore Wizard Step 2 window, select the backup file you want to restore.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>The backup filename indicates the date and time that the system created the backup file.</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Next.</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>In the Restore Wizard Step 3 window, click Next.</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>Choose the features that you want to restore.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>The features that you have selected for backup will be displayed.</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>Select the node to restore.</td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td>Click Restore to restore the data.</td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td>Click Next.</td>
<td></td>
</tr>
</tbody>
</table>
Step 11  When you are prompted to select the nodes to restore, choose only the first node (the publisher).

Caution  Do not select the subsequent (subscriber) nodes in this condition as this will result in failure of the restore attempt.

Step 12  (Optional) From the Select Server Name drop-down list, select the subscriber node from which you want to restore the publisher database. Ensure that the subscriber node that you chose is in-service and connected to the cluster.

The Disaster Recovery System restores all non-database information from the backup file and pulls the latest database from the chosen subscriber node.

Note  This option appears only if the backup file that you selected includes the CCMDB database component. Initially, only the publisher node is fully restored, but when you perform Step 14 and restart the subsequent cluster nodes, the Disaster Recovery System performs database replication and fully synchronizes all cluster node databases. This ensures that all cluster nodes are using current data.

Step 13  Click Restore.

Step 14  Your data is restored on the publisher node. Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore.

Note  Restoring the first node restores the whole Cisco Unified Communications Manager database to the cluster. This may take up to several hours based on number of nodes and size of database that is being restored. Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore.

Step 15  When the Percentage Complete field on the Restore Status window, shows 100%, restart the server. Restart of all the nodes in the cluster is required in case of restoring only to the first node. Ensure that you restart the first node before you restart the subsequent nodes. For information about how to restart the server, see the What to Do Next section.

Note  If you are restoring a Cisco Unified Communications Manager node only, the Cisco Unified Communications Manager and IM and Presence Service cluster must be restarted.

If you are restoring an IM and Presence Service Publisher node only, the IM and Presence Service cluster must be restarted.

What to do next

• (Optional) To view the status of the restore, see Check Restore Job Status, on page 282

• To restart a node, see Restart a Node, on page 281

Restore Subsequent Cluster Node

This procedure is applicable to the Cisco Unified Communications Manager subscriber (subsequent) nodes only. The first Cisco Unified Communications Manager node installed is the publisher node. All other Cisco Unified Communications Manager nodes, and all IM and Presence Service nodes are subscriber nodes.
Follow this procedure to restore one or more Cisco Unified Communications Manager subscriber nodes in the cluster.

**Before you begin**

Before you perform a restore operation, ensure that the hostname, IP address, DNS configuration, and deployment type of the restore matches the hostname, IP address, DNS configuration, and deployment type of the backup file that you want to restore. Disaster Recovery System does not restore across different hostnames, IP addresses, DNS configurations and deployment types.

Ensure that the software version that is installed on the server matches the version of the backup file that you want to restore. Disaster Recovery System supports only matching software versions for restore operations. If you are restoring the subsequent nodes after a rebuild, you must configure the backup device.

**Procedure**

**Step 1** From the Disaster Recovery System, select **Restore > Restore Wizard**.

**Step 2** In the **Restore Wizard Step 1** window, **Select Backup Device** area, choose the backup device from which to restore.

**Step 3** Click **Next**.

**Step 4** In the **Restore Wizard Step 2** window, select the backup file that you want to restore.

**Step 5** Click **Next**.

**Step 6** In the **Restore Wizard Step 3** window, select the features that you want to restore.

*Note* Only the features that were backed up to the file that you chose display.

**Step 7** Click **Next**. The Restore Wizard Step 4 window displays.

**Step 8** In the **Restore Wizard Step 4** window, when you are prompted to choose the nodes to restore, select only the subsequent nodes.

**Step 9** Click **Restore**.

**Step 10** Your data is restored on the subsequent nodes. For more information about how to view the status of the restore, see the What to Do Next section.

*Note* During the restore process, do not perform any tasks with Cisco Unified Communications Manager Administration or User Options.

**Step 11** When the **Percentage Complete** field on the **Restore Status** window shows 100%, restart the secondary servers you just restored. Restart of all the nodes in the cluster is required in case of restoring only to the first node. Ensure that you restart the first node before you restart the subsequent nodes. For information about how to restart the server, see the What to Do Next section.

*Note* If the IM and Presence Service first node is restored. Ensure to restart the IM and Presence Service first node before you restart the IM and Presence Service subsequent nodes.

**What to do next**

* (Optional) To view the status of the restore, see **Check Restore Job Status**, on page 282
• To restart a node, see Restart a Node, on page 281

## Restore Cluster in One Step After Publisher Rebuilds

Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore. Follow this procedure to restore the entire cluster in one step if the publisher has already been rebuilt or freshly installed.

### Procedure

**Step 1** From the Disaster Recovery System, select **Restore > Restore Wizard**.

**Step 2** In the **Restore Wizard Step 1** window **Select Backup Device** area, choose the backup device from which to restore.

**Step 3** Click **Next**.

**Step 4** In the **Restore Wizard Step 2** window, select the backup file that you want to restore.

The backup filename indicates the date and time that the system created the backup file.

Choose only the backup file of the cluster from which you want to restore the entire cluster.

**Step 5** Click **Next**.

**Step 6** In the **Restore Wizard Step 3** window, select the features that you want to restore.

The screen displays only those features that were saved to the backup file.

**Step 7** Click **Next**.

**Step 8** In the **Restore Wizard Step 4** window, click **One-Step Restore**.

This option appears on **Restore Wizard Step 4** window only if the backup file selected for restore is the backup file of the cluster and the features chosen for restore includes the feature(s) that is registered with both publisher and subscriber nodes. For more information, see Restore the First Node Only, on page 275 and Restore Subsequent Cluster Node, on page 276.

**Note** If a status message indicates that Publisher has failed to become cluster aware. Cannot start one-step restore, you need to restore the publisher node and then the subscriber node. See the Related topics for more information.

This option allows the publisher to become cluster aware and will take five minutes to do so. Once you click on this option, a status message displays as “Please wait for 5 minutes until Publisher becomes cluster aware and do not start any backup or restore activity in this time period”.

After the delay, if the publisher becomes cluster aware, a status message displays as “Publisher has become cluster aware. Please select the servers and click on Restore to start the restore of entire cluster”.

After the delay, if the publisher has not become cluster aware, a status message displays as "Publisher has failed to become cluster aware. Cannot start one-step restore. Please go ahead and do a normal two-step restore." To restore the whole cluster in two-step (publisher and then subscriber), perform the steps mentioned in Restore the First Node Only, on page 275 and Restore Subsequent Cluster Node, on page 276.

**Step 9** When you are prompted to choose the nodes to restore, choose all the nodes in the cluster.
The Disaster Recovery System restores the Cisco Unified Communications Manager database (CCMDB) on subsequent nodes automatically when you restore a first node. This may take up to several hours based on number of nodes and size of that database that is being restored.

**Step 10**
Click **Restore**.
Your data is restored on all the nodes of the cluster.

**Step 11**
When the **Percentage Complete** field on the **Restore Status window** shows 100%, restart the server. Restart of all the nodes in the cluster is required in case of restoring only to the first node. Ensure that you restart the first node before you restart the subsequent nodes. For information about how to restart the server, see the What to Do Next section.

---

**What to do next**
- (Optional) To view the status of the restore, see Check Restore Job Status, on page 282
- To restart a node, see Restart a Node, on page 281

---

**Restore Entire Cluster**

If a major hard drive failure or upgrade occurs, or in the event of a hard drive migration, you have to rebuild all nodes in the cluster. Follow these steps to restore an entire cluster.

If you are doing most other types of hardware upgrades, such as replacing a network card or adding memory, you do not need to perform this procedure.

**Procedure**

**Step 1**
From Disaster Recovery System, select **Restore > Restore Wizard**.

**Step 2**
In the **Select Backup Device** area, select the appropriate backup device to restore.

**Step 3**
Click **Next**.

**Step 4**
In the **Restore Wizard Step 2** window, select the backup file you want to restore.

**Note**
The backup filename indicates the date and time that the system created the backup file.

**Step 5**
Click **Next**.

**Step 6**
In the **Restore Wizard Step 3** window, click **Next**.

**Step 7**
In the **Restore Wizard Step 4** window, select all the nodes when prompted to choose restore nodes.

**Step 8**
Click **Restore** to restore the data.

The Disaster Recovery System restores the Cisco Unified Communications Manager database (CCMDB) on subsequent nodes automatically when you restore a first node. This may take up to several hours based on number of nodes and size of that database.

Data is restored on all the nodes.
During the restore process, do not perform any tasks with Cisco Unified Communications Manager Administration or User Options.

Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore.

**Step 9** Restart the server once the restoration process is completed. See the What to Do Next section for more information about how to restart the server.

**Note** Make sure that you restart the first node before you restart the subsequent nodes.

After the first node has restarted and is running the restored version of Cisco Unified Communications Manager, restart the subsequent nodes.

**Step 10** Replication will be setup automatically after cluster reboot. Check the Replication Status value on all nodes by using the “utils dbreplication runtimestate” CLI command as described in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*. The value on each node should equal 2.

**Note** Database replication on the subsequent nodes may take enough time to complete after the subsequent node restarts, depending on the size of the cluster.

**Tip** If replication does not set up properly, use the "utils dbreplication rebuild" CLI command as described in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

---

**What to do next**
- (Optional) To view the status of the restore, see Check Restore Job Status, on page 282
- To restart a node, see Restart a Node, on page 281

---

**Restore Node Or Cluster to Last Known Good Configuration**

Follow this procedure to restore node or cluster to last known good configuration.

**Before you begin**
- Ensure that the restore file contains the hostname, IP address, DNS configuration, and deployment type that is configured in the backup file.
- Ensure that the Cisco Unified Communications Manager version installed on the server matches the version of the backup file that you want to restore.
- Ensure this procedure is used only to restore node to a last known good configuration.

**Procedure**

**Step 1** From the Disaster Recovery System, choose **Restore > Restore Wizard**.
**Step 2** In the **Select Backup Device** area, select the appropriate backup device to restore.
**Step 3** Click **Next**.
**Step 4**  In the **Restore Wizard Step 2** window, select the backup file you want to restore.

*Note*  The backup filename indicates the date and time that the system created the backup file.

**Step 5**  Click **Next**.

**Step 6**  In the **Restore Wizard Step 3** window, click **Next**.

**Step 7**  Select the appropriate node, when prompted to choose restore nodes.

Data is restored on the chosen nodes.

**Step 8**  Restart all nodes in the cluster. Restart the first Cisco Unified Communications Manager node before restarting the subsequent Cisco Unified Communications Manager nodes. If the cluster also has Cisco IM and Presence nodes, restart the first Cisco IM and Presence node before restarting the subsequent IM and Presence nodes. See the What to Do Next section for more information.

---

## Restart a Node

You must restart a node after you restore data.

If you are restoring a publisher node (first node), you must restart the publisher node first. Restart subscriber nodes only after the publisher node has restarted and is successfully running the restored version of the software.

**Caution**

This procedure causes the system to restart and become temporarily out of service.

Perform this procedure on every node in the cluster that you need to restart.

### Procedure

**Step 1**  From Cisco Unified OS Administration, select **Settings > Version**.

**Step 2**  To restart the node, click **Restart**.

**Step 3**  Replication will be setup automatically after cluster reboot. Check the Replication Status value on all nodes by using the `utils dbreplication runtimestate` CLI command. The value on each node should be equal 2. See *Cisco Unified Communications (CallManager) Command References* for more information about CLI commands.

If replication does not set up properly, use the `utils dbreplication reset` CLI command as described in the *Command Line Reference Guide for Cisco Unified Communications Solutions*.

*Note*  Database replication on the subsequent nodes may take several hours to complete after the subsequent nodes restart, depending on the size of the cluster.

### What to do next

(Optional) To view the status of the restore, see *Check Restore Job Status, on page 282*. 

---

Configuration and Administration for the IM and Presence Service, Release 11.5(1)SU5  
281
Check Restore Job Status

Follow this procedure to check the restore job status.

Procedure

**Step 1**
From the Disaster Recovery System, select Restore > Current Status.

**Step 2**
In the Restore Status window, click the log filename link to view the restore status.

View Restore History

Perform the following steps to view the restore history.

Procedure

**Step 1**
From Disaster Recovery System, choose Restore > History.

**Step 2**
From the Restore History window, you can view the restores that you have performed, including filename, backup device, completion date, result, version, features that were restored, and failed features.

The Restore History window displays only the last 20 restore jobs.

Data Authentication

Trace Files

The following trace file locations are used during troubleshooting or while collecting the logs.

Trace files for the Master Agent, the GUI, each Local Agent, and the JSch library get written to the following locations:

- For the Master Agent, find the trace file at platform/drf/trace/drfMA0*
- For each Local Agent, find the trace file at platform/drf/trace/drfLA0*
- For the GUI, find the trace file at platform/drf/trace/drfConfLib0*
- For the JSch, find the trace file at platform/drf/trace/drfJSch*

Command Line Interface

The Disaster Recovery System also provides command line access to a subset of backup and restore functions, as shown in the following table. For more information on these commands and on using the command line interface, see the Command Line Interface Reference Guide for Cisco Unified Communications Solutions at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html.

Table 32: Disaster Recovery System Command Line Interface

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>utils disaster_recovery estimate_tar_size</code></td>
<td>Displays estimated size of backup tar from SFTP/Local device and requires one parameter for feature list</td>
</tr>
<tr>
<td><code>utils disaster_recovery backup</code></td>
<td>Starts a manual backup by using the features that are configured in the Disaster Recovery System interface</td>
</tr>
<tr>
<td><code>utils disaster_recovery jschLogs</code></td>
<td>Enables or disables JSch library logging</td>
</tr>
<tr>
<td><code>utils disaster_recovery restore</code></td>
<td>Starts a restore and requires parameters for backup location, filename, features, and nodes to restore</td>
</tr>
<tr>
<td><code>utils disaster_recovery status</code></td>
<td>Displays the status of ongoing backup or restore job</td>
</tr>
<tr>
<td><code>utils disaster_recovery show_backupfiles</code></td>
<td>Displays existing backup files</td>
</tr>
<tr>
<td><code>utils disaster_recovery cancel_backup</code></td>
<td>Cancels an ongoing backup job</td>
</tr>
<tr>
<td><code>utils disaster_recovery show_registration</code></td>
<td>Displays the currently configured registration</td>
</tr>
<tr>
<td><code>utils disaster_recovery device add</code></td>
<td>Adds the network device</td>
</tr>
<tr>
<td><code>utils disaster_recovery device delete</code></td>
<td>Deletes the device</td>
</tr>
<tr>
<td><code>utils disaster_recovery device list</code></td>
<td>Lists all the devices</td>
</tr>
<tr>
<td><code>utils disaster_recovery schedule add</code></td>
<td>Adds a schedule</td>
</tr>
<tr>
<td><code>utils disaster_recovery schedule delete</code></td>
<td>Deletes a schedule</td>
</tr>
<tr>
<td><code>utils disaster_recovery schedule disable</code></td>
<td>Disables a schedule</td>
</tr>
<tr>
<td><code>utils disaster_recovery schedule enable</code></td>
<td>Enables a schedule</td>
</tr>
<tr>
<td><code>utils disaster_recovery schedule list</code></td>
<td>Lists all the schedules</td>
</tr>
<tr>
<td><code>utils disaster_recovery backup</code></td>
<td>Starts a manual backup by using the features that are configured in the Disaster Recovery System interface.</td>
</tr>
<tr>
<td><code>utils disaster_recovery restore</code></td>
<td>Starts a restore and requires parameters for backup location, filename, features, and nodes to restore.</td>
</tr>
<tr>
<td><code>utils disaster_recovery status</code></td>
<td>Displays the status of ongoing backup or restore job.</td>
</tr>
</tbody>
</table>
### Configuration and Administration for the IM and Presence Service, Release 11.5(1)SU5

#### Administer the System

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>utils disaster_recovery show_backupfiles</td>
<td>Displays existing backup files.</td>
</tr>
<tr>
<td>utils disaster_recovery cancel_backup</td>
<td>Cancels an ongoing backup job.</td>
</tr>
<tr>
<td>utils disaster_recovery show_registration</td>
<td>Displays the currently configured registration.</td>
</tr>
</tbody>
</table>

### Alarms and Messages

#### Alarms and Messages

The Disaster Recovery System issues alarms for various errors that could occur during a backup or restore procedure. The following table provides a list of Cisco Disaster Recovery System alarms.

