Configuration and Administration of the IM and Presence Service on Cisco Unified Communications Manager, Release 12.0(1)

First Published: 2017-08-17

Last Modified: 2020-06-09

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

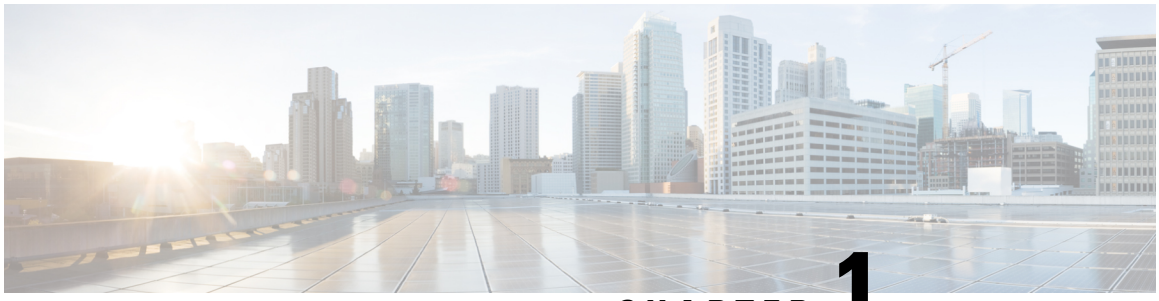
CHAPTER 15 **Managed File Transfer** 191

Revision History

Date	Revision
Mar. 28 2018	Updated the Prerequisites for the IM and Presence Centralized Deployment feature.
April 12, 2018	Updated Managed File Transfer feature with Restricted version requirement to use Managed File Transfer over MRA.

PART I

Deployment Planning



CHAPTER 1

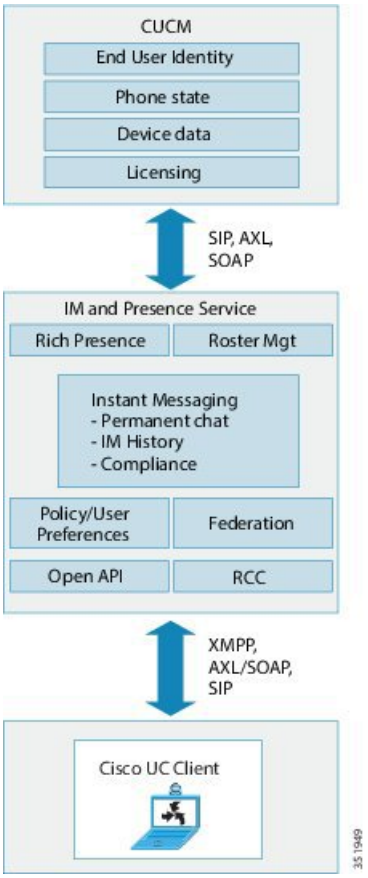
IM and Presence Service Features and Functions

IM and Presence Service Components

Main Components

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

Figure 1: IM and Presence Service Basic Deployment



SIP Interface

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

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

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

Related Topics

SIP Trunk Configuration on Cisco Unified Communications Manager, on page 52
Presence Gateway Configuration Option, on page 108

AXL/SOAP Interface

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

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

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

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

Related Topics

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

LDAP Interface

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

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

Related Topics

LDAP Directory Integration, on page 111
LDAP Server Name, Address, and Profile Configuration, on page 111
Secure Connection Between Cisco Unified Communications Manager and LDAP Directory, on page 112
Configure LDAP Server Names and Addresses for XMPP Clients, on page 117

XMPP Interface

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

Related Topics

Configure Secure Connection Between IM and Presence Service and XMPP Clients, on page 150

CTI interface

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

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

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

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

Cisco IM and Presence Data Monitor

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

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

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

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

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

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

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

- Use this CLI command:

  utils dbreplication runtimestate

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

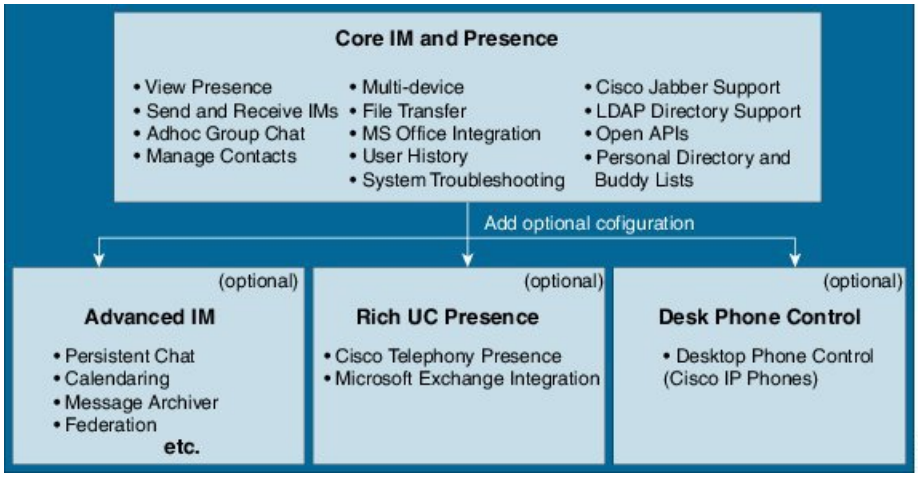
To check the status of the Cisco Sync Agent, navigate to the Cisco Unified CM IM and Presence Administration interface and select **Diagnostics** > **System Dashboard**. You will find the CUCM Publisher IP address as well as the Sync Status.

IM and Presence Service Feature Deployment Options

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

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

Figure 2: IM and Presence Service Feature Deployment Options



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

Table 1: IM and Presence Service Feature Deployment Options

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

Deployment models

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

IM and Presence Service supports single-node, multiple-node.

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

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

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

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

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

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

Presence Redundancy Groups and High Availability

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

- Failover - Occurs in a presence redundancy group when one or more critical services fails on an IM and Presence Service node in the group or a node in the group fails. Clients automatically connect to the other IM and Presence Service node in that group.
- Fallback - Occurs when a fallback command is issued from the Command Line Interface (CLI) or Cisco Unified Communications Manager during either of these conditions:

- The failed IM and Presence Service node comes back into service and all critical services are running. The failed over clients in that group reconnect with the recovered node when it becomes available.
- The backup activated IM and Presence Service node fails due to a critical service failure, and the peer node is in the Failed Over state and supports the automatic recovery fallback.

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

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

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

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

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

Clustering Over WAN

The IM and Presence Service supports Clustering over WAN deployments.

Related Topics

Clustering Over WAN for Intracluster and Intercluster Deployments, on page 27

User Assignment

To allow users to receive availability and Instant Messaging (IM) services on IM and Presence Service, you must assign users to nodes, and presence redundancy groups, in your IM and Presence Service deployment. You can manually or automatically assign users in a IM and Presence deployment. You manage user assignment

using the **User Assignment Mode for Presence Server** Enterprise Parameter setting. This parameter specifies the mode in which the sync agent distributes users to the nodes in the cluster.

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

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

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

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

End User Management

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

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

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

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

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

Availability and Instant Messaging

Chat

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

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

Related Topics

Turn On or Off Instant Messaging for IM and Presence Service Cluster, on page 164
Turn On or Off Availability Sharing for IM and Presence Service Cluster, on page 161

IM Forking

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

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

Related Topics

Turn On or Off Offline Instant Messaging, on page 164

Offline IM

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

Broadcast IM

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

Chat Rooms on IM and Presence Service

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

Ad hoc Chat Rooms

Ad hoc chat rooms are IM sessions that remain in existence only as long as one person is still connected to the chat room, and are deleted from the system when the last user leaves the room. Records of the IM conversation are not maintained permanently.

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

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

Persistent Chat Rooms

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

Rooms Privacy Policy in the Important Notes section of the Release Notes for Cisco Unified Communications Manager and IM and Presence Service, Release 11.0(1).

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

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

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

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

Note For users searching for chat rooms across intercluster connections, search results discover ad hoc chat rooms from clusters older than Release 11.5(1) SU2, but not from clusters for this release or greater. Ad hoc chat rooms on Release 11.5(1) SU2 clusters or greater can only be discovered by the owner or administrator of those chat rooms.

Chat Room Limits

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

Table 2: Chat Room Limits for IM and Presence Service

Number Of...	Maximum
Persistent chat rooms per node	1500 rooms
Total rooms per node (ad hoc and persistent)	16500 rooms
Occupants per room	1000 occupants
Messages retrieved from the archive This is the max number of messages that are returned when a user queries the room history.	100 messages
Messages in chat history displayed by default This is the number of messages that are displayed when a user joins a chat room.	15 messages

File Transfer

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

Related Topics

Enable File Transfer

Important Notes About IM and Presence Service and Chat

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

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

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

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

IM Compliance

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

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

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

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

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

Presence Data Overview

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

- System Determined Presence
- Manual Presence

Manual Presence

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

- A user setting Do Not Disturb on their IM Client
- A user setting Away on their IM Client

- A user setting Available on their IM client to override a system-determined status such as phone/calendar presence.
- A user setting any of the above from a third party application

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

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

System Determined Presence

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

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

There are four categories of System Determined Presence:

- IM Device Status

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

- Calendar Status

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

- Phone Status

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

- Third Party Application Status

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

Enterprise Groups

With Cisco Unified Communications Manager Release 11.0, Cisco Jabber users can search for 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 gets automatically updated. Cisco Unified Communications Manager synchronizes its database with Microsoft Active Directory groups at specified intervals.

When a Cisco Jabber user adds a group to their contact list, IM and Presence Service provides the following information for each group member:

- display name
- user ID
- title
- phone number
- mail ID

Only the group members that are assigned to IM and Presence Service nodes can be added to the contact list. Other group members are discarded.

Note Currently, the enterprise groups feature is supported only on Microsoft Active Directory server. It is not supported on other corporate directories.

The enterprise groups feature is enabled system-wide with the Cisco Unified Communications Manager **Directory Group Operations on Cisco IM and Presence** enterprise parameter. For more information about enterprise groups, see the *Feature Configuration Guide for Cisco Unified Communications Manager*.

Tested OVA information for Enterprise Groups

In a Intercluster deployment with two clusters Cluster A and Cluster B:

Cluster A has 15K OVA and 15K users enabled for IM and Presence Service out of 160K users that are synced from Active Directory. The tested and supported average number of enterprise groups per user on 15K OVA cluster is 13 enterprise groups .

Cluster B has 25K OVA and 25K users enabled for IM and Presence Service out of 160K users that are synced from Active Directory. The tested and supported average number of enterprise groups per user on 25K OVA is 8 enterprise groups.

The tested and supported sum of user's personal contacts in roster and the contacts from enterprise groups that are in a user's roster is less than or equal to 200.

Note In environments with more than 2 clusters these numbers are not supported.

LDAP Integrations

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

- **User provisioning**: You can provision users automatically from the LDAP directory into the Cisco Unified Communications Manager database. Cisco Unified Communications Manager synchronizes with the LDAP directory content so you avoid having to add, remove, or modify user information manually each time a change occurs in the LDAP directory.

- **User authentication**: You can authenticate users using the LDAP directory credentials. IM and Presence Service synchronizes all the user information from Cisco Unified Communications Manager to provide authentication for users of the Cisco Jabber client and IM and Presence Service user interface.

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

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

Related Topics

LDAP Directory Integration with Cisco Unified Communications Manager Task List, on page 111

Third-Party Integrations

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

Guide Title	This Guide Contains ...
Microsoft Exchange for IM and Presence Service on Cisco Unified Communications Manager	• Integrating with Microsoft Exchange 2007, 2010, and 2013 • Configuring Microsoft Active Directory for this integration
Microsoft Office Communicator Call Control with Microsoft OCS for IM and Presence Service on Cisco Unified Communications Manager	• Configuring IM and Presence Service as a CSTA gateway for remote call control from the Microsoft Office Communicator client • Configuring Microsoft Active Directory for this integration • Load-balancing MOC requests in a dual node IM and Presence Service deployment over TCP • Load-balancing MOC requests in a dual node IM and Presence Service deployment over TLS
Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager	• Configuring IM and Presence Service for interdomain federation over the SIP protocol with Microsoft OCS and AOL, and over the XMPP protocol with IBM Sametime, Googletalk, Webex Connect, and another IM and Presence Service Release 9.x enterprise.

Guide Title	This Guide Contains ...
Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager	• Configuring IM and Presence Service for Partitioned Intradomain Federation • Configuring Microsoft OCS for Partitioned Intradomain Federation • Configuring Microsoft LCS for Partitioned Intradomain Federation • User Migration
Remote Call Control with Microsoft Lync Server for IM and Presence Service on Cisco Unified Communications Manager	• Configuring Cisco Unified Communications Manager and IM and Presence Service for integration with Microsoft Lync • Configuring Microsoft Active Directory • Configuring normalization rules • Configuring security between IM and Presence Service and Microsoft Lync

Third-Party Client Integration

Supported Third-Party XMPP Clients

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

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

http://developer.cisco.com/

Note The IM and Presence Service does not support High Availability for third-party web clients. Regardless of whether the High Availability feature is configured, when the primary node fails, the third-party client loses the connection and is unable to reconnect. To ensure that you have redundancy for third-party clients, you must provision the client with a backup node beforehand so that the third-party client can fail over to the backup node if the primary node fails .

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

License Requirements for Third-Party Clients

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

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

XMPP Client Integration on Cisco Unified Communications Manager

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

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

Related Topics

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

LDAP Integration for XMPP Contact Search

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

Related Topics

LDAP Directory Integration for Contact Searches on XMPP Clients, on page 116

DNS Configuration for XMPP Clients

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

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

IPv6 Support

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

Outbound IPv6 traffic is allowed when IPv6 is enabled. For example, SIP S2S can be configured to use either static routes or DNS queries. When a static route is configured and IPv6 is enabled, the SIP proxy attempts to establish an IPv6 connection if IPv6 IP traffic is provided. You can use IPv6 for connections to external databases, LDAP and Exchange servers, and for federation connections on IM and Presence Service even though the connection between IM and Presence Service and Cisco Unified Communications Manager uses IPv4.

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

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

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

- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager Features and Services Guide*
- *Command Line Interface Guide for Cisco Unified Communications Solutions*
- *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager*
- *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*

IM Address Schemes and Default Domain

The IM and Presence Service supports two IM addressing schemes:

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

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

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

Related Topics

Configure IM Address Scheme
IM Address Using UserID@Default_Domain, on page 19

IM Address Using Directory URI, on page 19

IM Address Using UserID@Default_Domain

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

IM Address Using Directory URI

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

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

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

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

- Synchronize the Directory URI from the LDAP directory source.

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

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

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

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

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

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

IM Address Examples

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

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

For more information about configuring IM addresses, see *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

IM Address Integration with Cisco Unified Communications Manager

UserID@Default_Domain Integration with Cisco Unified Communications Manager

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

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

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

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

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

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

Directory URI Integration with Cisco Unified Communications Manager

Unlike the *UserID@Default_Domain* IM address scheme, which is limited to a single IM domain, the Directory URI IM address scheme supports multiple IM domains. Any domain specified in the Directory URI is treated as hosted by IM and Presence Service. The user's IM address is used to align with their Directory URI, as configured on Cisco Unified Communications Manager.

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

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

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

Multiple IM Domain Management

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

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

Security

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

For more information, see topics related to security configuration.