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Description</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRFBackupDeviceError</td>
<td>DRF backup process has problems accessing device.</td>
<td>DRS backup process encountered errors while it was accessing device.</td>
</tr>
<tr>
<td>DRFBackupFailure</td>
<td>Cisco DRF Backup process failed.</td>
<td>DRS backup process encountered errors.</td>
</tr>
<tr>
<td>DRFBackupInProgress</td>
<td>New backup cannot start while another backup is still running</td>
<td>DRS cannot start new backup while another backup is still running.</td>
</tr>
<tr>
<td>DRFInternalProcessFailure</td>
<td>DRF internal process encountered an error.</td>
<td>DRS internal process encountered an error.</td>
</tr>
<tr>
<td>DRFLA2MAFailure</td>
<td>DRF Local Agent cannot connect to Master Agent.</td>
<td>DRS Local Agent cannot connect to Master Agent.</td>
</tr>
<tr>
<td>DRFLocalAgentStartFailure</td>
<td>DRF Local Agent does not start.</td>
<td>DRS Local Agent might be down.</td>
</tr>
<tr>
<td>DRFMA2LAFailure</td>
<td>DRF Master Agent does not connect to Local Agent.</td>
<td>DRS Master Agent cannot connect to Local Agent.</td>
</tr>
<tr>
<td>DRFMABackupComponentFailure</td>
<td>DRF cannot back up at least one component.</td>
<td>DRS requested a component to back up its data; however, an error occurred during the backup process, and the component did not get backed up.</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Description</td>
<td>Explanation</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DRFMABackupNodeDisconnect</td>
<td>The node that is being backed up disconnected from the Master Agent prior to being fully backed up.</td>
<td>While the DRS Master Agent was running a backup operation on a Cisco Unified Communications Manager node, the node disconnected before the backup operation completed.</td>
</tr>
<tr>
<td>DRFMARestoreComponentFailure</td>
<td>DRF cannot restore at least one component.</td>
<td>DRS requested a component to restore its data; however, an error occurred during the restore process, and the component did not get restored.</td>
</tr>
<tr>
<td>DRFMARestoreNodeDisconnect</td>
<td>The node that is being restored disconnected from the Master Agent prior to being fully restored.</td>
<td>While the DRS Master Agent was running a restore operation on a Cisco Unified Communications Manager node, the node disconnected before the restore operation completed.</td>
</tr>
<tr>
<td>DRFMasterAgentStartFailure</td>
<td>DRF Master Agent did not start.</td>
<td>DRS Master Agent might be down.</td>
</tr>
<tr>
<td>DRFNoRegisteredComponent</td>
<td>No registered components are available, so backup failed.</td>
<td>DRS backup failed because no registered components are available.</td>
</tr>
<tr>
<td>DRFNoRegisteredFeature</td>
<td>No feature got selected for backup.</td>
<td>No feature got selected for backup.</td>
</tr>
<tr>
<td>DRFRestoreDeviceError</td>
<td>DRF restore process has problems accessing device.</td>
<td>DRS restore process cannot read from device.</td>
</tr>
<tr>
<td>DRFRestoreFailure</td>
<td>DRF restore process failed.</td>
<td>DRS restore process encountered errors.</td>
</tr>
<tr>
<td>DRFSftpFailure</td>
<td>DRF SFTP operation has errors.</td>
<td>Errors exist in DRS SFTP operation.</td>
</tr>
<tr>
<td>DRFSecurityViolation</td>
<td>DRF system detected a malicious pattern that could result in a security violation.</td>
<td>The DRF Local Agent cannot connect to Master Agent.</td>
</tr>
<tr>
<td>DRFTruststoreMissing</td>
<td>The IPsec truststore is missing on the node.</td>
<td>The IPsec truststore is missing on the node. DRS Local Agent cannot connect to Master Agent.</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Description</td>
<td>Explanation</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DRFUnknownClient</td>
<td>DRF Master Agent on the Pub received a Client connection request from an unknown server outside the cluster. The request has been rejected.</td>
<td>The DRF Master Agent on the Pub received a Client connection request from an unknown server outside the cluster. The request has been rejected.</td>
</tr>
<tr>
<td>DRFBackupCompleted</td>
<td>DRF backup completed successfully.</td>
<td>DRF backup completed successfully.</td>
</tr>
<tr>
<td>DRFRestoreCompleted</td>
<td>DRF restore completed successfully.</td>
<td>DRF restore completed successfully.</td>
</tr>
<tr>
<td>DRFNoBackupTaken</td>
<td>DRF did not find a valid backup of the current system.</td>
<td>DRF did not find a valid backup of the current system after an Upgrade/Migration or Fresh Install.</td>
</tr>
<tr>
<td>DRFComponentRegistered</td>
<td>DRF successfully registered the requested component.</td>
<td>DRF successfully registered the requested component.</td>
</tr>
<tr>
<td>DRFRegistrationFailure</td>
<td>DRF Registration operation failed.</td>
<td>DRF Registration operation failed for a component due to some internal error.</td>
</tr>
<tr>
<td>DRFComponentDeRegistered</td>
<td>DRF successfully deregistered the requested component.</td>
<td>DRF successfully deregistered the requested component.</td>
</tr>
<tr>
<td>DRFDeRegistrationFailure</td>
<td>DRF deregistration request for a component failed.</td>
<td>DRF deregistration request for a component failed.</td>
</tr>
<tr>
<td>DRFFailure</td>
<td>DRF Backup or Restore process has failed.</td>
<td>DRF Backup or Restore process encountered errors.</td>
</tr>
<tr>
<td>DRFRestoreInternalError</td>
<td>DRF Restore operation has encountered an error. Restore cancelled internally.</td>
<td>DRF Restore operation has encountered an error. Restore cancelled internally.</td>
</tr>
<tr>
<td>DRFLogDirAccessFailure</td>
<td>DRF could not access the log directory.</td>
<td>DRF could not access the log directory.</td>
</tr>
<tr>
<td>DRFDeRegisteredServer</td>
<td>DRF automatically de-registered all the components for the server.</td>
<td>The server may have been disconnected from the Unified Communications Manager cluster.</td>
</tr>
<tr>
<td>DRFSchedulerDisabled</td>
<td>DRF Scheduler is disabled because no configured features are available for backup.</td>
<td>DRF Scheduler is disabled because no configured features are available for backup.</td>
</tr>
<tr>
<td>DRFSchedulerUpdated</td>
<td>DRF Scheduled backup configuration is updated automatically due to feature de-registration.</td>
<td>DRF Scheduled backup configuration is updated automatically due to feature de-registration.</td>
</tr>
</tbody>
</table>
## Restore Interactions and Restrictions

### Restore Restrictions

The following restrictions apply to using Disaster Recovery System to restore Cisco Unified Communications Manager or IM and Presence Service

**Table 34: Restore Restrictions**

<table>
<thead>
<tr>
<th>Restriction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export Restricted</td>
<td>You can restore the DRS backup from a restricted version only to a restricted version and the backup from an unrestricted version can be restored only to an unrestricted version. Note that if you upgrade to the U.S. export unrestricted version of Cisco Unified Communications Manager, you will not be able to later upgrade to or be able to perform a fresh install of the U.S. export restricted version of this software</td>
</tr>
<tr>
<td>Platform Migrations</td>
<td>You cannot use the Disaster Recovery System to migrate data between platforms (for example, from Windows to Linux or from Linux to Windows). A restore must run on the same product version as the backup. For information on data migration from a Windows-based platform to a Linux-based platform, see the <em>Data Migration Assistant User Guide</em>.</td>
</tr>
<tr>
<td>HW Replacement and Migrations</td>
<td>When you perform a DRS restore to migrate data to a new server, you must assign the new server the identical IP address and hostname that the old server used. Additionally, if DNS was configured when the backup was taken, then the same DNS configuration must be present prior to performing a restore. For more information about replacing a server, refer to the <em>Replacing a Single Server or Cluster for Cisco Unified Communications Manager</em> guide. In addition, you must run the Certificate Trust List (CTL) client after a hardware replacement. You must run the CTL client if you do not restore the subsequent node (subscriber) servers. In other cases, DRS backs up the certificates that you need. For more information, see the “Installing the CTL Client” and “Configuring the CTL Client” procedures in the <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
<tr>
<td>Extension Mobility Cross Cluster</td>
<td>Extension Mobility Cross Cluster users who are logged in to a remote cluster at backup shall remain logged in after restore.</td>
</tr>
</tbody>
</table>

Configuration and Administration for the IM and Presence Service, Release 11.5(1)SU5 287
Troubleshooting

DRS Restore to Smaller Virtual Machine Fails

**Problem**
A database restore may fail if you restore an IM and Presence Service node to a VM with smaller disks.

**Cause**
This failure occurs when you migrate from a larger disk size to a smaller disk size.

**Solution**
Deploy a VM for the restore from an OVA template that has 2 virtual disks.
Bulk Administration of Contact Lists

- Bulk Administration Overview, on page 289
- Bulk Administration Prerequisites, on page 289
- Bulk Administration Task Flow, on page 290

Bulk Administration Overview

With the IM and Presence Service Bulk Administration Tool, you can perform bulk transactions on many IM and Presence Service users, including:

- Rename User Contact IDs for use in the Microsoft migration process.
- Export the contact lists and non-presence contact lists, of users who belong to a particular node or presence redundancy group, to a CSV data file.

Note

Non-presence contacts are contacts who do not have an IM address and can only be exported using this procedure.

- You can import user contacts lists and non-presence contact lists you had exported to another node or presence redundancy group in a different cluster. Prepopulate contact lists for new users or add to existing contact lists.
- These features facilitate the migration of users between clusters.

Bulk Administration Prerequisites

Before importing your user contact lists:

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.
The default contact list import rate is based on the virtual machine deployment hardware type. You can change the contact list import rate by choosing **Cisco Unified CM IM and Presence Administration > System > Service Parameters > Cisco Bulk Provisioning Service**. However, if you increase the default import rate, this will result in higher CPU and memory usage on IM and Presence Service.

### Bulk Administration Task Flow

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Bulk Rename User Contact IDs, on page 290</td>
<td>Upload the CSV file and rename the contact IDs for a list of users.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Bulk Export User Contact Lists and Non-Presence Contact Lists, on page 291</td>
<td>Use this procedure to export your users' contact lists to a CSV file. You can then use Bulk Administration to move user contact lists to another node or cluster.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Carry out these tasks to import your user contact lists into IM and Presence Service:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Verify Maximum Contact List Size, on page 294</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Upload Input File, on page 294</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Create New Bulk Administration Job, on page 297</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Check Results of Bulk Administration Job, on page 297</td>
<td></td>
</tr>
</tbody>
</table>

### Bulk Rename User Contact IDs

**Caution**

Bulk rename of contact IDs is used in the migration of users from a Microsoft server (for example Lync) to IM and Presence Service Service. See the Partitioned Intradomain Federation Guide on Cisco.com for detailed instructions on how this tool should be used as part of the user migration process. Using this tool in any other circumstances is not supported.

Upload the CSV file and rename the contact IDs for a list of users.

**Procedure**

**Step 1**

Upload the CSV file with the list of contact IDs that you want to rename in all contact lists:

a) Go to the IM and Presence Service database publisher node.
b) In Cisco Unified CM IM and Presence Administration, choose Bulk Administration > Upload/Download Files.
c) Click Add New.
d) Click Browse to locate and choose the CSV file. For more on the input file, see Bulk Rename User Contact IDs File Details, on page 291.
e) Choose Contacts as the Target.
f) Choose Rename Contacts – Custom File as the Transaction Type.
g) Click Save to upload the file.

Step 2  In Cisco Unified CM IM and Presence Administration on the publisher node, choose Bulk Administration > Contact List > Rename Contacts.

Step 3  In the File Name field, choose the file that you uploaded.

Step 4  Choose one of the following actions:
   • Click Run Immediately to execute the Bulk Administration job immediately.
   • Click Run Later to schedule a time to execute the Bulk Administration job. For more information about scheduling jobs in the Bulk Administration Tool, see the Online Help in Cisco Unified CM IM and Presence Administration.

Step 5  Click Submit.
   If you chose to run the job immediately, the job runs after you click Submit.

What to do next
Bulk Export User Contact Lists and Non-Presence Contact Lists, on page 291

Bulk Rename User Contact IDs File Details

The file that you upload before you can run this job must be a CSV file with the following format:
<Contact ID>, <New Contact ID>
where <Contact ID> is the existing contact ID and <New Contact ID> is the new format of the contact ID.
(Contact ID) is the user's IM address as it appears on the Presence Topology User Assignment window.
The following is a sample CSV file with one entry:

Contact ID, New Contact ID
john.smith@example.com, jsmith@example.com

Bulk Export User Contact Lists and Non-Presence Contact Lists

Use this procedure to export your users' contact lists to a CSV file. You can then use Bulk Administration to move user contact lists to another node or cluster.
   • Contact Lists—This list consists of IM and Presence contacts. Contacts whom do not have an IM address will not be exported (you must export a non-presence contact list).
   • Non-preservation Contact Lists—This list consists of contacts whom do not have an IM address.
Procedure

Step 1  From Cisco Unified CM IM and Presence Administration, do either of the following:

• To export Contact Lists, choose Bulk Administration > Contact List > Export Contact List
• To export Non-presentation Contact Lists, choose Bulk Administration > Non-presentation Contact List > Export Non-presence Contact List and skip the next step.

Step 2  Contact Lists only. Select the users for whom you will export contact lists:

a) Under Export Contact List Options, choose the category of users for whom you will export contact lists.
   The default is to export contact lists for all users.

b) Click Find to bring up the list of users and then click Next.

Step 3  In the File Name field, enter a name for the CSV file.

Step 4  Under Job Information, configure when you want to run this job:

• Run Immediately—Check this button to export contact lists right away.
• Run Later—Check this button if you want to schedule a time for the job. With this option, you will need to use the Job Scheduler page at Bulk Administration > Job Scheduler to schedule a time for this job to run.

Step 5  Click Submit.
If you choose Run Immediately, the export job runs right away.

Step 6  After the export file is created, download the exported file:

a) From Cisco Unified CM IM and Presence Administration, choose Bulk Administration > Upload/Download Files.

b) Click Find and select the export file.

c) Click Download Selected and download the file to a location you can access.

File Details for Export Contact Lists

The following is a sample CSV file entry:

userA,example.com,userB,example.com,buddyB,General

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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>The user ID of the IM and Presence Service user.</td>
</tr>
<tr>
<td></td>
<td>Note: This value is the user portion of the user's IM address.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User Domain</td>
<td>The Presence domain of the IM and Presence Service user.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This value is the domain portion of the user's IM address.</td>
</tr>
<tr>
<td></td>
<td><strong>Example 1:</strong> <a href="mailto:bjones@example.com">bjones@example.com</a>—bjones is the user ID and example.com is the user domain.</td>
</tr>
<tr>
<td></td>
<td><strong>Example 2:</strong> bjones@<a href="mailto:usa@example.com">usa@example.com</a>—bjones@usa is the user ID and example.com is the user domain.</td>
</tr>
<tr>
<td>Contact ID</td>
<td>The user ID of the contact list entry.</td>
</tr>
<tr>
<td>Contact Domain</td>
<td>The Presence domain of the contact list entry.</td>
</tr>
<tr>
<td>Nickname</td>
<td>The nickname of the contact list entry.</td>
</tr>
<tr>
<td></td>
<td>If the user has not specified a nickname for a contact, the Nickname parameter will be blank.</td>
</tr>
<tr>
<td>Group Name</td>
<td>The name of the group to which the contact list entry is to be added.</td>
</tr>
<tr>
<td></td>
<td>If a user’s contacts are not sorted into groups, the default group name will be specified in the Group Name field.</td>
</tr>
</tbody>
</table>

**File Details for Export Non-Presence Contact Lists**

The non-presence user contact lists are exported to a CSV file with the following format:

```
<User JID>,<Contact JID>,<Group Name>,<Content Type>,<Version>,<Info>
```

The following table describes the parameters in the export file:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User JID</td>
<td>The User JID. This is the IM address of the user.</td>
</tr>
<tr>
<td>Contact JID</td>
<td>The User JID of the contact list entry, if available, otherwise it is the UUID.</td>
</tr>
<tr>
<td>Group Name</td>
<td>The name of the group to which the contact list entry is to be added.</td>
</tr>
<tr>
<td>Content Type</td>
<td>The textmimetype and subtype used in the info field.</td>
</tr>
<tr>
<td>Version</td>
<td>The content type used in the info field.</td>
</tr>
<tr>
<td>Info</td>
<td>The contact information of the contact list entry in vCard format.</td>
</tr>
</tbody>
</table>
The following is a sample CSV file entry:

```
user2@cisco.com,ce463d44-02c3-4975-a37f-d4553e3f17e1,group01,text/directory,3,BEGIN:VCARD
ADR;TYPE=WORK:ADR;WORK:;123 Dublin rd,\;Oranmore\;Galway\;\;Ireland
EMAIL;TYPE=X-CUSTOM1;X LABEL=Custom:testuser01@test.com N:test;user;;; NICKNAME:pizzaguy01
ORG:ABC TEL;TYPE=WORK,VOICE:5323534535 TITLE:QA VERSION:3.0 END:VCARD
```

**Bulk Import Of User Contact Lists**

### Verify Maximum Contact List Size

Check the Maximum Contact List Size and Maximum Watchers settings on IM and Presence Service. 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. Even though you exceed the maximum contact list size without losing data when importing contact lists using BAT, this step 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.