SAML Single Sign-On

The Security Assertion Markup Language (SAML) Single Sign-On feature allows administrative users to access the following Cisco Unified Communications Manager and IM and Presence Service web applications without logging in again:

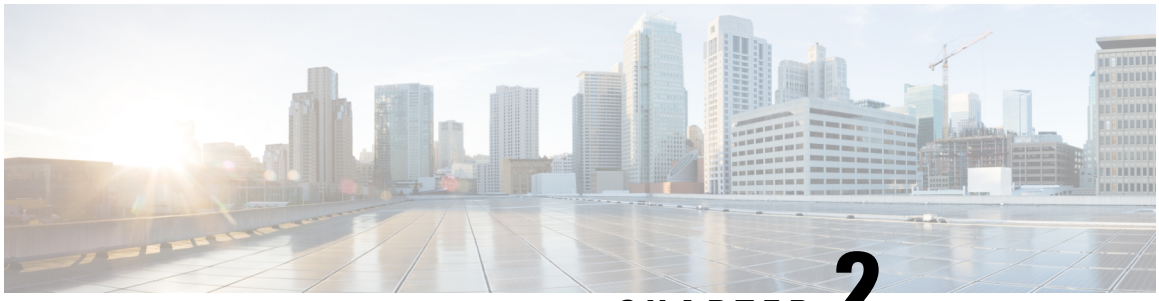
- Cisco Unified CM IM and Presence Administration
- Cisco Unified IM and Presence Serviceability
- Cisco Unified IM and Presence Reporting

- Cisco Unified Communications Manager Administration
- Cisco Unified Reporting
- Cisco Unified Serviceability
- Unified Communications Self Care Portal

Note Only LDAP-synchronized users can access SAML SSO-enabled web applications. Local end users and applications users cannot access them.

For more information about how to enable SAML SSO for Cisco Unified Communications Manager and IM and Presence Service web applications, see the *Administration Guide for Cisco Unified Communications Manager* at this link.

For more information about SAML SSO and how to enable SAML SSO across certain Unified Communications applications, see the *SAML SSO Deployment Guide for Cisco Unified Communications Applications* at this link.



CHAPTER 2

Multinode Scalability and WAN Deployments

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 per cluster 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://docwiki.cisco.com/wiki/Virtualization_for_Unified_CM_IM_and_Presence

OVA Requirements

The following OVA requirements apply:

- For intercluster deployments, you must deploy a minimum OVA of 15,000 users. It is possible to have different clusters running different OVA sizes so long as all clusters are running at least the 15,000 user OVA.
- For Persistent Chat deployments, we recommend that you deploy a minimum OVA of 15,000 users.
- For Centralized Deployments, we recommend the 25,000 user IM and Presence OVA with a minimum OVA of 15,000 users. The 15,000 user OVA can grow to 25,000 users. 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**. For the Unified Communications Manager publisher node in the central cluster, the following requirements apply:
  - A 25,000 IM and Presence OVA (maximum 75,000 users) can be deployed with a 10,000 user OVA installed on the central cluster's Unified Communications Manager publisher node
  - A 15,000 IM and Presence OVA (maximum 45,000 users) can be deployed with a 7,500 user OVA installed on the central cluster's Unified Communications Manager publisher node

Note If you plan to enable Multiple Device Messaging, measure deployments by the number of clients instead of the number of users as each user may have multiple Jabber clients. For example, if you have 25,000 users, and each user has two Jabber clients, your deployment requires the capacity of 50,000 users.

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: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html.

Scalability Options for Deployment

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

Table 3: Multinode Scalability Options

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

Cluster-Wide DNS SRV

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

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

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

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

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

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

Related Topics

Configure Cluster-Wide DNS SRV Name for SIP Publish Trunk, on page 109

Local Failover

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

Presence Redundancy Group Failure Detection

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

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

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

Method Event Routing

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

External Database Recommendations

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

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

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

Clustering Over WAN for Intracluster and Intercluster Deployments

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

Intracluster Deployments Over WAN

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

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

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

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

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

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

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

Multinode Configuration for Deployment Over WAN

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

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

Related Topics

Intracluster Deployments Over WAN, on page 27
http://www.cisco.com/go/designzone

Intercluster Deployments

Intercluster Deployments Over WAN

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

Related Topics

WAN Bandwidth Requirements, on page 33

Intercluster Peer Relationships

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

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

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

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

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

Intercluster Router to Router Connections

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

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

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

Related Topics

Secure Intercluster Router to Router Connection, on page 30

Node Name Value for Intercluster Deployments

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

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

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

Related Topics

IM and Presence Default Domain Value for Intercluster Deployments, on page 30

IM and Presence Default Domain Value for Intercluster Deployments

If you configure an intercluster deployment, note the following:

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

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

Related Topics

IM and Presence Service Default Domain Configuration

Node Name Value for Intercluster Deployments, on page 29

IM Address Scheme for Intercluster Deployments

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

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

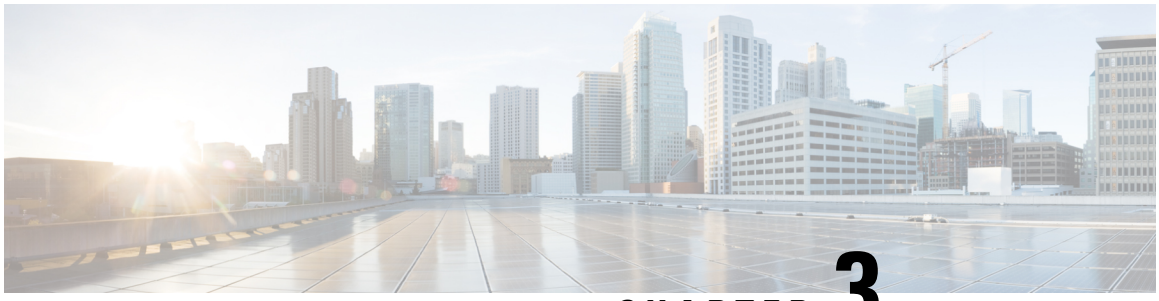
Secure Intercluster Router to Router Connection

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

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

Related Topics

Intercluster Router to Router Connections, on page 29



CHAPTER 3

IM and Presence Service Planning Requirements

Multinode Hardware Recommendations

When configuring the multinode feature, consider the following:

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

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

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

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

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

Intercluster Hardware Recommendations

For Intercluster deployments, we recommend that you deploy a minimum OVA size of 15,000 users. It is possible to have different clusters running different OVA sizes, so long as all clusters are running at least the 15k OVA.

Note If you plan to enable Multiple Device Messaging, measure deployments by the number of clients instead of by the number of users as each user may have multiple Jabber clients. For example, if you have 15,000 users, and each user has two Jabber clients, your deployment must have the capacity of 30,000 users.

Supported End Points

The multinode scalability feature supports the following end points:

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

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

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

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

LDAP Directory Servers Supported

IM and Presence Service integrates with these LDAP directory servers:

- Microsoft Active Directory 2000, 2003, 2008, 2012, 2016
- Netscape Directory Server
- Sun ONE Directory Server 5.2
- OpenLDAP

Related Topics

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

WAN Bandwidth Requirements

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

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

WAN Bandwidth Considerations

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

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

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

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

Multinode Scalability and Performance

Multinode Scalability Requirements

IM and Presence Service supports multinode scalability:

- Six nodes per cluster
- 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 per cluster 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://docwiki.cisco.com/wiki/Virtualization_for_Unified_CM_IM_and_Presence

Multinode Performance Recommendations

You can achieve optimum performance with the multinode feature when:

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

Related Topics

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

User License Requirements

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

You can assign IM and Availability on a per user basis, regardless of the number of clients you associate with each user. When you assign IM and Availability to a user, this enables the user to send and receive IMs and

also to send and receive availability updates. If the user is not enabled for IM and Availability, no availability updates are allowed for that user.

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

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

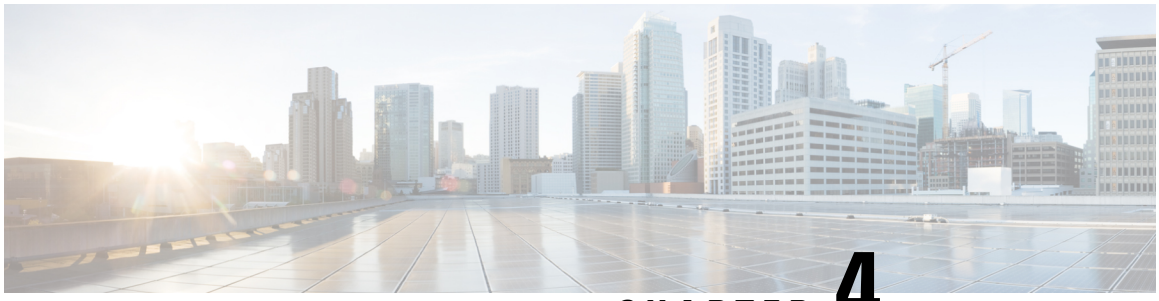
DNS Domain and Default Domain Requirements

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

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

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

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



CHAPTER 4

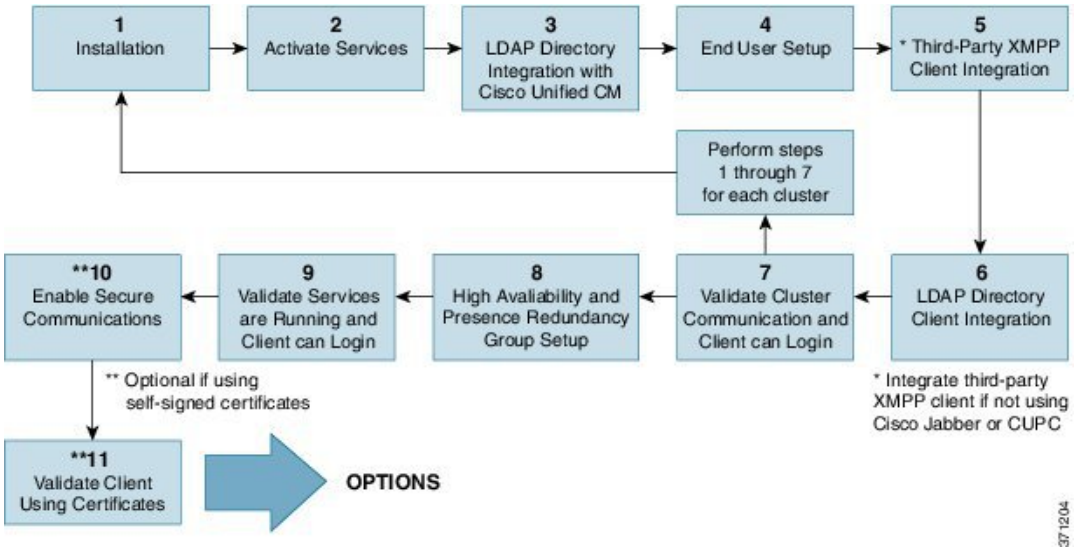
Workflows

Basic Deployment with High Availability Workflow

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

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

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



The following table describes each task in the workflow.

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

Table 4: Task List for Basic Workflow with High Availability

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

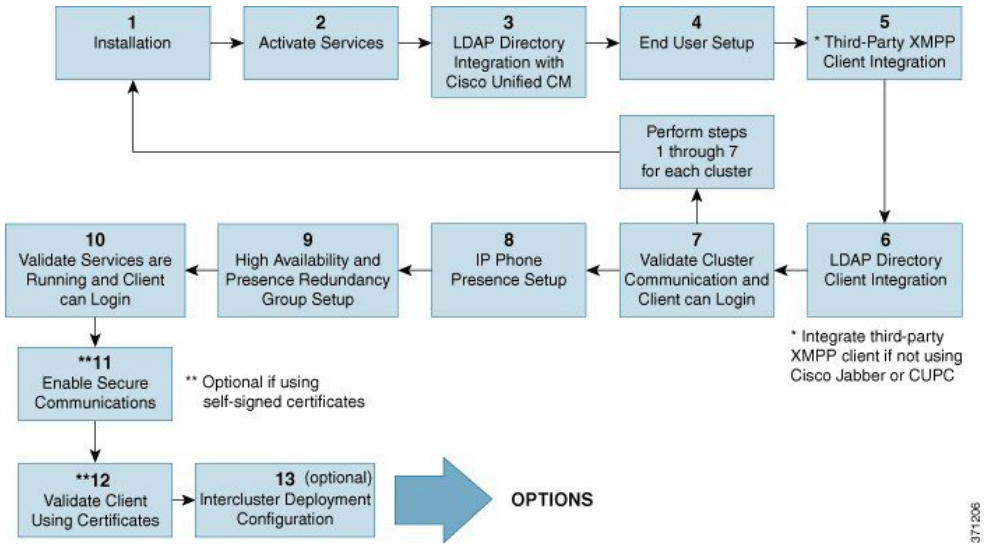
	Task	Description
7	Validate Cluster Communications and Client can Login	Confirm that IM and availability can be exchanged within the cluster. Verify that IM's can be sent and received, and that changes in a user's availability can be seen. When more than one cluster is setup, validate basic IM and availability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

Basic Deployment with High Availability and IP Phone Presence Workflow

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

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

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



The following table describes each task in the workflow.

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

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

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

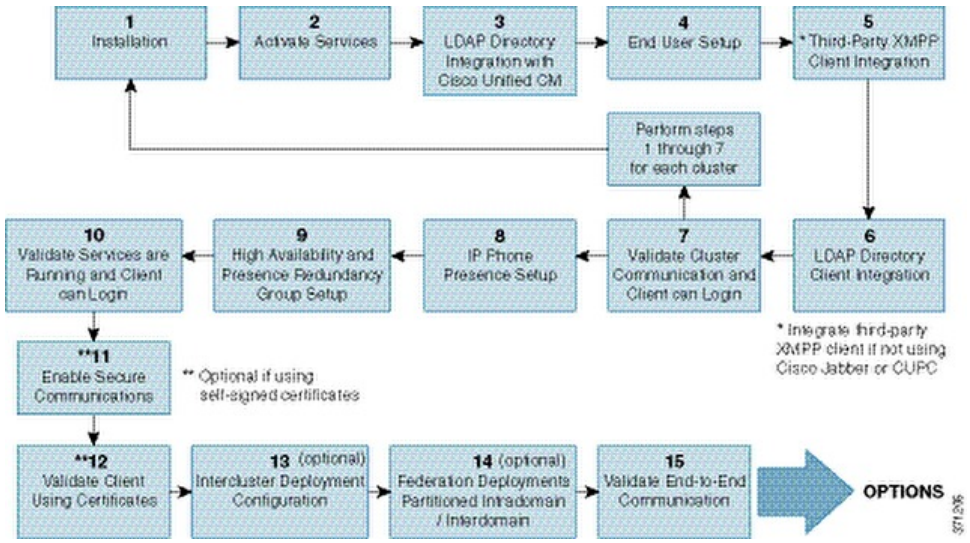
	Task	Description
11	Enable Secure Communications	Perform the following tasks to enable secure communications on the IM and Presence Service node: • Configure certificate exchange between IM and Presence Service and Cisco Unified Communications Manager. • Upload CA signed certificates to IM and Presence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

Federation Deployment Workflow

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

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

Figure 5: IM and Presence Service Workflow for Federation Deployment



The following table describes each task in the workflow.

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

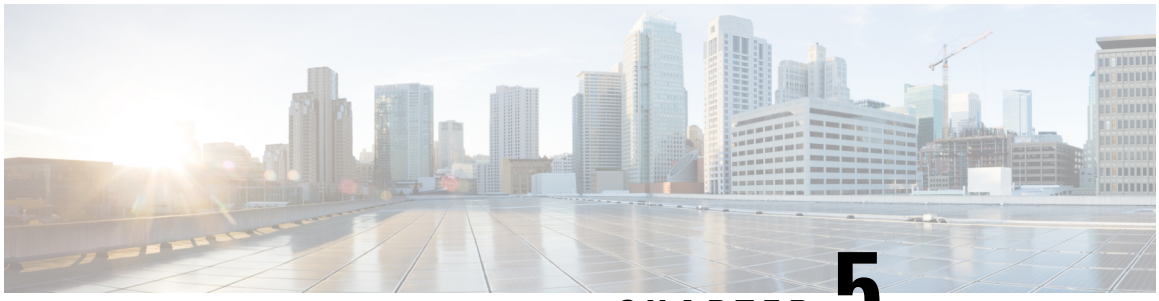
	Task	Description
1	Installation	For detailed Installation instructions, see *Installing Cisco Unified Communications Manager*.
2	Activate Services	You must manually activate feature services after you install the node. For detailed instructions, see *Installing Cisco Unified Communications Manager*.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

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

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

PART II

System Configuration



CHAPTER 5

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

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

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

Table 7: Task List to Configure Users and Devices on Cisco Unified Communications Manager Before Integration with IM and Presence Service

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

Note 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.