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 Input File, on page 294

### Upload Input File

The following procedure describes how to upload the CSV input file using BAT for contact lists and non-presence contact lists.

**Before you begin**

Verify Maximum Contact List Size, on page 294

**Procedure**

**Step 1**

In Cisco Unified CM IM and Presence Administration, choose **Bulk Administration > Upload/Download Files**.

**Step 2**

Click **Add New**.

**Step 3**

Click **Browse** to locate and choose the CSV file.

**Step 4**

For the Target setting:

- If you want to upload an input file for contact lists, choose **Contact Lists**. For more on user contact list input files, see File Details for Import Contact Lists, on page 295.
- If you want to upload an input file for non-presence contact lists, choose **Non-presence Contact Lists**. For more on non-presence user contact list input files, see File Details for Import Non-Presence Contact Lists, on page 296.
Step 5  For the Transaction Type: Choose as the Transaction Type.
   • If you want to upload an input file for contact lists, choose Import Users’ Contacts – Custom File
   • If you want to upload an input file for non-presence contact lists, choose Import Users’ Non Presence Contacts

Step 6  Click Save to upload the file.

What to do next
Create New Bulk Administration Job, on page 297

File Details for Import 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>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>This is a mandatory parameter. The user ID of the IM and Presence Service user. It can have a maximum of 132 characters. Note This value is the user portion of the user's IM address.</td>
</tr>
<tr>
<td>User Domain</td>
<td>This is a mandatory parameter. The Presence domain of the IM and Presence Service user. It can have a maximum of 128 characters. Note This value is the domain portion of the user's IM address. Example 1: <a href="mailto:bjones@example.com">bjones@example.com</a>—bjones is the user ID and example.com is the user domain. Example 2: bjones@<a href="mailto:usa@example.com">usa@example.com</a>—bjones@usa is the user ID and example.com is the user domain.</td>
</tr>
<tr>
<td>Contact ID</td>
<td>This is a mandatory parameter. The user ID of the contact list entry. It can have a maximum of 132 characters.</td>
</tr>
</tbody>
</table>
**Parameter** | **Description**
---|---
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.

GroupName | 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.

---

**File Details for Import Non-Presence Contact Lists**

The input file must be a CSV file in the following format:

<User JID>,<Contact JID>,<Group Name>,<Content Type>,<Version>,<Info>

The following is a sample CSV file entry:

user2@cisco.com,ce463d44-02c3-4975-a37f-d4553e3f17e1,group01,text/directory,3,BEGIN:VCARD ADR;TYPE=WORK:ADR;WORK:;123 Dublin rd,\;Oranmore\;Galway\;Ireland EMAIL;TYPE=X-CUSTOM1;X LABEL=Custom:testuser01@test.com N:testuser01; NICKNAME:pizzaguy01 ORG:ABC TEL;TYPE=WORK,VOICE:5323534535 TITLE:QA VERSION:3.0 END:VCARD

⚠️ **Caution**

We recommend that you do not manually modify the CSV file, due to the size of the file itself and the risk of corrupting the vCard information.

The following table describes the parameters in the input file for non-presence contacts:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User JID</td>
<td>The User JID. This is the IM address of the user.</td>
</tr>
<tr>
<td>Contact JID</td>
<td>The User JID of the contact list entry, if available, otherwise it is the UUID.</td>
</tr>
</tbody>
</table>
Create New Bulk Administration Job

Create a new bulk administration job for contact lists and non-presence contact lists.

Before you begin
Upload Input File, on page 294

Procedure

Step 1 In Cisco Unified CM IM and Presence Administration:
- If you want to create a new bulk administration job for contact lists, choose Bulk Administration > Contact List > Update
- If you want to create a new bulk administration job for contact lists, choose Bulk Administration > Contact Non-presence List > Import Non-presence Contact List.

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 Results of Bulk Administration Job, on page 297

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.

**Before you begin**

Create New Bulk Administration Job, on page 297

**Procedure**

**Step 1**  
In Cisco Unified CM IM and Presence Administration, choose 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.
Troubleshoot the System

- Troubleshooting Overview, on page 299
- Run the System Troubleshooter, on page 299
- Run Diagnostics, on page 300
- Using Trace Logs for Troubleshooting, on page 302
- Troubleshooting UserID and Directory URI Errors, on page 310

Troubleshooting Overview

Use the procedures in this chapter to troubleshoot issues with your IM and Presence deployment. With your IM and Presence Service deployment, you can:

- Use the Command Line Interface (CLI) to build trace logs that you can use to check to resolve issues.
- Run diagnostics, to check for issues with your system.
- Run the system troubleshooter to confirm the health of your system.
- Troubleshoot duplicate directory URI issues.

Run the System Troubleshooter

Run the troubleshooter to diagnose issues with your IM and Presence Service deployment. The troubleshooter checks automatically for a wide range of issues with your deployment including:

- System Issues
- Sync Agent Issues
- Presence Engine Issues
- SIP Proxy Issues
- Microsoft RCC Issues
- Calendaring Issues
- Inter-clustering Issues
- Topology Issues
**Run Diagnostics**

When administering an up and running system, you may encounter problems which affect the normal running of the system. You can use the IM and Presence Service Diagnostic tools to help determine the root causes of these problems.

Use this procedure to access the Diagnostic tools on IM and Presence Service.

These tools can be accessed in **Cisco Unified CM IM and Presence Administration** by clicking **Diagnostics** and choosing from one of these options:

**Procedure**

**Step 1**  
In **Cisco Unified CM IM and Presence Administration**, choose **Diagnostics**.

**Step 2**  
Click the Diagnostic tool you want to use from the drop-down list.

See Diagnostic Tools Overview for more on the purpose of these tools.
## Diagnostic Tools Overview

<table>
<thead>
<tr>
<th>Diagnostic Tool</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Dashboard</td>
<td>Use the System Dashboard to acquire a snapshot of the state of your IM and Presence Service system including a summary data view of these system components - number of devices, number of users, per-user data such as contacts, and primary extension.</td>
</tr>
</tbody>
</table>
| System Configuration Troubleshooter     | Use the System Configuration Troubleshooter to diagnose IM and Presence Service configuration issues after your initial configuration or whenever you make configuration changes. The Troubleshooter performs a set of tests on both the IM and Presence Service cluster and on the Cisco Unified Communications Manager cluster to validate the IM and Presence Service configuration. After the Troubleshooter finishes testing, it reports one of three possible states for each test:  
  - Test Passed  
  - Test Failed  
  - Test Warning, which indicates a possible configuration issue  
  For each test that fails or that results in a warning, the Troubleshooter provides a description of the problem and a possible solution. For any test failures or test warnings, click the fix link in the solution column to go to the Cisco Unified Communications Manager IM and Presence Administration window where the Troubleshooter found the problem. Correct any configuration errors that you find and rerun the Troubleshooter. |
| Microsoft RCC Troubleshooter            | Use the Microsoft Remote Call Control (RCC) Troubleshooter to diagnose integration issues between IM and Presence Service and the Microsoft Lync or Microsoft Office client application after your initial configuration or whenever you make configuration changes. The Troubleshooter validates user-related and connectivity-related issues between Microsoft Lync, LCS, or OCS servers and the IM and Presence Service, and between the Microsoft Lync or Microsoft Office client and the IM and Presence Service. |
Using Trace Logs for Troubleshooting

Use traces to troubleshoot system issues with IM and Presence services and features. You can configure automated system tracing for a variety of services, features, and system components. The results are stored in system logs that you can browse and view using the Cisco Unified Real-Time Monitoring Tool. Alternatively, you can use the Command Line Interface to pull a subset of the system log files and upload them to your own PC or laptop for further analysis.

To use traces, you must first configure the system for tracing. For details on how to configure system tracing, refer to the "Traces" chapter of the *Cisco Unified Serviceability Administration Guide*.

Once tracing is configured, you can use one of two methods to view the contents of trace files:

- **Real-Time Monitoring Tool**—With the Real-Time Monitoring Tool, you can browse and view the individual log files that are created as a result of system tracing. For details on how to use the Real-Time Monitoring Tool, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

- **Command Line Interface (CLI)**—If system tracing is configured, use the CLI to build customized traces from your system logs. With the CLI, you can specify the specific days that you want to include in a customized trace file. The CLI pulls the associated trace files from your system and saves them in a compressed zip file that you can copy to a PC or laptop for further analysis, thereby ensuring that the logs don't get overwritten by the system.

The subsequent tables and tasks in this section describe how to use CLI commands to build trace log files for the IM and Presence Service.

Common IM and Presence Issues via Trace

The following table lists common issues with the IM and Presence Service and which traces you can run to troubleshoot the issue.

*Table 35: Common IM and Presence Issue Troubleshooting*

<table>
<thead>
<tr>
<th>Issues with...</th>
<th>View Traces for These Services</th>
<th>Additional Instructions</th>
</tr>
</thead>
</table>
| Login and Authentication Traces | Client Profile Agent  
Cisco XCP Connection Manager  
Cisco XCP Router  
Cisco XCP Authentication Service  
Cisco Tomcat Security Logs | See Common Traces via CLI, on page 304 for CLI commands to build logs and output locations. |
| Availability Status       | Cisco XCP Connection Manager  
Cisco XCP Router  
Cisco Presence Engine | See Common Traces via CLI, on page 304 for CLI commands to build logs and output locations. |
| Sending and Receiving IMs| Cisco XCP Connection Manager  
Cisco XCP Router | See Common Traces via CLI, on page 304 for CLI commands to build logs and output locations. |
<table>
<thead>
<tr>
<th>Issues with...</th>
<th>View Traces for These Services</th>
<th>Additional Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Lists</td>
<td>Cisco XCP Connection Manager</td>
<td>See Common Traces via CLI, on page 304 for CLI commands to build logs and output locations.</td>
</tr>
<tr>
<td></td>
<td>Cisco XCP Router</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Presence Engine</td>
<td></td>
</tr>
<tr>
<td>Chat Rooms</td>
<td>Cisco XCP Connection Manager</td>
<td>See Common Traces via CLI, on page 304 for CLI commands to build logs and output locations.</td>
</tr>
<tr>
<td></td>
<td>Cisco XCP Router</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Presence Engine</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco XCP Text Conferencing Manager</td>
<td></td>
</tr>
<tr>
<td>Partitioned Intradomain Federation</td>
<td>Cisco XCP Router</td>
<td>See Common Traces via CLI, on page 304 for CLI commands to build logs and output locations.</td>
</tr>
<tr>
<td></td>
<td>Cisco XCP SIP Federation Connection Manager</td>
<td>Note Cisco SIP Proxy debug logging is required to see the SIP message exchange.</td>
</tr>
<tr>
<td></td>
<td>Cisco SIP Proxy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Presence Engine</td>
<td></td>
</tr>
<tr>
<td>Availability and IMs for XMPP Based Interdomain Federation Contact</td>
<td>Cisco XCP Connection Manager</td>
<td>See Common Traces via CLI, on page 304 for CLI commands to build logs and output locations.</td>
</tr>
<tr>
<td></td>
<td>Cisco XCP Router</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Presence Engine</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco XCP XMPP Federation Connection Manager</td>
<td></td>
</tr>
<tr>
<td>Availability and IMs for SIP Interdomain Federation Contact</td>
<td>Cisco XCP Connection Manager</td>
<td>See Common Traces via CLI, on page 304 for CLI commands to build logs and output locations.</td>
</tr>
<tr>
<td></td>
<td>Cisco XCP Router</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Presence Engine</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco SIP Proxy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco XCP SIP Federation Connection Manager</td>
<td></td>
</tr>
<tr>
<td>Calendaring Traces</td>
<td>Cisco Presence Engine</td>
<td>See Common Traces via CLI, on page 304 for CLI commands to build logs and output locations.</td>
</tr>
<tr>
<td>Intercluster Synchronization Traces and Intercluster Troubleshooter</td>
<td>Cisco Intercluster Sync Agent</td>
<td>Run the system troubleshooter at Diagnostics &gt; System Troubleshooter to check for interclustering errors.</td>
</tr>
<tr>
<td></td>
<td>Cisco AXL Web Service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Tomcat Security Log</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Syslog Agent</td>
<td></td>
</tr>
<tr>
<td>Issues with...</td>
<td>View Traces for These Services</td>
<td>Additional Instructions</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SIP Federation Traces</td>
<td>Cisco SIP Proxy</td>
<td>See Common Traces via CLI, on page 304 for CLI commands to build logs and file output locations.</td>
</tr>
<tr>
<td></td>
<td>Cisco XCP Router</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco XCP SIP Federation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Connection Manager</td>
<td></td>
</tr>
<tr>
<td>XMPP Federation Traces</td>
<td>Cisco XCP Router</td>
<td>See Common Traces via CLI, on page 304 for CLI commands to build logs and file output locations.</td>
</tr>
<tr>
<td></td>
<td>Cisco XCP XMPP Federation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Connection Manager</td>
<td></td>
</tr>
<tr>
<td>High CPU and Low VM Alert</td>
<td>Cisco XCP Router</td>
<td>For additional troubleshooting, run the following CLI commands:</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>Cisco XCP SIP Federation</td>
<td>• <code>show process using-most cpu</code></td>
</tr>
<tr>
<td></td>
<td>Connection Manager</td>
<td>• <code>show process using-most memory</code></td>
</tr>
<tr>
<td></td>
<td>Cisco SIP Proxy</td>
<td>• <code>utils dbreplication runtimestate</code></td>
</tr>
<tr>
<td></td>
<td>Cisco Presence Engine</td>
<td>• <code>utils service list</code></td>
</tr>
<tr>
<td></td>
<td>Cisco Tomcat Security Log</td>
<td>Run the following CLI to get RIS (Real-Time Information Service) data:</td>
</tr>
<tr>
<td></td>
<td>Cisco Syslog Agent</td>
<td>• <code>file get activelog cm/log/ris/csv</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
The CLI pulls a subset of the same individual traces files that you can view with the Cisco Unified Real-Time Monitoring Tool (RTMT), but groups and stores them in a single compressed zip file. For RTMT traces, see Common Traces via RTMT, on page 309.