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

Related Topics

LDAP Directory Integration, on page 111

Configure Inter-Presence Group Subscription Parameter

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

Restriction

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

Procedure

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

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

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

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

Step 5 Click **Save**.

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

What to do next

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

SIP Trunk Configuration on Cisco Unified Communications Manager

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

Configure SIP Trunk Security Profile for IM and Presence Service

Procedure

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

Step 2 Click **Find.**

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

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

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

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

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

Step 8 Check to enable these items:

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

Step 9 Click **Save**.

What to do next

Proceed to configure the SIP trunk on Cisco Unified Communication Manager

Configure SIP Trunk for IM and Presence Service

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

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

- Dotted IP Address

- Fully Qualified Domain Name (FQDN)
- DNS SRV

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

Before you begin

- Configure the SIP Trunk security profile on Cisco Unified Communications Manager.
- Read the Presence Gateway configuration options topic.

Procedure

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

Step 2 Click **Add New**.

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

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

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

Step 6 Click **Next**.

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

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

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

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

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

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

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

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

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

c) Enter `5060` for the Destination Port.

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

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

Step 10 Click **Save**.

Troubleshooting Tip

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

Related Topics

Configure Cluster-Wide DNS SRV Name for SIP Publish Trunk, on page 109
Configure SIP Trunk Security Profile for IM and Presence Service, on page 52
Configure SIP Publish Trunk on IM and Presence Service, on page 109
Presence Gateway Configuration Option, on page 108

Configure Phone Presence for Unified Communications Manager Outside of Cluster

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

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

Configure TLS Peer Subject

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

Procedure

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

Step 2 Click **Add New**.

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

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

Step 5 Click **Save**.

What to do next

Configure the TLS context.

Configure TLS Context

Use the following procedure to configure TLS context.

Before you begin

Configure the TLS peer subject.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence AdministrationSystemSecurityTLS Context Configuration**.
Step 2 Click **Find**.
Step 3 Click **Default_Cisco_UP_SIP_Proxy_Peer_Auth_TLS_Context**.
Step 4 From the list of available TLS peer subjects, choose the TLS peer subject that you configured.
Step 5 Move this TLS peer subject to Selected TLS Peer Subjects.
Step 6 Click **Save**.
Step 7 Restart the OAMAgent.
Step 8 Restart the Cisco Presence Engine.

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

Verify Required Services Are Running on Cisco Unified Communications Manager

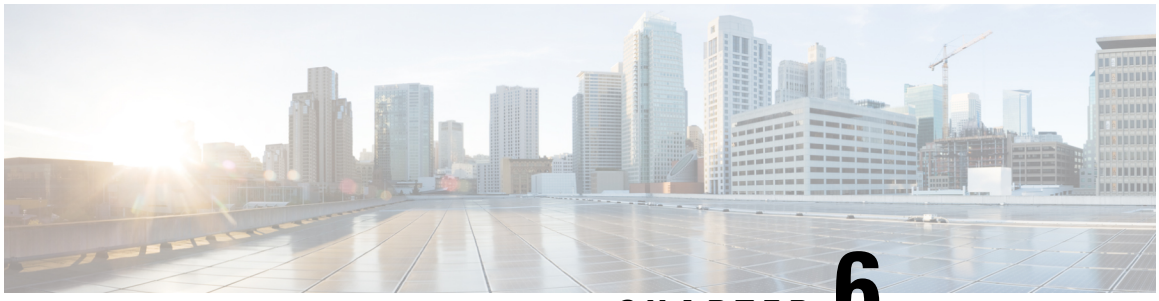
You can view, start, and stop Cisco Unified Communications Manager services from a Cisco Unified Communications Manager node or an IM and Presence Service node. The following procedure provides steps to follow on a Cisco Unified Communications Manager node. To view Cisco Unified Communications Manager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

Procedure

Step 1 On Cisco Unified Communications Manager, choose **Cisco Unified Serviceability** > **Tools** > **Control Center - Feature Services**.
Step 2 Choose a Cisco Unified Communications Manager node from the Server menu.
Step 3 Make sure that the following services are running:

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

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



CHAPTER 6

Configure Centralized Deployment

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–your 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.
- Supports calendar integration with Microsoft Outlook. For configuration details, refer to the document *Microsoft Outlook Calendar Integration for the IM and Presence Service*.

OVA Requirements

For Centralized Deployments, we recommend the 25,000 user IM and Presence OVA with a minimum OVA of 15,000 users. The 15,000 user OVA can grow to 25,000 users. 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**. For the Unified Communications Manager publisher node in the central cluster, the following requirements apply:

- A 25,000 IM and Presence OVA (maximum 75,000 users) can be deployed with a 10,000 user OVA installed on the central cluster's Unified Communications Manager publisher node
- A 15,000 IM and Presence OVA (maximum 45,000 users) can be deployed with a 7,500 user OVA installed on the central cluster's Unified Communications Manager publisher node

Note If you plan to enable Multiple Device Messaging, measure deployments by the number of clients instead of the number of users as each user may have multiple Jabber clients. For example, if you have 25,000 users, and each user has two Jabber clients, your deployment requires the capacity of 50,000 users.

Interclustering for Centralized Deployment

Interclustering is supported between two centralized clusters. Intercluster peering 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 (Decentralized) 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.

Setup Phase	Differences with Standard Deployments
Installation Phase	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.

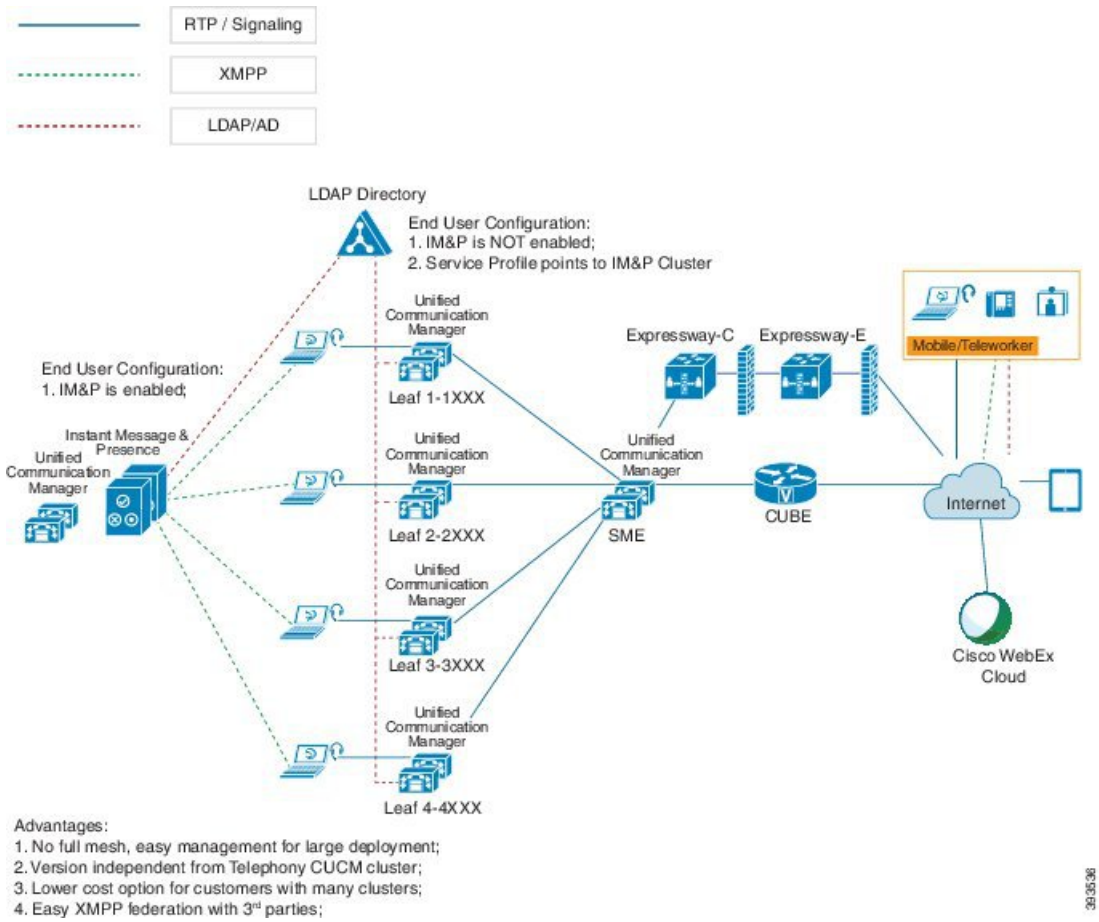
Setup Phase	Differences with Standard Deployments
Configuration Phase	Compared to standard (decentralized) deployments, the following extra configurations are required to set up the IM and Presence Service Central Deployment: • Users must be synced into both the telephony cluster and the IM and Presence Service central cluster so that they exist in both databases. • In your telephony clusters, end users should not be enabled for IM and Presence. • In your telephony clusters, the Service Profile must include the IM and Presence Service and must point to the IM and Presence central cluster. • In the IM and Presence central cluster, users must be enabled for the IM and Presence Service. • In the IM and Presence central cluster's database publisher node, add your remote Cisco Unified Communications Manager telephony cluster peers. The following configurations, which are used with Standard Deployments of the IM and Presence Service, but are not required with Central Deployments: • A Presence Gateway is not required. • A SIP Publish trunk is not required. • 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.