### Table 36: Common Traces for IM and Presence Services using CLI

<table>
<thead>
<tr>
<th>Service</th>
<th>CLI to Build Log</th>
<th>CLI Output File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Audit Logs</td>
<td>file build log cisco_audit_logs &lt;duration&gt;</td>
<td>/epas/trace/log_cisco_audit_logs_*.tar.gz</td>
</tr>
<tr>
<td>Cisco Client Profile Agent</td>
<td>file build log cisco_client_profile_agent &lt;duration&gt;</td>
<td>/epas/trace/log_cisco_client_profile_agent_*.tar.gz</td>
</tr>
<tr>
<td>Cisco Cluster Manager</td>
<td>file build log cisco_config_agent &lt;duration&gt;</td>
<td>/epas/trace/log_cisco_cluster_manager_*.tar.gz</td>
</tr>
<tr>
<td>Cisco Config Agent</td>
<td>file build log cisco_config_agent &lt;duration&gt;</td>
<td>/epas/trace/log_cisco_config_agent_*.tar.gz</td>
</tr>
<tr>
<td>Cisco Database Layer Monitor</td>
<td>file build log cisco_database_layer_monitor &lt;duration&gt;</td>
<td>/epas/trace/log_cisco_database_layer_monitor_*.tar.gz</td>
</tr>
<tr>
<td>Cisco Intercluster Sync Agent</td>
<td>file build log cisco_inter_cluster_sync_agent &lt;duration&gt;</td>
<td>/epas/trace/log_cisco_inter_cluster_sync_agent_*.tar.gz</td>
</tr>
<tr>
<td>Cisco OAM Agent</td>
<td>file build log cisco_oam_agent &lt;duration&gt;</td>
<td>/epas/trace/log_cisco_oam_agent_*.tar.gz</td>
</tr>
<tr>
<td>Cisco Presence Engine</td>
<td>file build log cisco_presence_engine &lt;duration&gt;</td>
<td>/epas/trace/log_cisco_presence_engine_*.tar.gz</td>
</tr>
<tr>
<td>Cisco RIS (Real-time Information Service) Data Collector</td>
<td>file build log cisco_ris_data_collector &lt;duration&gt;</td>
<td>/epas/trace/log_cisco_ris_data_collector_*.tar.gz</td>
</tr>
<tr>
<td>Cisco Service Management</td>
<td>file build log cisco_service_management &lt;duration&gt;</td>
<td>/epas/trace/log_cisco_service_management_*.tar.gz</td>
</tr>
<tr>
<td>Cisco SIP Proxy</td>
<td>file build log cisco_sip_proxy &lt;duration&gt;</td>
<td>/epas/trace/log_cisco_sip_proxy_*.tar.gz</td>
</tr>
<tr>
<td>Cisco Sync Agent</td>
<td>file build log cisco_sync_agent &lt;duration&gt;</td>
<td>/epas/trace/log_cisco_sync_agent_*.tar.gz</td>
</tr>
</tbody>
</table>
### Common Traces via CLI

<table>
<thead>
<tr>
<th>Service</th>
<th>CLI to Build Log</th>
<th>CLI Output File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco XCP Config Manager</td>
<td>file build log cisco_xcp_config_mgr &lt;duration&gt;</td>
<td>/epas/trace/log_cisco_xcp_config_mgr_*.tar.gz</td>
</tr>
<tr>
<td>Cisco XCP Router</td>
<td>file build log cisco_xcp_router &lt;duration&gt;</td>
<td>/epas/trace/log_cisco_xcp_router_*.tar.gz</td>
</tr>
</tbody>
</table>

Table 37: Common Traces for IM and Presence Features using CLI

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>CLI to Build Log</th>
<th>CLI Output File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration GUI</td>
<td>file build log admin_ui &lt;duration&gt;</td>
<td>/epas/trace/log_admin_ui_*.tar.gz</td>
</tr>
<tr>
<td>Bulk Administration</td>
<td>file build log bat &lt;duration&gt;</td>
<td>/epas/trace/log_bat_*.tar.gz</td>
</tr>
<tr>
<td>Bidirectional Streams over</td>
<td>file build log bosh &lt;duration&gt;</td>
<td>/epas/trace/log_bosh_*.tar.gz</td>
</tr>
<tr>
<td>Synchronous HTTP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificates</td>
<td>file build log certificates &lt;duration&gt;</td>
<td>/epas/trace/log_certificates_*.tar.gz</td>
</tr>
<tr>
<td>Config Agent Core</td>
<td>file build log cfg_agent_core &lt;duration&gt;</td>
<td>/epas/trace/log_cfg_agent_core_*.tar.gz</td>
</tr>
<tr>
<td>Customer Voice Portal</td>
<td>file build log cvp &lt;duration&gt;</td>
<td>/epas/trace/log_cvp_*.tar.gz</td>
</tr>
<tr>
<td>Directory Groups</td>
<td>file build log directory_groups &lt;duration&gt;</td>
<td>/epas/trace/log_directory_groups_*.tar.gz</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>file build log disaster_recovery &lt;duration&gt;</td>
<td>/epas/trace/log_disaster_recovery_*.tar.gz</td>
</tr>
<tr>
<td>Flexible IM address</td>
<td>file build log flexible_im_address &lt;duration&gt;</td>
<td>/epas/trace/logFlexible_im_address_*.tar.gz</td>
</tr>
<tr>
<td>General core</td>
<td>file build log general_core &lt;duration&gt;</td>
<td>/epas/trace/log_general_core_*.tar.gz</td>
</tr>
<tr>
<td>High Availability</td>
<td>file build log ha &lt;duration&gt;</td>
<td>/epas/trace/log_ha_*.tar.gz</td>
</tr>
<tr>
<td>High CPU</td>
<td>file build log high_cpu &lt;duration&gt;</td>
<td>/epas/trace/log_high_cpu_*.tar.gz</td>
</tr>
<tr>
<td>High Memory</td>
<td>file build log high_memory &lt;duration&gt;</td>
<td>/epas/trace/log_high_memory_*.tar.gz</td>
</tr>
<tr>
<td>Instant Messaging Database Core</td>
<td>file build log imdb &lt;duration&gt;</td>
<td>/epas/trace/log_imdb_core_*.tar.gz</td>
</tr>
<tr>
<td>Intercluster Peering</td>
<td>file build log inter_cluster &lt;duration&gt;</td>
<td>/epas/trace/log_inter_cluster_*.tar.gz</td>
</tr>
<tr>
<td>Feature Name</td>
<td>CLI to Build Log</td>
<td>CLI Output File</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Managed File Transfer</td>
<td>file build log managed_file_transfer &lt;duration&gt;</td>
<td>/epas/trace/log_managed_file_transfer_*.tar.gz</td>
</tr>
<tr>
<td>Microsoft Exchange</td>
<td>file build log msft_exchange &lt;duration&gt;</td>
<td>/epas/trace/log_msft_exchange_*.tar.gz</td>
</tr>
<tr>
<td>Message Archiver</td>
<td>file build log msg_archiver &lt;duration&gt;</td>
<td>/epas/trace/log_msg_archiver_*.tar.gz</td>
</tr>
<tr>
<td>Presence Engine Core</td>
<td>file build log pe_core &lt;duration&gt;</td>
<td>/epas/trace/log_pe_core_*.tar.gz</td>
</tr>
<tr>
<td>Presence and IM Message Exchange</td>
<td>file build log presence_im_exchange &lt;duration&gt;</td>
<td>/epas/trace/log_presence_im_exchange_*.tar.gz</td>
</tr>
<tr>
<td>SIP Login Issues</td>
<td>file build log pws &lt;duration&gt;</td>
<td>/epas/trace/log_pws_*.tar.gz</td>
</tr>
<tr>
<td>Remote Call Control</td>
<td>file build log remote_call_control &lt;duration&gt;</td>
<td>/epas/trace/log_remote_call_control_*.tar.gz</td>
</tr>
<tr>
<td>Security Vulnerabilities</td>
<td>file build log sec_vulnerability &lt;duration&gt;</td>
<td>/epas/trace/log_sec_vulnerability_*.tar.gz</td>
</tr>
<tr>
<td>Serviceability GUI</td>
<td>file build log serviceability_ui &lt;duration&gt;</td>
<td>/epas/trace/log_serviceability_ui_*.tar.gz</td>
</tr>
<tr>
<td>SIP Interdomain Federation</td>
<td>file build log sip_inter_federation &lt;duration&gt;</td>
<td>/epas/trace/log_sip_inter_federation_*.tar.gz</td>
</tr>
<tr>
<td>SIP Partitioned Intradomain Federation</td>
<td>file build log sip_partitioned_federation &lt;duration&gt;</td>
<td>/epas/trace/log_sip_partitioned_federation_*.tar.gz</td>
</tr>
<tr>
<td>SIP Proxy Core</td>
<td>file build log sipd_core &lt;duration&gt;</td>
<td>/epas/trace/log_sipd_core_*.tar.gz</td>
</tr>
<tr>
<td>Persistent Chat High Availability</td>
<td>file build log tc_ha &lt;duration&gt;</td>
<td>/epas/trace/log_tc_ha_*.tar.gz</td>
</tr>
<tr>
<td>Persistent Chat</td>
<td>file build log text_conference &lt;duration&gt;</td>
<td>/epas/trace/log_text_conference_*.tar.gz</td>
</tr>
<tr>
<td>Upgrade Issues</td>
<td>file build log upgrade_issues &lt;duration&gt;</td>
<td>/epas/trace/log_upgrade_issues_*.tar.gz</td>
</tr>
<tr>
<td>User Connectivity</td>
<td>file build log user_connectivity &lt;duration&gt;</td>
<td>/epas/trace/log_user_connectivity_*.tar.gz</td>
</tr>
<tr>
<td>Rosters</td>
<td>file build log user_rosters &lt;duration&gt;</td>
<td>/epas/trace/log_user_rosters_*.tar.gz</td>
</tr>
</tbody>
</table>
Run Traces via CLI

Use this procedure to create a customized trace file via the Command Line Interface (CLI). With the CLI, you can specify, via the duration parameter, the number of days looking backwards that you want to include in your trace. The CLI pulls a subset of the system logs.

**Note**
Make sure to use SFTP servers only to transfer files.

**Before you begin**
You must have trace configured for your system. For details on setting up trace, see the "Trace" chapter of the Cisco Unified Serviceability Administration Guide.

Review **Common Traces via CLI, on page 304** for a list of traces that you can run.

**Procedure**

**Step 1**
Log in to the Command Line Interface.

**Step 2**
To build the log, run the `file build log <name of service> <duration>` CLI command where duration is the number of days to include in the trace.

For example, `file build log cisco_cluster_manager 7` to view Cisco Cluster Manager logs for the past week.

**Step 3**
To get the log, run the `file get activelog <log filepath>` CLI command to get the trace files.

For example, `file get activelog epas/trace/log_cisco_cluster_manager__2016-09-30-09h41m37s.tar.gz`.

**Step 4**
To maintain a stable system, delete the log after you retrieve it. Run the `file delete activelog <filepath>` command to delete the log.

For example, `file delete activelog epas/trace/log_cisco_cluster_manager__2016-09-30-09h41m37s.tar.gz`.

---

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>CLI to Build Log</th>
<th>CLI Output File</th>
</tr>
</thead>
<tbody>
<tr>
<td>XCP Router Core</td>
<td>file build log xcp_core &lt;duration&gt;</td>
<td>/epas/trace/log_xcp_core_*_.tar.gz</td>
</tr>
<tr>
<td>XMPP Interdomain Federation</td>
<td>file build log xmpp_inter_federation &lt;duration&gt;</td>
<td>/epas/trace/log_xmpp_inter_federation_*_.tar.gz</td>
</tr>
<tr>
<td>Deployment Info</td>
<td>file build log deployment_info &lt;duration&gt;</td>
<td>/epas/trace/log_deployment_info_*_.tar.gz</td>
</tr>
</tbody>
</table>
Common Traces via RTMT

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).

<table>
<thead>
<tr>
<th>Service</th>
<th>Trace Log Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco AXL Web Services</td>
<td>/tomcat/logs/axl/log4j/axl*.log</td>
</tr>
<tr>
<td>Cisco Intercluster Sync Agent</td>
<td>/epas/trace/cupicsa/log4j/icSyncAgent*.log</td>
</tr>
<tr>
<td>Cisco Presence Engine</td>
<td>/epas/trace/epe/sdi/epe*.txt</td>
</tr>
<tr>
<td>Cisco SIP Proxy</td>
<td>/epas/trace/esp/sdi/esp*.txt</td>
</tr>
<tr>
<td>Cisco Syslog Agent</td>
<td>/cm/trace/syslogmib/sdi/syslogmib*.txt</td>
</tr>
<tr>
<td>Cisco XCP Authentication Service</td>
<td>/epas/trace/xcp/log/auth-svc-1*.log</td>
</tr>
<tr>
<td>Cisco XCP Config Manager</td>
<td>/epas/trace/xcpconfigmgr/log4j/xcpconfigmgr*.log</td>
</tr>
<tr>
<td>Cisco XCP Connection Manager</td>
<td>/epas/trace/xcp/log/client-cm-1*.log</td>
</tr>
<tr>
<td>Cisco XCP Router</td>
<td>/epas/trace/xcp/log/rtr-jsm-1*.log</td>
</tr>
<tr>
<td>Cisco XCP SIP Federation Connection Manager</td>
<td>/epas/trace/xcp/log/sip-cm-3*.log</td>
</tr>
<tr>
<td>Cisco XCP Text Conferencing Manager</td>
<td>/epas/trace/xcp/log/txt-conf-1*.log</td>
</tr>
<tr>
<td>Cisco XCP XMPP Federation Connection Manager</td>
<td>/epas/trace/xcp/log/xmpp-cm-4*.log</td>
</tr>
<tr>
<td>Cluster Manager</td>
<td>/platform/log/clustermgr*.log</td>
</tr>
</tbody>
</table>

The CLI can be used to pull a subset of the same individual traces files that you can view with RTMT, but groups and stores them in a single compressed zip file. For CLI traces, see Common Traces via CLI, on page 304.

The following table shows the output locations for 11.5(1). Please note that automatic log file compression with gzip was introduced for many of these services as of release 11.5(1)SU2. For 11.5(1)SU2 and later details, see Release Notes for Cisco Unified Communications Manager and the IM and Presence Service, Release 11.5(1)SU2.
Troubleshooting UserID and Directory URI Errors

Received Duplicate UserID Error

Problem I received an alarm indicating that there are duplicate user IDs and I have to modify the contact information for those users.

Solution Perform the following steps.

1. Use the `utils users validate { all | userid | uri }` CLI command to generate a list of all users. For more information about using the CLI, see the Command Line Interface Guide for Cisco Unified Communications Solutions.

   The UserID is entered in the result set and is followed by the list of servers where the duplicate UserIDs are homed. The following sample CLI output shows UserID errors during output:

   Users with Duplicate User IDs
   ---------------------------------------------
   User ID: user3
   Node Name
   cucm-imp-1
   cucm-imp-2

2. If the same user is assigned to two different clusters, then unassign the user from one of the clusters.

3. If different users on different clusters have the same UserID assigned to them, then rename the UserID value for one of the users to ensure there is no longer any duplication.

4. If the user information is invalid or empty, proceed to correct the user ID information for that user using the Cisco Unified Communications Manager Administration GUI.

5. You can modify the user records in Cisco Unified Communications Manager using the End User Configuration window, (User Management > EndUser) to ensure that all users have a valid UserID or Directory URI value as necessary. For more information, see the Cisco Unified Communications Manager Administration Guide.

   Note The user ID and directory URI fields in the user profile may be mapped to the LDAP Directory. In that case, apply the fix in the LDAP Directory server.

6. Run the CLI command to validate users again to ensure that there are no more duplicate user ID errors.
Received Duplicate or Invalid Directory URI Error

**Problem** I received an alarm indicating that there are duplicate or invalid user Directory URIs and I have to modify the contact information for those users.

**Solution** Perform the following steps.

1. Use the `utils users validate { all | userid | uri }` CLI command to generate a list of all users. For more information about using the CLI, see the Command Line Interface Guide for Cisco Unified Communications Solutions.

   The Directory URI value is entered in the result set and is followed by the list of servers where the duplicate or invalid Directory URIs are homed. The following sample CLI output shows Directory URI errors detected during a validation check:

   ```
   Users with No Directory URI Configured
   ----------------------------------------
   Node Name: cucm-imp-2
   User ID user4

   Users with Invalid Directory URI Configured
   ----------------------------------------
   Node Name: cucm-imp-2
   User ID Directory URI
   user1 asdf@ASDF@asdf@ADSF@cisco

   Users with Duplicate Directory URIs
   ----------------------------------------
   Directory URI: user1@cisco.com
   Node Name User ID
   cucm-imp-1 user4
   cucm-imp-2 user3
   ```

2. If the same user is assigned to two different clusters, then unassign the user from one of the clusters.

3. If different users on different clusters have the same Directory URI value assigned to them, then rename the Directory URI value for one of the users to ensure there is no longer any duplication.

4. If the user information is invalid or empty, proceed to correct the user's Directory URI information.

5. You can modify the user records in Cisco Unified Communications Manager using the **End User Configuration** window, (User Management > EndUser) to ensure that all users have a valid user ID or Directory URI value as necessary. For more information, see the Cisco Unified Communications Manager Administration Guide.

   **Note** The user ID and directory URI fields in the user profile may be mapped to the LDAP Directory. In that case, apply the fix in the LDAP Directory server.

6. Run the CLI command to validate users again to ensure that there are no more duplicate or invalid Directory URI errors.
Received Duplicate or Invalid Directory URI Error

Administer the System
PART V

Reference Information

- Cisco Unified Communications Manager TCP and UDP Port Usage, on page 315
- Port Usage Information for the IM and Presence Service, on page 333
- Additional Requirements, on page 345
Cisco Unified Communications Manager TCP and UDP Port Usage

This chapter provides a list of the TCP and UDP ports that Cisco Unified Communications Manager uses for intracluster connections and for communication with external applications or devices. You will also find important information for the configuration of firewalls, Access Control Lists (ACLs), and quality of service (QoS) on a network when an IP Communications solution is implemented.

- Cisco Unified Communications Manager TCP and UDP Port Usage Overview, on page 315
- Port Descriptions, on page 316
- Port References, on page 331

Cisco Unified Communications Manager TCP and UDP Port Usage Overview

Cisco Unified Communications Manager TCP and UDP ports are organized into the following categories:

- Intracluster Ports Between Cisco Unified Communications Manager Servers
- Common Service Ports
- Ports Between Cisco Unified Communications Manager and LDAP Directory
- Web Requests From CCMAdmin or CCMUser to Cisco Unified Communications Manager
- Web Requests From Cisco Unified Communications Manager to Phone
- Signaling, Media, and Other Communication Between Phones and Cisco Unified Communications Manager
- Signaling, Media, and Other Communication Between Gateways and Cisco Unified Communications Manager
- Communication Between Applications and Cisco Unified Communications Manager
- Communication Between CTL Client and Firewalls
- Special Ports on HP Servers

See “Port Descriptions” for port details in each of the above categories.
Cisco has not verified all possible configuration scenarios for these ports. If you are having configuration problems using this list, contact Cisco technical support for assistance.

Port references apply specifically to Cisco Unified Communications Manager. Some ports change from one release to another, and future releases may introduce new ports. Therefore, make sure that you are using the correct version of this document for the version of Cisco Unified Communications Manager that is installed.

While virtually all protocols are bidirectional, directionality from the session originator perspective is presumed. In some cases, the administrator can manually change the default port numbers, though Cisco does not recommend this as a best practice. Be aware that Cisco Unified Communications Manager opens several ports strictly for internal use.

Installing Cisco Unified Communications Manager software automatically installs the following network services for serviceability and activates them by default. Refer to “Intracluster Ports Between Cisco Unified Communications Manager Servers” for details:

- Cisco Log Partition Monitoring (To monitor and purge the common partition. This uses no custom common port.)
- Cisco Trace Collection Service (TCTS port usage)
- Cisco RIS Data Collector (RIS server port usage)
- Cisco AMC Service (AMC port usage)

Configuration of firewalls, ACLs, or QoS will vary depending on topology, placement of telephony devices and services relative to the placement of network security devices, and which applications and telephony extensions are in use. Also, bear in mind that ACLs vary in format with different devices and versions.

You can also configure Multicast Music on Hold (MOH) ports in Cisco Unified Communications Manager. Port values for multicast MOH are not provided because the administrator specifies the actual port values.

The ephemeral port range for the system is 32768 to 61000. For more information, see http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html.

Make sure that you configure your firewall so that connections to port 22 are open, and are not throttled. During the installation of IM and Presence subscriber nodes, multiple connections to the Cisco Unified Communications Manager publisher node are opened in quick succession. Throttling these connections could lead to a failed installation.

Port Descriptions

- Intracluster Ports Between Cisco Unified Communications Manager Servers, on page 317
Intracluster Ports Between Cisco Unified Communications Manager Servers

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Destination Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint</td>
<td>Unified Communications Manager</td>
<td>514 / UDP</td>
<td>System logging service</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>RTMT</td>
<td>1090, 1099 / TCP</td>
<td>Cisco AMC Service for RTMT performance monitors, data collection, logging, and alerting</td>
</tr>
<tr>
<td>Unified Communications Manager (DB)</td>
<td>Unified Communications Manager (DB)</td>
<td>1500, 1501 / TCP</td>
<td>Database connection (1501 / TCP is the secondary connection)</td>
</tr>
<tr>
<td>Unified Communications Manager (DB)</td>
<td>Unified Communications Manager (DB)</td>
<td>1510 / TCP</td>
<td>CAR IDS DB. CAR IDS engine listens on waiting for connection requests from the clients.</td>
</tr>
<tr>
<td>Unified Communications Manager (DB)</td>
<td>Unified Communications Manager (DB)</td>
<td>1511 / TCP</td>
<td>CAR IDS DB. An alternate port used to bring up a second instance of CAR IDS during upgrade.</td>
</tr>
<tr>
<td>Unified Communications Manager (DB)</td>
<td>Unified Communications Manager (DB)</td>
<td>1515 / TCP</td>
<td>Database replication between nodes during installation</td>
</tr>
<tr>
<td>From (Sender)</td>
<td>To (Listener)</td>
<td>Destination Port</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Cisco Extended Functions (QRT)</td>
<td>Unified Communications Manager (DB)</td>
<td>2552 / TCP</td>
<td>Allows subscribers to receive Cisco Unified Communications Manager database change notification</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Unified Communications Manager</td>
<td>2551 / TCP</td>
<td>Intracluster communication between Cisco Extended Services for Active/Backup determination</td>
</tr>
<tr>
<td>Unified Communications Manager (RIS)</td>
<td>Unified Communications Manager (RIS)</td>
<td>2555 / TCP</td>
<td>Real-time Information Services (RIS) database server</td>
</tr>
<tr>
<td>Unified Communications Manager (RTMT/AMC/SOAP)</td>
<td>Unified Communications Manager (RIS)</td>
<td>2556 / TCP</td>
<td>Real-time Information Services (RIS) database client for Cisco RIS</td>
</tr>
<tr>
<td>Unified Communications Manager (DRS)</td>
<td>Unified Communications Manager (DRS)</td>
<td>4040 / TCP</td>
<td>DRS Master Agent</td>
</tr>
<tr>
<td>Unified Communications Manager (Tomcat)</td>
<td>Unified Communications Manager (SOAP)</td>
<td>5001/TCP</td>
<td>This port is used by SOAP monitor for Real Time Monitoring Service.</td>
</tr>
<tr>
<td>Unified Communications Manager (Tomcat)</td>
<td>Unified Communications Manager (SOAP)</td>
<td>5002/TCP</td>
<td>This port is used by SOAP monitor for Performance Monitor Service.</td>
</tr>
<tr>
<td>Unified Communications Manager (Tomcat)</td>
<td>Unified Communications Manager (SOAP)</td>
<td>5003/TCP</td>
<td>This port is used by SOAP monitor for Control Center Service.</td>
</tr>
<tr>
<td>Unified Communications Manager (Tomcat)</td>
<td>Unified Communications Manager (SOAP)</td>
<td>5004/TCP</td>
<td>This port is used by SOAP monitor for Log Collection Service.</td>
</tr>
<tr>
<td>Standard CCM Admin Users / Admin</td>
<td>Unified Communications Manager</td>
<td>5005 / TCP</td>
<td>This port is used by SOAP CDROnDemand2 services</td>
</tr>
<tr>
<td>Unified Communications Manager (Tomcat)</td>
<td>Unified Communications Manager (SOAP)</td>
<td>5007 / TCP</td>
<td>SOAP monitor</td>
</tr>
<tr>
<td>Unified Communications Manager (RTMT)</td>
<td>Unified Communications Manager (TCTS)</td>
<td>Ephemeral / TCP</td>
<td>Cisco Trace Collection Tool Service (TCTS) -- the back end service for RTMT Trace and Log Central (TLC)</td>
</tr>
<tr>
<td>From (Sender)</td>
<td>To (Listener)</td>
<td>Destination Port</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------------------------------------</td>
<td>------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Unified Communications Manager (Tomcat)</td>
<td>Unified Communications Manager (TCTS)</td>
<td>7000, 7001, 7002 / TCP</td>
<td>This port is used for communication between Cisco Trace Collection Tool Service and Cisco Trace Collection servlet.</td>
</tr>
<tr>
<td>Unified Communications Manager (DB)</td>
<td>Unified Communications Manager (CDLM)</td>
<td>8001 / TCP</td>
<td>Client database change notification</td>
</tr>
<tr>
<td>Unified Communications Manager (SDL)</td>
<td>Unified Communications Manager (SDL)</td>
<td>8002 / TCP</td>
<td>Intracluster communication service</td>
</tr>
<tr>
<td>Unified Communications Manager (SDL)</td>
<td>Unified Communications Manager (SDL)</td>
<td>8003 / TCP</td>
<td>Intracluster communication service (to CTI)</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>CMI Manager</td>
<td>8004 / TCP</td>
<td>Intracluster communication between Cisco Unified Communications Manager and CMI Manager</td>
</tr>
<tr>
<td>Unified Communications Manager (Tomcat)</td>
<td>Unified Communications Manager (Tomcat)</td>
<td>8005 / TCP</td>
<td>Internal listening port used by Tomcat shutdown scripts</td>
</tr>
<tr>
<td>Unified Communications Manager (Tomcat)</td>
<td>Unified Communications Manager (Tomcat)</td>
<td>8080 / TCP</td>
<td>Communication between servers used for diagnostic tests</td>
</tr>
<tr>
<td>Gateway</td>
<td>Unified Communications Manager</td>
<td>8090</td>
<td>HTTP Port for communication between CuCM and GW (Cayuga interface) for Gateway Recording feature.</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Gateway</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unified Communications Manager (IPSec)</td>
<td>Unified Communications Manager (IPSec)</td>
<td>8500 / TCP and UDP</td>
<td>Intracluster replication of system data by IPSec Cluster Manager</td>
</tr>
<tr>
<td>Unified Communications Manager (RIS)</td>
<td>Unified Communications Manager (RIS)</td>
<td>8888 - 8889 / TCP</td>
<td>RIS Service Manager status request and reply</td>
</tr>
<tr>
<td>Location Bandwidth Manager (LBM)</td>
<td>Location Bandwidth Manager (LBM)</td>
<td>9004 / TCP</td>
<td>Intracluster communication between LBMIs</td>
</tr>
<tr>
<td>Unified Communications Manager Publisher</td>
<td>Unified Communications Manager Subscriber</td>
<td>22 / TCP</td>
<td>Cisco SFTP service. You must open this port when installing a new subscriber.</td>
</tr>
</tbody>
</table>
## Common Service Ports

**Table 40: Common Service Ports**

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Destination Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint</td>
<td>Unified Communications Manager</td>
<td>7</td>
<td>Internet Control Message Protocol (ICMP) This protocol number carries echo-related traffic. It does not constitute a port as indicated in the column heading.</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Endpoint</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unified Communications Manager (DRS, CDR)</td>
<td>SFTP server</td>
<td>22 / TCP</td>
<td>Send the backup data to SFTP server. (DRS Local Agent) Send the CDR data to SFTP server.</td>
</tr>
<tr>
<td>Endpoint</td>
<td>Unified Communications Manager (DHCP Server)</td>
<td>67 / UDP</td>
<td>Cisco Unified Communications Manager acting as a DHCP server</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>DHCP Server</td>
<td>68 / UDP</td>
<td>Cisco Unified Communications Manager acting as a DHCP client</td>
</tr>
</tbody>
</table>

**Note**: Cisco does not recommend running DHCP server on Cisco Unified Communications Manager.

**Note**: Configure Cisco Unified Communications Manager with static IP addresses instead.
<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Destination Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint or Gateway</td>
<td>Unified Communications Manager</td>
<td>69, 6969, then Ephemeral / UDP</td>
<td>Trivial File Transfer Protocol (TFTP) service to phones and gateways</td>
</tr>
<tr>
<td>Endpoint or Gateway</td>
<td>Unified Communications Manager</td>
<td>6970 / TCP</td>
<td>Trivial File Transfer Protocol (TFTP) between master and proxy servers. HTTP service from the TFTP server to phones and gateways.</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>NTP Server</td>
<td>123 / UDP</td>
<td>Network Time Protocol (NTP)</td>
</tr>
<tr>
<td>SNMP Server</td>
<td>Unified Communications Manager</td>
<td>161 / UDP</td>
<td>SNMP service response (requests from management applications)</td>
</tr>
<tr>
<td>CUCM Server SNMP Master Agent application</td>
<td>SNMP trap destination</td>
<td>162 / UDP</td>
<td>SNMP traps</td>
</tr>
<tr>
<td>SNMP Server</td>
<td>Unified Communications Manager</td>
<td>199 / TCP</td>
<td>Native SNMP agent listening port for SMUX support</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>DHCP Server</td>
<td>546 / UDP</td>
<td>DHCPv6. DHCP port for IPv6.</td>
</tr>
<tr>
<td>Unified Communications Manager Serviceability</td>
<td>Location Bandwidth Manager (LBM)</td>
<td>5546 / TCP</td>
<td>Enhanced Location CAC Serviceability</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Location Bandwidth Manager (LBM)</td>
<td>5547 / TCP</td>
<td>Call Admission requests and bandwidth deductions</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Unified Communications Manager</td>
<td>6161 / UDP</td>
<td>Used for communication between Master Agent and Native Agent to process Native agent MIB requests</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Unified Communications Manager</td>
<td>6162 / UDP</td>
<td>Used for communication between Master Agent and Native Agent to forward notifications generated from Native Agent</td>
</tr>
<tr>
<td>Centralized TFTP</td>
<td>Alternate TFTP</td>
<td>6970 / TCP</td>
<td>Centralized TFTP File Locator Service</td>
</tr>
<tr>
<td>From (Sender)</td>
<td>To (Listener)</td>
<td>Destination Port</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------</td>
<td>------------------</td>
<td>----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Unified Communications Manager</td>
<td>7161 / TCP</td>
<td>Used for communication between SNMP Master Agent and subagents</td>
</tr>
<tr>
<td>SNMP Server</td>
<td>Unified Communications Manager</td>
<td>7999 / TCP</td>
<td>Cisco Discovery Protocol (CDP) agent communicates with CDP executable</td>
</tr>
<tr>
<td>Endpoint</td>
<td>Unified Communications Manager</td>
<td>443, 8443 / TCP</td>
<td>Used for Cisco User Data Services (UDS) requests</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Unified Communications Manager</td>
<td>9050 / TCP</td>
<td>Service CRS requests through the TAPS residing on Cisco Unified Communications Manager</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Unified Communications Manager</td>
<td>61441 / UDP</td>
<td>Cisco Unified Communications Manager applications send out alarms to this port through UDP. Cisco Unified Communications Manager MIB agent listens on this port and generates SNMP traps per Cisco Unified Communications Manager MIB definition.</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Unified Communications Manager</td>
<td>5060, 5061 / TCP</td>
<td>Provide trunk-based SIP services</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Unified Communications Manager</td>
<td>7501</td>
<td>Used by Intercluster Lookup Service (ILS) for certificate based authentication.</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Unified Communications Manager</td>
<td>7502</td>
<td>Used by ILS for password based authentication.</td>
</tr>
<tr>
<td>--</td>
<td>--</td>
<td>8000-48198</td>
<td>ASR and ISR G3 platforms default port range.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>16384-32766</td>
<td>ISR G2 platform default port range.</td>
</tr>
</tbody>
</table>
### Ports Between Cisco Unified Communications Manager and LDAP Directory

**Table 41: Ports Between Cisco Unified Communications Manager and LDAP Directory**

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Destination Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Directory</td>
<td>Unified Communications Manager</td>
<td>Ephemeral</td>
<td></td>
</tr>
</tbody>
</table>

### Web Requests From CCMAdmin or CCMUser to Cisco Unified Communications Manager

**Table 42: Web Requests From CCMAdmin or CCMUser to Cisco Unified Communications Manager**

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Destination Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser</td>
<td>Unified Communications Manager</td>
<td>80, 8080 / TCP</td>
<td>Hypertext Transport Protocol (HTTP)</td>
</tr>
<tr>
<td>Browser</td>
<td>Unified Communications Manager</td>
<td>443, 8443 / TCP</td>
<td>Hypertext Transport Protocol over SSL (HTTPS)</td>
</tr>
</tbody>
</table>

### Web Requests From Cisco Unified Communications Manager to Phone

**Table 43: Web Requests From Cisco Unified Communications Manager to Phone**

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Destination Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Communications Manager</td>
<td>Phone</td>
<td>80 / TCP</td>
<td>Hypertext Transport Protocol (HTTP)</td>
</tr>
<tr>
<td>• QRT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• RTMT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Find and List Phones page</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Phone Configuration page</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Signaling, Media, and Other Communication Between Phones and Cisco Unified Communications Manager