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.

Figure 6: IM and Presence Service Centralized Cluster Architecture

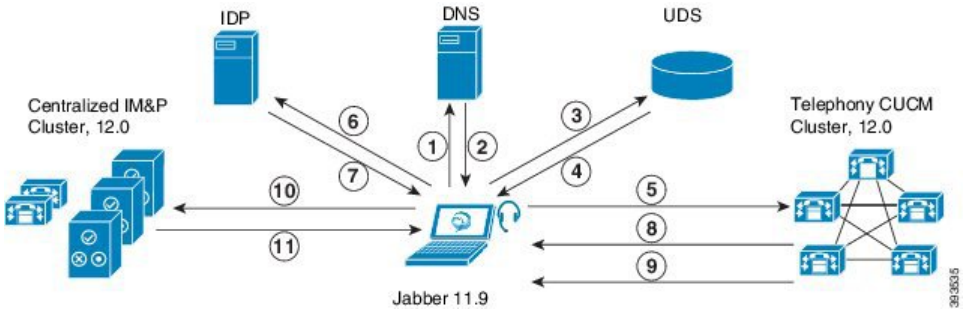


Centralized Cluster Use Case

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.

Figure 7: IM and Presence Service Centralized Cluster Use Case



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.
- You need to enable Cisco Cloud Onboarding on the CUCM Publisher node of the centralised IM and Presence cluster so that all instant messages for iOS devices can also use the Apple Push Notification service (APNs) solution.

  Additionally, you also need to enable Cisco Cloud Onboarding option on the leaf CUCM clusters so that the TCT devices that normally register to those clusters, can have calls routed via the APNs when the Jabber for iOS devices have been suspended or killed by the iOS.

  For more information about how to enable Cisco Cloud Onboarding in the IM and Presence Service cluster, see the *Enable Cisco Cloud Onboarding* chapter in Push Notifications Deployment Guide.
- 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 a new IM and Presence Service deployment to use the centralized deployment option.

Note Use this task flow for new IM and Presence Service deployments only.

Table 8: Centralized Cluster Configuration Task Flow

	IM and Presence Central Cluster	Remote Telephony Clusters	Purpose
Step 1	Enable IM and Presence via Feature Group Template, on page 64		In your IM and Presence central cluster, configure a template that enables the IM and Presence Service.
Step 2	Complete LDAP Sync on IM and Presence Central Cluster, on page 65		Complete an LDAP sync to propagate settings to LDAP-synced users in your IM and Presence central cluster.
Step 3	Enable Users for IM and Presence via Bulk Admin, on page 65		Optional. If you have already completed an LDAP sync, use Bulk Administration to enable IM and Presence for users.
Step 4	Add Remote Telephony Clusters, on page 66		Add your remote telephony clusters to the IM and Presence central cluster.
Step 5		Configure an IM and Presence UC Service, on page 67	In your telephony clusters, add a UC service that points to the IM and Presence central cluster.
Step 6		Create Service Profile for IM and Presence, on page 68	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.
Step 7		Disable Presence Users in Telephony Cluster, on page 68	In the telephony cluster, edit Presence user settings to point to the IM and Presence central cluster.
Step 8		Configure OAuth Refresh Logins , on page 69	Configuring OAuth in the telephony cluster will enable the feature for the central cluster.
Step 9		Configure an ILS Network, on page 70	If more than one telephony cluster exists, you must configure ILS.

What to do Next

- If you want to connect your central cluster to other IM and Presence clusters as part of an intercluster network, configure intercluster peering.

Enable IM and Presence via Feature Group Template

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 65.

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 add the Feature Group Template to an LDAP directory configuration where the initial sync has not yet occurred, and then complete the initial sync.

Complete LDAP Sync on IM and Presence Central Cluster, on page 65

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 services via the feature group template.

Note You cannot apply edits to an LDAP sync configuration after the initial sync has occured. If the initial sync has already occurred, use Bulk Administration instead. For additional detail on how to set up an LDAP Directory sync, see the "Configure End Users" part of the *System Configuration Guide for Cisco Unified Communications Manager*.

Before you begin

Enable IM and Presence via Feature Group Template, on page 64

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 **System** > **LDAP** > **LDAP Directory**.

Step 3 Do either of the following:

a) Click **Find** and select an existing LDAP Directory sync.
b) Click **Add New** to create a new LDAP Directory.

Step 4 From the **Feature Group Template** drop-down list box, select the IM and Presence-enabled feature group template that you created in the previous task.

Step 5 Complete the remaining fields in the **LDAP Directory** window. For help with the fields and their settings, refer to the online help.

Step 6 Click **Save**.

Step 7 Click **Perform Full Sync**.

Cisco Unified Communications Manager synchronizes the database with the external LDAP directory. End users are configured with IM and Presence services.

What to do next

Add Remote Telephony Clusters, on page 66

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.

Note 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 the 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.

Note If you have more than one telephony cluster, you must deploy ILS. In this case, the telephony cluster to which the IM and Presence central cluster connects must be a hub 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.

What to do next

Configure an IM and Presence UC Service, on page 67

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. Users in the telephony cluster will get IM and Presence services from the IM and Presence 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.

What to do next

Create Service Profile for IM and Presence, on page 68.

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. Users in the telephony cluster will use this service profile to get IM and Presence services from the central cluster.

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

Disable Presence Users in Telephony Cluster, on page 68

Disable 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.
- **Enable User for Unified CM IM and Presence**—Leave the right check box unchecked. This setting disables the telephony cluster as the provider of IM and Presence.
- **UC Service Profile**—From the drop-down, select the service profile that you configured in the previous task. This setting points users to the IM and Presence central cluster, which will be the provider of the IM and Presence Service.

Note For Expressway MRA configuration, see *Mobile and Remote Access via Cisco Expressway Deployment Guide* at https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html.

Step 5 Complete any remaining fields that you want. For help with the fields and their settings, see the online help.

Step 6 Under **Job Information**, select **Run Immediately**.

Step 7 Click **Submit**.