### Table 44: Signaling, Media, and Other Communication Between Phones and Cisco Unified Communications Manager

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Destination Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone</td>
<td>Unified Communications Manager</td>
<td>53/ TCP</td>
<td>Session Initiation Protocol (SIP) phones resolve the Fully Qualified Domain Name (FQDN) using a Domain Name System (DNS)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note</strong> By default, some wireless access points block TCP 53 port, which prevents wireless SIP phones from registering when CUCM is configured using FQDN.</td>
</tr>
<tr>
<td>Phone</td>
<td>Unified Communications Manager (TFTP)</td>
<td>69, then Ephemeral / UDP</td>
<td>Trivial File Transfer Protocol (TFTP) used to download firmware and configuration files</td>
</tr>
<tr>
<td>Phone</td>
<td>Unified Communications Manager</td>
<td>2000 / TCP</td>
<td>Skinny Client Control Protocol (SCCP)</td>
</tr>
<tr>
<td>Phone</td>
<td>Unified Communications Manager</td>
<td>2443 / TCP</td>
<td>Secure Skinny Client Control Protocol (SCCPS)</td>
</tr>
<tr>
<td>Phone</td>
<td>Unified Communications Manager</td>
<td>2445 / TCP</td>
<td>Provide trust verification service to endpoints.</td>
</tr>
<tr>
<td>Phone</td>
<td>Unified Communications Manager (CAPF)</td>
<td>3804 / TCP</td>
<td>Certificate Authority Proxy Function (CAPF) listening port for issuing Locally Significant Certificates (LSCs) to IP phones</td>
</tr>
<tr>
<td>From (Sender)</td>
<td>To (Listener)</td>
<td>Destination Port</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------</td>
<td>------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>Phone</td>
<td>Unified Communications Manager</td>
<td>5060 / TCP and UDP</td>
<td>Session Initiation Protocol (SIP) phone</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Phone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone</td>
<td>Unified Communications Manager</td>
<td>5061 TCP</td>
<td>Secure Session Initiation Protocol (SIPS) phone</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Phone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone</td>
<td>Unified Communications Manager (TFTP)</td>
<td>6970 TCP</td>
<td>HTTP-based download of firmware and configuration files</td>
</tr>
<tr>
<td>Phone</td>
<td>Unified Communications Manager (TFTP)</td>
<td>6971, 6972 / TCP</td>
<td>HTTPS interface to TFTP. Phones use this port to download a secure configuration file from TFTP.</td>
</tr>
<tr>
<td>Phone</td>
<td>Unified Communications Manager</td>
<td>8080 / TCP</td>
<td>Phone URLs for XML applications, authentication, directories, services, etc. You can configure these ports on a per-service basis.</td>
</tr>
<tr>
<td>Phone</td>
<td>Unified Communications Manager</td>
<td>9443 / TCP</td>
<td>Phone use this port for authenticated contact search.</td>
</tr>
<tr>
<td>IP VMS</td>
<td>Phone</td>
<td>16384 - 32767 / UDP</td>
<td>Real-Time Protocol (RTP), Secure Real-Time Protocol (SRTP)</td>
</tr>
<tr>
<td>Phone</td>
<td>IP VMS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note** Cisco Unified Communications Manager only uses 24576-32767 although other devices use the full range.
Signaling, Media, and Other Communication Between Gateways and Cisco Unified Communications Manager

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Destination Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway</td>
<td>Unified Communications Manager</td>
<td>47, 50, 51</td>
<td>Generic Routing Encapsulation (GRE), Encapsulating Security Payload (ESP), Authentication Header (AH). These protocols numbers carry encrypted IPSec traffic. They do not constitute a port as indicated in the column heading.</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Gateway</td>
<td></td>
<td>Internet Key Exchange (IKE) for IP Security protocol (IPSec) establishment</td>
</tr>
<tr>
<td>Gateway</td>
<td>Unified Communications Manager</td>
<td>500 / UDP</td>
<td>Trivial File Transfer Protocol (TFTP)</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Gateway</td>
<td></td>
<td>Port mapping service. Only used in the CIME off-path deployment model.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Unified Communications Manager (TFTP)</td>
<td>69, then Ephemeral / UDP</td>
<td>Gatekeeper (H.225) RAS</td>
</tr>
<tr>
<td>Unified Communications Manager with Cisco Intercompany Media Engine (CIME) trunk</td>
<td>CIME ASA</td>
<td>1024-65535 / TCP</td>
<td>H.225 signaling services for H.323 gateways and Intercluster Trunk (ICT)</td>
</tr>
<tr>
<td>Gatekeeper</td>
<td>Unified Communications Manager</td>
<td>1719 / UDP</td>
<td>H.225 signaling services on gatekeeper-controlled trunk</td>
</tr>
<tr>
<td>Gateway</td>
<td>Unified Communications Manager</td>
<td>1720 / TCP</td>
<td></td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Gateway</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td>Unified Communications Manager</td>
<td>Ephemeral / TCP</td>
<td></td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Gateway</td>
<td></td>
<td></td>
</tr>
<tr>
<td>From (Sender)</td>
<td>To (Listener)</td>
<td>Destination Port</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Gateway</td>
<td>Unified Communications Manager</td>
<td>Ephemeral / TCP</td>
<td>H.245 signaling services for establishing voice, video, and data</td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td></td>
<td>The H.245 port used by the remote system depends on the type of gateway.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For IOS gateways, the H.245 port range is from 11000 to 65535.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Unified Communications Manager</td>
<td>2000 / TCP</td>
<td>Skinny Client Control Protocol (SCCP)</td>
</tr>
<tr>
<td>Gateway</td>
<td>Unified Communications Manager</td>
<td>2001 / TCP</td>
<td>Upgrade port for 6608 gateways with Cisco Unified Communications Manager deployments</td>
</tr>
<tr>
<td>Gateway</td>
<td>Unified Communications Manager</td>
<td>2002 / TCP</td>
<td>Upgrade port for 6624 gateways with Cisco Unified Communications Manager deployments</td>
</tr>
<tr>
<td>Gateway</td>
<td>Unified Communications Manager</td>
<td>2427 / UDP</td>
<td>Media Gateway Control Protocol (MGCP) gateway control</td>
</tr>
<tr>
<td>Gateway</td>
<td>Unified Communications Manager</td>
<td>2428 / TCP</td>
<td>Media Gateway Control Protocol (MGCP) backhaul</td>
</tr>
<tr>
<td>--</td>
<td>--</td>
<td>4000 - 4005 / TCP</td>
<td>These ports are used as phantom Real-Time Transport Protocol (RTP) and Real-Time Transport Control Protocol (RTCP) ports for audio, video and data channel when Cisco Unified Communications Manager does not have ports for these media.</td>
</tr>
</tbody>
</table>
### Communication Between Applications and Cisco Unified Communications Manager

#### Table 46: Communication Between Applications and Cisco Unified Communications Manager

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Destination Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway</td>
<td>Unified Communications Manager</td>
<td>5060 / TCP and UDP</td>
<td>Session Initiation Protocol (SIP) gateway and Intercluster Trunk (ICT)</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Gateway</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td>Unified Communications Manager</td>
<td>5061 / TCP</td>
<td>Secure Session Initiation Protocol (SIPS) gateway and Intercluster Trunk (ICT)</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Gateway</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td>Unified Communications Manager</td>
<td>16384 - 32767 / UDP</td>
<td>Real-Time Protocol (RTP), Secure Real-Time Protocol (SRTP)</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Gateway</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note**: Cisco Unified Communications Manager only uses 24576-32767 although other devices use the full range.
<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Destination Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Communications Manager</td>
<td>Unified Communications Manager</td>
<td>2912 / TCP</td>
<td>Cisco Unified Communications Manager Assistant server (formerly IPMA)</td>
</tr>
<tr>
<td>Manager Attendant Console</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Unified Communications Manager</td>
<td>1103-1129 / TCP</td>
<td>Cisco Unified Communications Manager Attendant Console (AC) JAVA RMI Registry server</td>
</tr>
<tr>
<td>Manager Attendant Console</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Unified Communications Manager</td>
<td>1101 / TCP</td>
<td>RMI server sends RMI callback messages to clients on these ports.</td>
</tr>
<tr>
<td>Manager Attendant Console</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Unified Communications Manager</td>
<td>1102 / TCP</td>
<td>Attendant Console (AC) RMI server bind port -- RMI server sends RMI messages on these ports.</td>
</tr>
<tr>
<td>Manager Attendant Console</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Unified Communications Manager</td>
<td>3223 / UDP</td>
<td>Cisco Unified Communications Manager Attendant Console (AC) server line state port receives ping and registration message from, and sends line states to, the attendant console server.</td>
</tr>
<tr>
<td>Manager Attendant Console</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Unified Communications Manager</td>
<td>3224 / UDP</td>
<td>Cisco Unified Communications Manager Attendant Console (AC) clients register with the AC server for line and device state information.</td>
</tr>
<tr>
<td>Manager Attendant Console</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Unified Communications Manager</td>
<td>4321 / UDP</td>
<td>Cisco Unified Communications Manager Attendant Console (AC) clients register to the AC server for call control.</td>
</tr>
<tr>
<td>Manager Attendant Console</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>IOS Router running SAF image</td>
<td>5050 / TCP</td>
<td>Multi-Service IOS Router running EIGRP/SAF Protocol.</td>
</tr>
<tr>
<td>From (Sender)</td>
<td>To (Listener)</td>
<td>Destination Port</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Unified Communications Manager</td>
<td>Cisco Intercompany Media Engine (IME) Server</td>
<td>5620 / TCP</td>
<td>VAP protocol used to communicate to the Cisco Intercompany Media Engine server. If Cisco recommends a value of 5620 for this port, but you can change the value by executing the <code>add ime vapserver</code> or <code>set ime vapserver port</code> CLI command on the Cisco IME server.</td>
</tr>
<tr>
<td>Cisco Unified Communications App</td>
<td>Unified Communications Manager</td>
<td>8443 / TCP</td>
<td>AXL / SOAP API for programmatic reads from or writes to the Cisco Unified Communications Manager database that third parties such as billing or telephony management applications use.</td>
</tr>
</tbody>
</table>

**Communication Between CTL Client and Firewalls**

*Table 47: Communication Between CTL Client and Firewalls*

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Destination Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTL Client</td>
<td>TLS Proxy Server</td>
<td>2444 / TCP</td>
<td>Certificate Trust List (CTL) provider listening service in an ASA firewall</td>
</tr>
</tbody>
</table>

**Special Ports on HP Servers**

*Table 48: Special Ports on HP Servers*

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Destination Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint</td>
<td>HP SIM</td>
<td>2301 / TCP</td>
<td>HTTP port to HP agent</td>
</tr>
<tr>
<td>Endpoint</td>
<td>HP SIM</td>
<td>2381 / TCP</td>
<td>HTTPS port to HP agent</td>
</tr>
<tr>
<td>Endpoint</td>
<td>Compaq Management Agent</td>
<td>25375, 25376, 25393 / UDP</td>
<td>COMPAQ Management Agent extension (cmaX)</td>
</tr>
<tr>
<td>Endpoint</td>
<td>HP SIM</td>
<td>50000 - 50004 / TCP</td>
<td>HTTPS port to HP SIM</td>
</tr>
</tbody>
</table>
Port References

Firewall Application Inspection Guides
ASA Series reference information
PIX Application Inspection Configuration Guides
FWSM 3.1 Application Inspection Configuration Guide

IETF TCP/UDP Port Assignment List
Internet Assigned Numbers Authority (IANA) IETF assigned Port List
http://www.iana.org/assignments/port-numbers

IP Telephony Configuration and Port Utilization Guides
Cisco CRS 4.0 (IP IVR and IPCC Express) Port Utilization Guide
Port Utilization Guide for Cisco ICM/IPCC Enterprise and Hosted Editions
Cisco Unified Communications Manager Express Security Guide to Best Practices
Cisco Unity Express Security Guide to Best Practices

VMware Port Assignment List
TCP and UDP Ports for vCenter Server, ESX hosts, and Other Network Components Management Access
Port Usage Information for the IM and Presence Service

IM and Presence Service Port Usage Overview

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

Note

Cisco has not verified all possible configuration scenarios for these ports. If you are having configuration problems using this list, contact Cisco technical support for assistance.

While virtually all protocols are bidirectional, this document gives directionality from the session originator perspective. In some cases, the administrator can manually change the default port numbers, though Cisco does not recommend this as a best practice. Be aware that the IM and Presence Service opens several ports strictly for internal use.

Ports in this document apply specifically to the IM and Presence Service. Some ports change from one release to another, and future releases may introduce new ports. Therefore, make sure that you are using the correct version of this document for the version of IM and Presence Service that is installed.

Configuration of firewalls, ACLs, or QoS will vary depending on topology, placement of devices and services relative to the placement of network security devices, and which applications and telephony extensions are in use. Also, bear in mind that ACLs vary in format with different devices and versions.

Information Collated in Table

This table defines the information collated in each of the tables in this document.
**Table 49: Definition of Table Information**

<table>
<thead>
<tr>
<th>Table Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>The client sending requests to this port</td>
</tr>
<tr>
<td>To</td>
<td>The client receiving requests on this port</td>
</tr>
<tr>
<td>Role</td>
<td>A client or server application or process</td>
</tr>
<tr>
<td>Protocol</td>
<td>Either a Session-layer protocol used for establishing and ending communications, or an Application-layer protocol used for request and response transactions</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>A Transport-layer protocol that is connection-oriented (TCP) or connectionless (UDP)</td>
</tr>
<tr>
<td>Destination / Listener</td>
<td>The port used for receiving requests</td>
</tr>
<tr>
<td>Source / Sender</td>
<td>The port used for sending requests</td>
</tr>
</tbody>
</table>

**IM and Presence Service Port List**

The following tables show the ports that the IM and Presence Service uses for intracluster and intercluster traffic.

**Table 50: IM and Presence Service Ports - SIP Proxy Requests**

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Gateway</td>
<td>IM and Presence</td>
<td>SIP</td>
<td>TCP/UDP</td>
<td>5060</td>
<td>Ephemeral</td>
<td>Default SIP Proxy UDP and TCP Listener</td>
</tr>
<tr>
<td>IM and Presence</td>
<td>SIP Gateway</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal port. Localhost traffic only.</td>
<td>Used for HTTP requests from the Config Agent to indicate a change in configuration.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 51: IM and Presence Service Ports - Presence Engine Requests

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-party Client</td>
<td>IM and Presence</td>
<td>HTTP</td>
<td>TCP</td>
<td>8082</td>
<td>Ephemeral</td>
<td>Default IM and Presence HTTP Listener. Used for Third-Party Clients to connect</td>
</tr>
<tr>
<td>Third-party Client</td>
<td>IM and Presence</td>
<td>HTTPS</td>
<td>TLS / TCP</td>
<td>8083</td>
<td>Ephemeral</td>
<td>Default IM and Presence HTTPS Listener. Used for Third-Party Clients to connect</td>
</tr>
</tbody>
</table>

### Table 52: IM and Presence Service Ports - Cisco Tomcat WebRequests

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence (Presence Engine)</td>
<td>IM and Presence (Presence Engine)</td>
<td>SIP</td>
<td>UDP / TCP</td>
<td>5080</td>
<td>Ephemeral</td>
<td>Default SIP UDP/TCP Listener port</td>
</tr>
<tr>
<td>IM and Presence (Presence Engine)</td>
<td>IM and Presence (Presence Engine)</td>
<td>Livebus</td>
<td>UDP</td>
<td>50000</td>
<td>Ephemeral</td>
<td>Internal port. Localhost traffic only. LiveBus messaging port. The IM and Presence Service uses this port for cluster communication.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser</td>
<td>IM and Presence</td>
<td>HTTPS</td>
<td>TCP</td>
<td>8080</td>
<td>Ephemeral</td>
<td>Used for web access</td>
</tr>
<tr>
<td>Browser</td>
<td>IM and Presence</td>
<td>AXL / HTTPS</td>
<td>TLS / TCP</td>
<td>8443</td>
<td>Ephemeral</td>
<td>Provides database and serviceability access via SOAP</td>
</tr>
<tr>
<td>Browser</td>
<td>IM and Presence</td>
<td>HTTPS</td>
<td>TLS / TCP</td>
<td>8443</td>
<td>Ephemeral</td>
<td>Provides access to Web administration</td>
</tr>
<tr>
<td>Browser</td>
<td>IM and Presence</td>
<td>HTTPS</td>
<td>TLS / TCP</td>
<td>8443</td>
<td>Ephemeral</td>
<td>Provides access to User option pages</td>
</tr>
<tr>
<td>From (Sender)</td>
<td>To (Listener)</td>
<td>Protocol</td>
<td>Transport Protocol</td>
<td>Destination / Listener</td>
<td>Source / Sender</td>
<td>Remarks</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------</td>
<td>----------</td>
<td>--------------------</td>
<td>-----------------------</td>
<td>----------------</td>
<td>---------</td>
</tr>
<tr>
<td>Browser</td>
<td>IM and Presence</td>
<td>SOAP</td>
<td>TLS / TCP</td>
<td>8443</td>
<td>Ephemeral</td>
<td>Provides access to Cisco Unified Personal Communicator, Cisco Unified Mobility Advantage, and third-party API clients via SOAP</td>
</tr>
</tbody>
</table>

Table 53: IM and Presence Service Ports - External Corporate Directory Requests

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence External Corporate Directory</td>
<td>External Corporate Directory</td>
<td>LDAP</td>
<td>TCP</td>
<td>389 / 3268</td>
<td>Ephemeral</td>
<td>Allows the Directory protocol to integrate with the external Corporate Directory. The LDAP port depends on the Corporate Directory (389 is the default). In case of Netscape Directory, customer can configure different port to accept LDAP traffic. Allows LDAP to communicate between IM&amp;P and the LDAP server for authentication.</td>
</tr>
<tr>
<td>IM and Presence External Corporate Directory</td>
<td>External Corporate Directory</td>
<td>LDAPS</td>
<td>TCP</td>
<td>636</td>
<td>Ephemeral</td>
<td>Allows the Directory protocol to integrate with the external Corporate Directory. LDAP port depends on the Corporate Directory (636 is the default).</td>
</tr>
</tbody>
</table>

Table 54: IM and Presence Service Ports - Configuration Requests

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence (Config Agent)</td>
<td>IM and Presence (Config Agent)</td>
<td>TCP</td>
<td>TCP</td>
<td>8600</td>
<td>Ephemeral</td>
<td>Config Agent heartbeat port</td>
</tr>
</tbody>
</table>
Table 55: IM and Presence Service Ports - Certificate Manager Requests

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence</td>
<td>Certificate Manager</td>
<td>TCP</td>
<td>TCP</td>
<td>7070</td>
<td>Ephemeral</td>
<td>Internal port - Localhost traffic only</td>
</tr>
</tbody>
</table>

Table 56: IM and Presence Service Ports - IDS Database Requests

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence (Database)</td>
<td>IM and Presence (Database)</td>
<td>TCP</td>
<td>TCP</td>
<td>1500</td>
<td>Ephemeral</td>
<td>Internal IDS port for Database clients. Localhost traffic only.</td>
</tr>
<tr>
<td>IM and Presence (Database)</td>
<td>IM and Presence (Database)</td>
<td>TCP</td>
<td>TCP</td>
<td>1501</td>
<td>Ephemeral</td>
<td>Internal port - this is an alternate port to bring up a second instance of IDS during upgrade. Localhost traffic only.</td>
</tr>
<tr>
<td>IM and Presence (Database)</td>
<td>IM and Presence (Database)</td>
<td>XML</td>
<td>TCP</td>
<td>1515</td>
<td>Ephemeral</td>
<td>Internal port. Localhost traffic only. DB replication port</td>
</tr>
</tbody>
</table>

Table 57: IM and Presence Service Ports - IPSec Manager Requests

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence (IPSec)</td>
<td>IM and Presence (IPSec)</td>
<td>Proprietary</td>
<td>UDP/TCP</td>
<td>8500</td>
<td>8500</td>
<td>Internal port - cluster manager port used by the ipsec_mngr daemon for cluster replication of platform data (hosts) certs</td>
</tr>
</tbody>
</table>

Table 58: IM and Presence Service Ports - DRF Master Agent Server Requests

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence (DRF)</td>
<td>IM and Presence (DRF)</td>
<td>TCP</td>
<td>TCP</td>
<td>4040</td>
<td>Ephemeral</td>
<td>DRF Master Agent server port, which accepts connections from Local Agent, GUI, and CLI</td>
</tr>
</tbody>
</table>
### Table 59: IM and Presence Service Ports - RISDC Requests

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence (RIS)</td>
<td>IM and Presence (RIS)</td>
<td>TCP</td>
<td>TCP</td>
<td>2555</td>
<td>Ephemeral</td>
<td>Real-time Information Services (RIS) database server. Connects to other RISDC services in the cluster to provide clusterwide real-time information</td>
</tr>
<tr>
<td>IM and Presence (RTMT/AMC/SOAP)</td>
<td>IM and Presence (RIS)</td>
<td>TCP</td>
<td>TCP</td>
<td>2556</td>
<td>Ephemeral</td>
<td>Real-time Information Services (RIS) database client for Cisco RIS. Allows RIS client connection to retrieve real-time information</td>
</tr>
<tr>
<td>IM and Presence (RIS)</td>
<td>IM and Presence (RIS)</td>
<td>TCP</td>
<td>TCP</td>
<td>8889</td>
<td>8888</td>
<td>Internal port. Localhost traffic only. Used by RISDC (System Access) to link to servM via TCP for service status request and reply</td>
</tr>
</tbody>
</table>

### Table 60: IM and Presence Service Ports - SNMP Requests

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Server</td>
<td>IM and Presence</td>
<td>SNMP</td>
<td>UDP</td>
<td>161, 8161</td>
<td>Ephemeral</td>
<td>Provides services for SNMP-based management applications</td>
</tr>
<tr>
<td>IM and Presence</td>
<td>IM and Presence</td>
<td>SNMP</td>
<td>UDP</td>
<td>6162</td>
<td>Ephemeral</td>
<td>Native SNMP agent that listens for requests forwarded by SNMP master agents</td>
</tr>
<tr>
<td>IM and Presence</td>
<td>IM and Presence</td>
<td>SNMP</td>
<td>UDP</td>
<td>6161</td>
<td>Ephemeral</td>
<td>SNMP Master agent that listens for traps from the native SNMP agent, and forwards to management applications</td>
</tr>
<tr>
<td>SNMP Server</td>
<td>IM and Presence</td>
<td>TCP</td>
<td>TCP</td>
<td>7999</td>
<td>Ephemeral</td>
<td>Used as a socket for the cdp agent to communicate with the cdp binary</td>
</tr>
</tbody>
</table>

---

**Reference Information**

*IM and Presence Service Port List*

---

**Configuration and Administration for the IM and Presence Service, Release 11.5(1)SU5**

338
<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence</td>
<td>IM and Presence</td>
<td>TCP</td>
<td>TCP</td>
<td>7161</td>
<td>7161</td>
<td>Ephemeral. Used for communication between the SNMP master agent and subagents</td>
</tr>
<tr>
<td>IM and Presence</td>
<td>SNMP Trap Monitor</td>
<td>SNMP</td>
<td>UDP</td>
<td>162</td>
<td>162</td>
<td>Ephemeral. Sends SNMP traps to management applications</td>
</tr>
<tr>
<td>IM and Presence</td>
<td>IM and Presence</td>
<td>SNMP</td>
<td>UDP</td>
<td>Configurable</td>
<td>61441</td>
<td>Internal SNMP trap receiver</td>
</tr>
</tbody>
</table>

**Table 61: IM and Presence Service Ports - Racoon Server Requests**

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway ------</td>
<td>-------------</td>
<td>----------</td>
<td>--------------------</td>
<td>------------------------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IM and Presence</td>
<td>Gateway</td>
<td>Ipsec</td>
<td>UDP</td>
<td>500</td>
<td>500</td>
<td>Ephemeral. Enables Internet Security Association and the Key Management Protocol</td>
</tr>
</tbody>
</table>

**Table 62: IM and Presence Service Ports - System Service Requests**

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence</td>
<td>IM and Presence</td>
<td>XML</td>
<td>TCP</td>
<td>8888 and 8889</td>
<td>8888 and 8889</td>
<td>Ephemeral. Internal port. Localhost traffic only. Used to listen to clients communicating with the RIS Service Manager (servM).</td>
</tr>
</tbody>
</table>

**Table 63: IM and Presence Service Ports - DNS Requests**

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence</td>
<td>DNS Server</td>
<td>DNS</td>
<td>UDP</td>
<td>53</td>
<td>53</td>
<td>Ephemeral. The port that DNS server listen on for IM and Presence DNS queries. To: DNS Server</td>
</tr>
</tbody>
</table>
### Table 64: IM and Presence Service Ports - SSH/SFTP Requests

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence</td>
<td>Endpoint</td>
<td>SSH / SFTP</td>
<td>TCP</td>
<td>22</td>
<td>Ephemeral</td>
<td>Used by many applications to get command line access to the server. Also used between nodes for certificate and other file exchanges (sftp)</td>
</tr>
</tbody>
</table>

### Table 65: IM and Presence Service Ports - ICMP Requests

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence</td>
<td>Cisco Unified Communications Manager</td>
<td>ICMP</td>
<td>IP</td>
<td>Not Applicable</td>
<td>Ephemeral</td>
<td>Internet Control Message Protocol (ICMP). Used to communicate with the Cisco Unified Communications Manager server</td>
</tr>
<tr>
<td>Cisco Unified</td>
<td>--------------</td>
<td>---------</td>
<td>-------------------</td>
<td>-----------------------</td>
<td>---------------</td>
<td>---------</td>
</tr>
<tr>
<td>Communications Manager</td>
<td>IM and Presence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 66: IM and Presence Service Ports - NTP Requests

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence</td>
<td>NTP Server</td>
<td>NTP</td>
<td>UDP</td>
<td>123</td>
<td>Ephemeral</td>
<td>Cisco Unified Communications Manager is the acting NTP server. Used by subscriber nodes to synchronize time with the publisher node.</td>
</tr>
</tbody>
</table>
Table 67: IM and Presence Service Ports - Microsoft Exchange Notify Requests

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Exchange</td>
<td>IM and Presence</td>
<td>HTTP (HTTPu)</td>
<td>) WebDAV - HTTP /UDP/IP notifications 2) EWS - HTTP/TCP /IP SOAP notifications</td>
<td>IM and Presence server port (default 50020)</td>
<td>Ephemeral</td>
<td>Microsoft Exchange uses this port to send notifications (using NOTIFY message) to indicate a change to a particular subscription identifier for calendar events. Used to integrate with any Exchange server in the network configuration. Both ports are created. The kind of messages that are sent depend on the type of Calendar Presence Backend gateway(s) that are configured.</td>
</tr>
</tbody>
</table>

Table 68: IM and Presence Service Ports - SOAP Services Requests

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence (Tomcat)</td>
<td>IM and Presence (SOAP)</td>
<td>TCP</td>
<td>TCP</td>
<td>5007</td>
<td>Ephemeral</td>
<td>SOAP monitor port</td>
</tr>
</tbody>
</table>

Table 69: IM and Presence Service Ports - AMC RMI Requests

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
</table>
### Table 70: IM and Presence Service Ports - XCP Requests

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMPP Client</td>
<td>IM and Presence</td>
<td>TCP</td>
<td>TCP</td>
<td>5222</td>
<td>Ephemeral</td>
<td>Client access port</td>
</tr>
<tr>
<td>IM and Presence</td>
<td>IM and Presence</td>
<td>TCP</td>
<td>TCP</td>
<td>5269</td>
<td>Ephemeral</td>
<td>Server to Server connection (S2S) port</td>
</tr>
<tr>
<td>Third-party BOSH client</td>
<td>IM and Presence</td>
<td>TCP</td>
<td>TCP</td>
<td>7335</td>
<td>Ephemeral</td>
<td>HTTP listening port used by the XCP Web Connection Manager for BOSH third-party API connections</td>
</tr>
<tr>
<td>IM and Presence (XCP Services)</td>
<td>IM and Presence (XCP Router)</td>
<td>TCP</td>
<td>TCP</td>
<td>7400</td>
<td>Ephemeral</td>
<td>XCP Router Master Accept Port. XCP services that connect to the router from an Open Port Configuration (for example XCP Authentication Component Service) typically connect on this port.</td>
</tr>
<tr>
<td>IM and Presence (XCP Router)</td>
<td>IM and Presence (XCP Router)</td>
<td>UDP</td>
<td>UDP</td>
<td>5353</td>
<td>Ephemeral</td>
<td>MDNS port. XCP routers in a cluster use this port to discover each other.</td>
</tr>
<tr>
<td>IM and Presence (XCP Router)</td>
<td>IM and Presence (XCP Router)</td>
<td>TCP</td>
<td>TCP</td>
<td>7336</td>
<td>HTTPS</td>
<td>MFT File transfer (On-Premises only).</td>
</tr>
</tbody>
</table>

### Table 71: IM and Presence Service Ports - External Database (PostgreSQL) Requests

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence</td>
<td>PostgreSQL database</td>
<td>TCP</td>
<td>TCP</td>
<td>5432(^1)</td>
<td>Ephemeral</td>
<td>PostgreSQL database listening port</td>
</tr>
</tbody>
</table>

\(^1\) This is the default port, however you can configure the PostgreSQL database to listen on any port.
### Table 72: IM and Presence Service Ports - High Availability Requests

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence (Server Recovery Manager)</td>
<td>IM and Presence (Server Recovery Manager)</td>
<td>TCP</td>
<td>TCP</td>
<td>20075</td>
<td>Ephemeral</td>
<td>The port that Cisco Server Recovery Manager uses to provide admin rpc requests.</td>
</tr>
<tr>
<td>IM and Presence (Server Recovery Manager)</td>
<td>IM and Presence (Server Recovery Manager)</td>
<td>UDP</td>
<td>UDP</td>
<td>22001</td>
<td>Ephemeral</td>
<td>The port that Cisco Server Recovery Manager uses to communicate with its peer.</td>
</tr>
</tbody>
</table>

### Table 73: IM and Presence Service Ports - In Memory Database Replication Messages

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence</td>
<td>IM and Presence</td>
<td>Proprietary</td>
<td>TCP</td>
<td>6603*</td>
<td>Ephemeral</td>
<td>Cisco Presence Datastore</td>
</tr>
<tr>
<td>IM and Presence</td>
<td>IM and Presence</td>
<td>Proprietary</td>
<td>TCP</td>
<td>6604*</td>
<td>Ephemeral</td>
<td>Cisco Login Datastore</td>
</tr>
<tr>
<td>IM and Presence</td>
<td>IM and Presence</td>
<td>Proprietary</td>
<td>TCP</td>
<td>6605*</td>
<td>Ephemeral</td>
<td>Cisco SIP Registration Datastore</td>
</tr>
<tr>
<td>IM and Presence</td>
<td>IM and Presence</td>
<td>Proprietary</td>
<td>TCP</td>
<td>9003</td>
<td>Ephemeral</td>
<td>Cisco Presence Datastore dual node presence redundancy group replication.</td>
</tr>
<tr>
<td>IM and Presence</td>
<td>IM and Presence</td>
<td>Proprietary</td>
<td>TCP</td>
<td>9004</td>
<td>Ephemeral</td>
<td>Cisco Login Datastore dual node presence redundancy group replication.</td>
</tr>
<tr>
<td>IM and Presence</td>
<td>IM and Presence</td>
<td>Proprietary</td>
<td>TCP</td>
<td>9005</td>
<td>Ephemeral</td>
<td>Cisco SIP Registration Datastore dual node presence redundancy group replication.</td>
</tr>
</tbody>
</table>

* If you want to run the Administration CLI Diagnostic Utility, using the `utils imdb_replication status` command, these ports must be open on all firewalls that are configured between IM and Presence Service nodes in the cluster. This setup is not required for normal operation.
Table 74: IM and Presence Service Ports - In Memory Database SQL Messages

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence</td>
<td>IM and Presence</td>
<td>Proprietary</td>
<td>TCP</td>
<td>6603</td>
<td>Ephemeral</td>
<td>Cisco Presence Datastore SQL Queries.</td>
</tr>
<tr>
<td>IM and Presence</td>
<td>IM and Presence</td>
<td>Proprietary</td>
<td>TCP</td>
<td>6604</td>
<td>Ephemeral</td>
<td>Cisco Login Datastore SQL Queries.</td>
</tr>
<tr>
<td>IM and Presence</td>
<td>IM and Presence</td>
<td>Proprietary</td>
<td>TCP</td>
<td>6605</td>
<td>Ephemeral</td>
<td>Cisco SIP Registration Datastore SQL Queries.</td>
</tr>
<tr>
<td>IM and Presence</td>
<td>IM and Presence</td>
<td>Proprietary</td>
<td>TCP</td>
<td>6606</td>
<td>Ephemeral</td>
<td>Cisco Route Datastore SQL Queries.</td>
</tr>
</tbody>
</table>

Table 75: IM and Presence Service Ports - In Memory Database Notification Messages

<table>
<thead>
<tr>
<th>From (Sender)</th>
<th>To (Listener)</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Destination / Listener</th>
<th>Source / Sender</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence</td>
<td>IM and Presence</td>
<td>Proprietary</td>
<td>TCP</td>
<td>6609</td>
<td>Ephemeral</td>
<td>Cisco SIP Registration Datastore XML-based change notification.</td>
</tr>
<tr>
<td>IM and Presence</td>
<td>IM and Presence</td>
<td>Proprietary</td>
<td>TCP</td>
<td>6610</td>
<td>Ephemeral</td>
<td>Cisco Route Datastore XML-based change notification.</td>
</tr>
</tbody>
</table>

See the *Cisco Unified Serviceability Administration Guide* for information about SNMP.
Chapter 34

Additional Requirements

• XMPP Standards Compliance, on page 345
• Configuration Changes and Service Restart Notifications, on page 346

XMPP Standards Compliance

The IM and Presence Service is compliant with the following XMPP standards:

• RFC 3920 Extensible Messaging and Presence Protocol (XMPP): Core
    • 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
Configuration Changes and Service Restart Notifications

Whenever you need to restart a service, an Active Notifications popup appears. There is an Active Notifications Summary in the top right of the Cisco Unified CM IM and Presence Administration GUI header.