What to do next

Configure OAuth Refresh Logins , on page 69

Configure OAuth Refresh Logins

Enable OAuth Refresh Logins in the telephony cluster. This will enable the feature in the central clsuter as well.

Procedure

Step 1 Log in to Cisco Unified CM Administration on the telephony cluster.

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

Step 3 Under **SSO And OAuth Configuration,** set the **OAuth with Refresh Login Flow** enterprise parameter to **Enabled**.

Step 4 If you edited the parameter setting, click **Save**.

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.

Note This task flow focuses on ILS requirements around IM and Presence centralized cluster deployments. For additional ILS configuration around telephony, such as configuring Global Dial Plan Replication or URI Dialing, see the "Configure the Dial Plan" section of the *System Configuration Guide for Cisco Unified Communications Manager*.

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.

For information on designing an ILS network, see the *Cisco Collaboration System Solution Reference Network Design* at http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-implementation-design-guides-list.html.

Procedure

	Command or Action	Purpose
Step 1	Configure Cluster IDs for ILS, on page 71	Set unique Cluster IDs for each telephony cluster. ILS will not work while the Cluster ID is set to `StandAloneCluster` (the default setting).
Step 2	Enable ILS on Telephony Clusters, on page 71	Configure and activate ILS on the publisher node of each telephony cluster in the ILS network.
Step 3	Verify ILS Network is Running, on page 72	When ILS is working, you can see all of your remote clusters from the **ILS Configuration** window of your telephony clusters with an "Up to Date" synchronization status.

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

Step 1 Log in to Cisco Unified CM Administration on the publisher node.

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

Step 3 Change the value of the **Cluster ID** parameter from `StandAloneCluster` to a unique value that you set. ILS will not work while the Cluster ID is `StandAloneCluster`.

Step 4 Click **Save**.

Step 5 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.

What to do next

Enable ILS on Telephony Clusters, on page 71

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 71

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 72

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.
2. **Security** : Secure business-to-business communications.
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 9: OAuth Enable Configuration

Authentication path	UCM / LADP basic authentication
Authorize by OAuth token with refresh	ON
Authorize by OAuth token	ON
Authorize by user credentia	No
Allow Jabber iOS clients to use embedded Safari browser	No
Check for internal authentication availability	Yes

Table 10: OAuth Disable Configuration

Authentication path	UCM / LADP basic authentication
Authorize by OAuth token with refresh	Off
Authorize by user credentia	On
Allow Jabber iOS clients to use embedded Safari browser	Off
Check for internal authentication availability	Yes

Note **For Information on Basic MRA Configuration , Please refer :** https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

IM and Presence Centralized Cluster Setup with SSO Enabled Remote Telephony Clusters for Subdomains

In the IM and Presence centralized deployment, if your remote telephony clusters are having multiple sub-domains, you can enable SOAP login to the remote access client (for example, Jabber) with SSO enabled.

This section covers the steps to configure a subdomain user login to Jabber in the SSO enabled remote telephony clusters. Consider a centralized deployment scenario, which consists of a centralized cluster and an SSO enabled remote telephony cluster associated with that centralized cluster.

To set up SSO enabled login for subdomains, complete the following steps:

Procedure

Step 1 Log in to the Cisco Unified CM Administration and do the following:

a) Synchronize users from LDAP to the leaf nodes and set the **Directory URI** field to **Mail ID** and SSO enabled. To know how to synchronize LDAP users, see LDAP Synchronization .

b) Synchronize the same users to the remote telephony node and set the **Directory URI** field to **Mail ID**.

c) In the **End User Configuration** page (**End Users** > **End User Management**), check the **Enable Users for Cisco Unified IM and Presence Service (Configure IM and Presence in the associated UC Service Profile)** option under **Service Settings** for the IM and Presence nodes to have the same users as in the centralized cluster.

d) In the **End User Configuration** page (**End Users** > **End User Management**), add users to the Cisco Call Manager (CCM) End Users Group using the **Permission Information** section.

e) Disable users for IM and Presence on the remote telephony cluster. To do this, uncheck the **Enable Users for Cisco Unified IM and Presence Service (Configure IM and Presence in the associated UC Service Profile)** option under **ServiceSettings**

f) Create the UC Service on the central cluster for the remote telephony cluster (**User Management** > **User Settings** > **UC Service Configuration**).

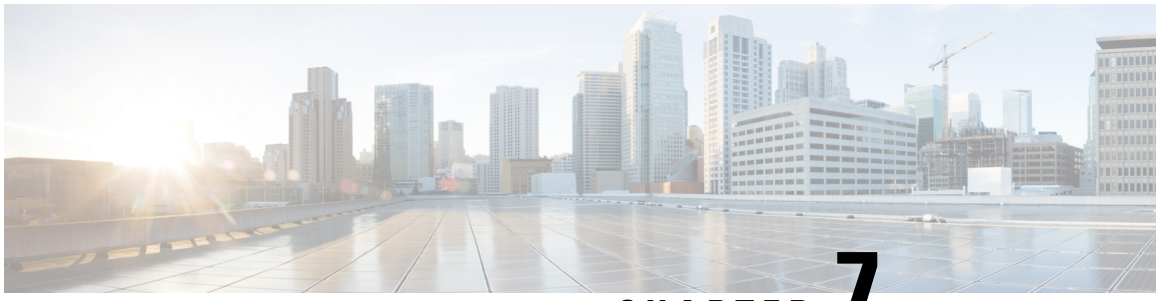
g) Create the service profile on central cluster and set this as the default service profile for the system and add the IM and Presence nodes to the IM and Presence Profile (**User Management** > **User Settings** > **Service Profile**).

h) Enable **OAuth with Refresh Login Flow** on the central cluster. In the **Enterprise Parameter Configuration** page, set the **OAuth with Refresh Login Flow** parameter to **Enabled**.

Step 2 Log in to the Cisco Unified IM and Presence Administration console and add the leaf node to the IM and Presence Service node (**System** > **Centralized Deployment**).

Centralized Deployment Interactions and Restrictions

Feature	Interaction
ILS Hub Cluster	If the ILS hub cluster is down, and more than one telephony cluster exists, the Central Cluster feature does not work.
ILS Deployments	If you are deplying 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.
Rich Presence	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.
Unified Communications Manager Cluster Status	In a centralized deployment, the Unified Communications Manager cluster status appears as**Synchronized for OAuth Refresh Logins**. This feature is available from 11.5(1)SU3 onwards. When you add a Unified Communications Manager cluster to 11.5(1)SU3 or earlier release, the cluster status appears as Unsynchronized under Cisco Unified CM IM and Presence Administration, **System** > **Centralized Deployment** as it does not support OAuth Refresh Logins. Whereas these clusters are compatible for centralized IM and Presence Service deployment using SSO or LDAP directory credentials. **Note** There is no functional impact on Cisco Jabber user login.
Cisco Jabber Status	In a centralized deployment, when you change the Cisco Jabber status to Do Not Disturb (DND), the status change doesn't reflect on the controlled Cisco IP Phone and Jabber device.



CHAPTER 7

IM and Presence Service Network Setup

Configuration changes and service restart notifications

Service Restart Notifications

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

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

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

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.

Cisco XCP Router Restart

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

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

Restart Cisco XCP Router Service

Procedure

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

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

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

Step 4 Click **Restart**.

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

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.