In addition, you can access an Active Notifications Listing by choosing System > Notifications From the Cisco Unified CM IM and Presence Administration interface.

Configuration Changes that Require a Restart

For many IM and Presence configuration changes and updates, you must restart the Cisco XCP Router, Cisco SIP Proxy or Cisco Presence Engine.

The following table displays the configuration changes that require a restart of any of these services. This list includes configuration changes, but does not include platform changes such as installs or upgrades.

<table>
<thead>
<tr>
<th>Configurations that Require a Restart</th>
<th>Restart this Service</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application Listener Configuration</strong></td>
<td>Cisco SIP Proxy</td>
</tr>
<tr>
<td>(System &gt; Application Listeners)</td>
<td></td>
</tr>
<tr>
<td>Editing Application Listeners</td>
<td></td>
</tr>
<tr>
<td><strong>Compliance Profile Configuration</strong></td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>(Messaging &gt; Compliance &gt; Compliance Settings)</td>
<td></td>
</tr>
<tr>
<td>(Messaging &gt; Compliance &gt; Compliance Profiles)</td>
<td></td>
</tr>
<tr>
<td>If you edit settings for events that are assigned to a 3rd party compliance server</td>
<td></td>
</tr>
<tr>
<td><strong>Group Chat System Administrators</strong></td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>(Messaging &gt;Group Chat System Administrators)</td>
<td></td>
</tr>
<tr>
<td>If you enable or disable this setting</td>
<td></td>
</tr>
<tr>
<td>Configurations that Require a Restart</td>
<td>Restart this Service</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td><strong>External File Server Configuration</strong> (Messaging &gt; External Server Setup &gt; External File Servers)</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>If you edit the <strong>Host/IP Address Setting</strong></td>
<td></td>
</tr>
<tr>
<td>If you regenerate the <strong>External File Server Public Key</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Group Chat and Persistent Chat Configuration</strong> (Messaging &gt; Group Chat and Persistent Chat)</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>If a chat node cannot reach its external DB at startup, the Cisco XCP Text Conference Mgr Service is not running</td>
<td></td>
</tr>
<tr>
<td><strong>Group Chat Server Alias Mapping</strong> (Messaging &gt; Group Chat Server Alias Mapping)</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>Adding a chat alias</td>
<td></td>
</tr>
<tr>
<td><strong>ACL Configuration</strong> (System &gt; Security &gt; Incoming ACL)</td>
<td>Cisco SIP Proxy</td>
</tr>
<tr>
<td>(System &gt; Security &gt; Outgoing ACL)</td>
<td></td>
</tr>
<tr>
<td>Edit Incoming or Outgoing ACL Configuration</td>
<td></td>
</tr>
<tr>
<td><strong>Compliance Settings</strong> Message Archiver - edit the settings</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td><strong>LDAP Server</strong> (Application &gt; Third-Party Clients &gt; Third-party LDAP Settings)</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>LDAP Search - editing LDAP Search</td>
<td></td>
</tr>
<tr>
<td>Editing the Build vCards from LDAP</td>
<td></td>
</tr>
<tr>
<td>Editing the LDAP attribute to use for vCard FN</td>
<td></td>
</tr>
<tr>
<td><strong>Message Settings Configuration</strong> (Messaging &gt; Settings)</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>Editing the Enable instant message</td>
<td></td>
</tr>
<tr>
<td>Suppress offline instant messaging</td>
<td></td>
</tr>
<tr>
<td><strong>Microsoft RCC Configuration</strong> (Application &gt; Microsoft RCC &gt; Settings)</td>
<td>Cisco SIP Proxy</td>
</tr>
<tr>
<td>Editing any of the settings on this page</td>
<td></td>
</tr>
<tr>
<td>Configurations that Require a Restart</td>
<td>Restart this Service</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td><strong>Presence Gateway</strong></td>
<td></td>
</tr>
<tr>
<td>(Presence &gt; Gateways)</td>
<td></td>
</tr>
<tr>
<td>Add, edit, delete a presence gateway</td>
<td></td>
</tr>
<tr>
<td>After you upload MS Exchange certificates</td>
<td></td>
</tr>
<tr>
<td><strong>Presence Settings Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>(Presence &gt; Settings &gt; Standard Configuration)</td>
<td></td>
</tr>
<tr>
<td>Editing the Enable Availability Sharing setting</td>
<td></td>
</tr>
<tr>
<td>Allow users to view the availability of other users without being prompted for approval</td>
<td></td>
</tr>
<tr>
<td>Maximum Contact List Size (per user)</td>
<td></td>
</tr>
<tr>
<td>Maximum Watchers</td>
<td></td>
</tr>
<tr>
<td><strong>Presence Settings Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>(Presence &gt; Settings &gt; Standard Configuration)</td>
<td></td>
</tr>
<tr>
<td>Editing the <strong>Enable user of Email address for Interdomain Federation</strong> field</td>
<td></td>
</tr>
<tr>
<td><strong>Partitioned Intradomain Federation Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Presence &gt; Settings &gt; Standard Configuration (check box)</td>
<td></td>
</tr>
<tr>
<td>Presence &gt; Intradomain Federation Setup (wizard)</td>
<td></td>
</tr>
<tr>
<td>Enable Partitioned Intradomain Federation with LCS/OCS/Lync via the check box or via the wizard</td>
<td></td>
</tr>
<tr>
<td>Partitioned intradomain Routing Mode - configured via the Standard Configuration window or via the wizard</td>
<td></td>
</tr>
<tr>
<td>In addition, you must restart XCP Router</td>
<td></td>
</tr>
<tr>
<td><strong>Proxy Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>(Presence &gt; Routing &gt; Settings)</td>
<td></td>
</tr>
<tr>
<td>Any edit to the Proxy Configuration</td>
<td></td>
</tr>
<tr>
<td><strong>Security Settings</strong></td>
<td></td>
</tr>
<tr>
<td>(System &gt; Security &gt; Settings)</td>
<td></td>
</tr>
<tr>
<td>Editing any SIP security settings such as SIP Intracluster Proxy to Proxy Transport Protocol</td>
<td></td>
</tr>
<tr>
<td>Editing any XMPP security setting</td>
<td></td>
</tr>
<tr>
<td>Cisco XCP Router (for XMPP security edits)</td>
<td></td>
</tr>
<tr>
<td><strong>SIP Federated Domain</strong></td>
<td></td>
</tr>
<tr>
<td>(Presence &gt; Interdomain Federation &gt; SIP Federation)</td>
<td></td>
</tr>
<tr>
<td>Add, edit, delete this configuration</td>
<td></td>
</tr>
</tbody>
</table>
## Configurations that Require a Restart

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Restart this Service</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Third-Party Compliance Service</strong></td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>(Application &gt; Third-Party Clients &gt; Third-Party LDAP Servers)</td>
<td></td>
</tr>
<tr>
<td>Edit the Hostname/IP Address, Port, Password/Confirm Password fields</td>
<td></td>
</tr>
<tr>
<td><strong>TLS Peer Subject Configuration</strong></td>
<td>Cisco SIP Proxy</td>
</tr>
<tr>
<td>(System &gt; Security &gt; TLS Peer Subjects)</td>
<td></td>
</tr>
<tr>
<td>Any edits on this page</td>
<td></td>
</tr>
<tr>
<td><strong>TLS Context</strong></td>
<td>You may need to restart the associated chat server</td>
</tr>
<tr>
<td>(System &gt; Security &gt; TLS Context Configuration)</td>
<td></td>
</tr>
<tr>
<td>Any edits on this page</td>
<td></td>
</tr>
<tr>
<td><strong>XMPP Federation</strong></td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>(Presence &gt; Interdomain Federation &gt; XMPP Federation &gt; Settings)</td>
<td></td>
</tr>
<tr>
<td>(Presence &gt; Interdomain Federation &gt; XMPP Federation &gt; Policy)</td>
<td></td>
</tr>
<tr>
<td>Any edits to XMPP Federation</td>
<td></td>
</tr>
<tr>
<td><strong>Intercluster Peering</strong></td>
<td>You may be asked to restart the Cisco XCP Router (a notification appears in the top right window) in some cases</td>
</tr>
<tr>
<td>(Presence Inter-clustering)</td>
<td></td>
</tr>
<tr>
<td>Editing the intercluster peer configuration</td>
<td></td>
</tr>
<tr>
<td><strong>Ethernet settings</strong></td>
<td>Causes immediate system restart</td>
</tr>
<tr>
<td>(From Cisco Unified IM and Presence OS Administration, Settings &gt; IP &gt; Ethernet/Ethernet IPv6)</td>
<td></td>
</tr>
<tr>
<td>Editing any ethernet settings</td>
<td></td>
</tr>
<tr>
<td><strong>IPv6 Configuration</strong></td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>(System &gt; Enterprise Parameters)</td>
<td></td>
</tr>
<tr>
<td>Editing the Enable IPv6 enterprise parameter</td>
<td></td>
</tr>
<tr>
<td><strong>Troubleshooting</strong></td>
<td>Restart subscriber node</td>
</tr>
<tr>
<td>If an IM+P publisher changes while subscriber is offline</td>
<td></td>
</tr>
<tr>
<td>Edit the Settings &gt; IP &gt; Publisher setting from the subscriber</td>
<td></td>
</tr>
<tr>
<td>Upgrading IM+P and you need to switch to previous version</td>
<td></td>
</tr>
<tr>
<td>Regenerating the cup certificate</td>
<td>Cisco SIP Proxy</td>
</tr>
<tr>
<td>Regenerate cup-xmpp</td>
<td>Cisco Presence Engine</td>
</tr>
<tr>
<td><strong>Compatibility checking</strong></td>
<td></td>
</tr>
<tr>
<td>(Presence &gt; Interdomain Federation &gt; XMPP Federation &gt; Policy)</td>
<td></td>
</tr>
<tr>
<td>Configurations that Require a Restart</td>
<td>Restart this Service</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Regenerate cup-xmpp-s2s certificate</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>Upload new certificate</td>
<td>Restart relevant service for that certificate.</td>
</tr>
<tr>
<td>For Cup-trust certificates, restart the Cisco SIP Proxy</td>
<td></td>
</tr>
<tr>
<td>Remote Audit Log Transfer Protocol</td>
<td>Restart the node</td>
</tr>
<tr>
<td>if you run any of the util remotesyslog set protocol * CLI commands</td>
<td></td>
</tr>
<tr>
<td>If you get any of the following alerts:</td>
<td>It's recommended to restart Cisco Presence Engine</td>
</tr>
<tr>
<td>• PEIDSQueryError</td>
<td></td>
</tr>
<tr>
<td>• PEIDSotIMDBDatabaseSyncError</td>
<td></td>
</tr>
<tr>
<td>• PEIDSSubscribeError</td>
<td></td>
</tr>
<tr>
<td>• PEWebDAVInitializationFailure</td>
<td></td>
</tr>
<tr>
<td>If you get any of the following alerts:</td>
<td>It's recommended to restart Cisco XCP Router</td>
</tr>
<tr>
<td>• XCPConfigMgrJabberRestartRequired</td>
<td></td>
</tr>
<tr>
<td>• XCPConfigMgrR2RPasswordEncryptionFailed</td>
<td></td>
</tr>
<tr>
<td>• XCPConfigMgrR2RRequestTimedOut</td>
<td></td>
</tr>
<tr>
<td>• XCPConfigMgrHostNameResolutionFailed</td>
<td></td>
</tr>
<tr>
<td>PWSSCBInitFailed</td>
<td>It's recommended to restart Cisco SIP Proxy</td>
</tr>
<tr>
<td>Editing any of the Exchange Service Parameters</td>
<td>Cisco Presence Engine</td>
</tr>
<tr>
<td>• Microsoft Exchange Notification Port</td>
<td></td>
</tr>
<tr>
<td>• Calendar Spread</td>
<td></td>
</tr>
<tr>
<td>• Exchange Timeout (seconds)</td>
<td></td>
</tr>
<tr>
<td>• Exchange Queue</td>
<td></td>
</tr>
<tr>
<td>• Exchange Threads</td>
<td></td>
</tr>
<tr>
<td>• EWS Status Frequency</td>
<td></td>
</tr>
<tr>
<td>Upload Exchange Certificates</td>
<td>Cisco SIP Proxy</td>
</tr>
<tr>
<td></td>
<td>Cisco Presence Engine</td>
</tr>
</tbody>
</table>

Reference Information: Configuration Changes and Service Restart Notifications
### Configurations that Require a Restart

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Restart this Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing locales</td>
<td>Restart the IM and Presence Service</td>
</tr>
<tr>
<td>Create new MSSQL external database</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>Editing external database configuration</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>Merging external database</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>Configuring TLS Peer Subjects</td>
<td>Cisco SIP Proxy</td>
</tr>
<tr>
<td>Configuring Peer Authentication TLS Context</td>
<td>Cisco SIP Proxy</td>
</tr>
<tr>
<td>Editing the following Cisco SIP Proxy Service Parameters:</td>
<td>Cisco SIP Proxy</td>
</tr>
<tr>
<td>• CUCM Domain</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>• Server Name (supplemental)</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>• HTTP Port</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>• Stateful Server (transaction Stateful)</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>• Persist TCP Connections</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>• Shared memory size (bytes)</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>• Federation Routing IM/P FQDN</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>• Microsoft Federation User-Agent Headers (comma-delimited)</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>Edit the <strong>Routing Communication Type</strong> service parameter</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>Editing the IM address scheme</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>Assign a default domain</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>Deleting or removing a node from the cluster</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>Any edit to a parameter that affects the Cisco XCP router requires you to restart the Cisco XCP router</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td><strong>Routing Communication Type</strong> service parameters</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>Editing either of the Cisco XCP File Transfer Manager service parameters:</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>• External File Server Available Space Lower Threshold</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>• External File Server Available Space Upper Threshold</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>Edit the <strong>Enable Mulitple Device Messaging</strong> service parameter</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>Editing the <strong>Maximum number of logon sessions per user</strong> service parameter</td>
<td>Cisco XCP Router</td>
</tr>
</tbody>
</table>
**Configuration Changes and Service Restart Notifications**

<table>
<thead>
<tr>
<th>Configurations that Require a Restart</th>
<th>Restart this Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updating the install_dir /data/pg_hba.conf or install_dir /data/postgresql.conf config files on the external database</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>Migration utilities:</td>
<td>Cisco XCP Router</td>
</tr>
<tr>
<td>• Editing the <strong>Allow users to view the availability of other users without being prompted for approval</strong> setting in the Presence Settings window.</td>
<td></td>
</tr>
<tr>
<td>• Editing the <strong>Maximum Contact Lists Size (per user)</strong> and <strong>Maximum Watchers (per user)</strong> setting in the Presence Settings configuration window.</td>
<td></td>
</tr>
<tr>
<td>Deleting or removing a node from a cluster</td>
<td>Cisco XCP Router</td>
</tr>
</tbody>
</table>