DNS Domain Configuration

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

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

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

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

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

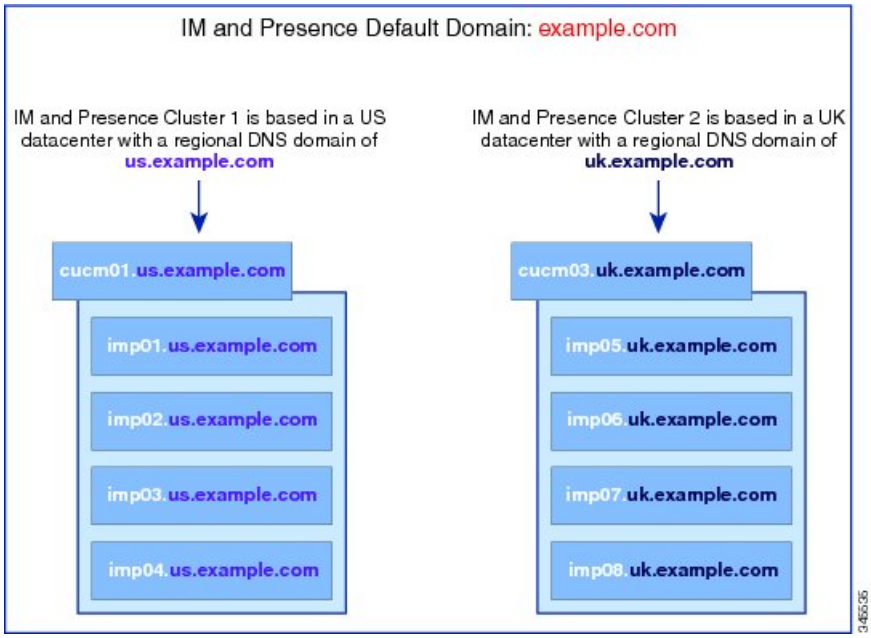
Related Topics

Specify DNS Domain Associated with Cisco Unified Communications Manager Cluster, on page 82
IM and Presence Service Default Domain Configuration
Node Name Recommendations

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

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

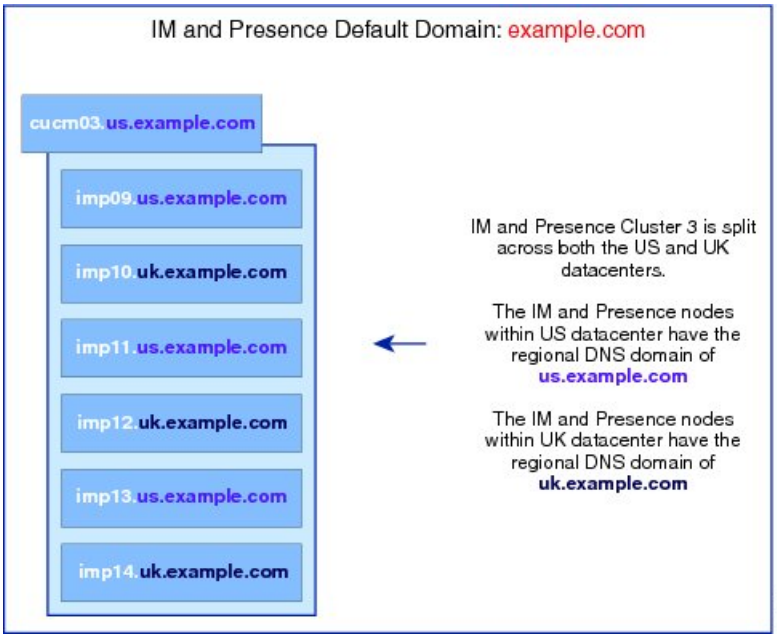
Figure 8: IM and Presence Service Clusters Deployed in Different DNS Domain or Subdomains



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

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

Figure 9: IM and Presence Service Nodes Within a Cluster Deployed in Different DNS Domains or Subdomains

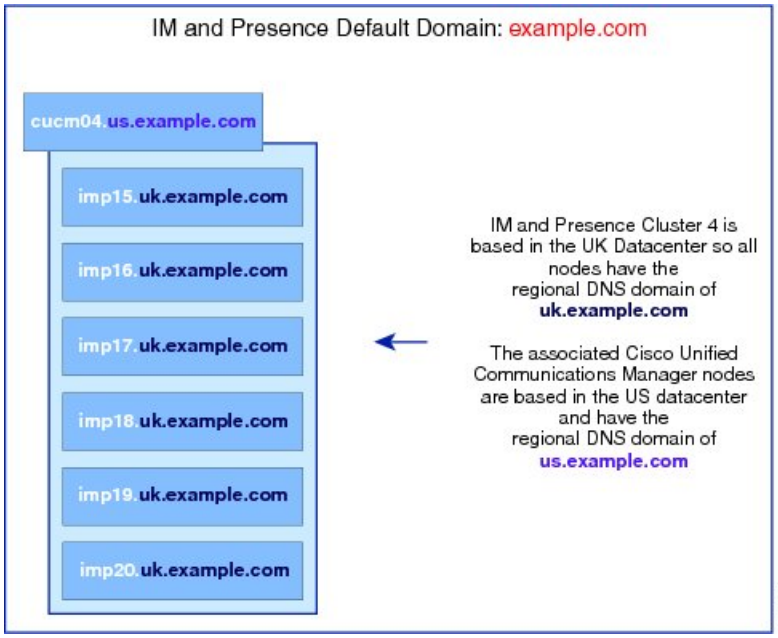


Note High availability is also fully supported in scenarios where the two nodes within a presence redundancy group are in different DNS domains or subdomains.

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

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

Figure 10: IM and Presence Service Nodes Within a Cluster Deployed in a DNS Domain That is Different Than the Associated Cisco Unified Communications Manager Cluster



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

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

Specify DNS Domain Associated with Cisco Unified Communications Manager Cluster

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

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

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

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

Procedure

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

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

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

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

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

Step 5 Click **Save**.

Related Topics

DNS Domain Configuration, on page 79

IM and Presence Service Default Domain Configuration

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

Caution Disable high availability for the presence redundancy group before you stop any services as part of this procedure. If you stop the services while high availability is enabled, a system failover occurs. Before you disable High Availability, take a record of the number of assigned users for each node via the **Presence Topology** window.

After disabling High Availability, wait at least two minutes for the new HA settings to sync across the cluster before you make any further configuration changes.

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

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

Procedure

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

- Cisco Client Profile Agent
- Cisco XCP Router

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

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

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

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

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

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

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

What to do next

If high availability was enabled before the update, confirm that your Cisco Jabber sessions have been recreated before you re-enable High Availability. Otherwise, Presence won't work for Jabber clients whose sessions weren't created.

To obtain the number of Jabber sessions, run the `show perf query counter "Cisco Presence Engine" ActiveJsmSessions` 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. If all of your Jabber sessions aren't recreated after 30 minutes, you have a larger system issue. Once your Jabber sessions are active, re-enable High Availability within your presence redundancy groups.

IM Address Configuration

IM Address Configuration Requirements

The IM and Presence Service default domain and the IM address scheme that you use must be consistent across all IM and Presence Service clusters. The IM address scheme you set affects all user JIDs and cannot

be performed in a phased manner without disrupting communication between clusters which may have different settings.

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

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

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

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

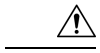
UserID@Default_Domain IM Address Interactions and Restrictions

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

- The UserID@Default_Domain IM address must be unique and cannot match existing IM addresses, directory URIs, or UserIDs. Otherwise, errors will result
- If the UserID is already in UPN format, the IM and Presence Service will escape the first @ (for example, if the userID is `alice@cisco.com`, the IM address would be `alice%20%cisco.com@cisco.com`).
- All IM addresses are part of the IM and Presence default domain, therefore, multiple domains are not supported.
- The IM address scheme must be consistent across all IM and Presence Service clusters.
- The default domain value must be consistent across all clusters.
- If *userid* is mapped to an LDAP field on Cisco Unified Communications Manager, that LDAP mapping must be consistent across all clusters.

Directory URI IM Address Interactions and Restrictions

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



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

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

- The directory URI must be unique and cannot match an existing IM address, directory URI, or UserID. Otherwise, errors will result.
- If any UserIDs are in UPN format (for example, the UserID is `alice@cisco.com`) and directory URI is used for the IM address scheme, the directory URI must be different from the UserID, or errors will result.
- All users have a valid Directory URI value configured on Cisco Unified Communications Manager.
- All deployed clients must support Directory URI as the IM address and use either EDI-based or UDS-based directory integration.

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

- The IM address scheme must be consistent across all IM and Presence Service clusters.
- All clusters must be running a version of Cisco Unified Communications Manager that supports the Directory URI addressing scheme.
- If LDAP Sync is disabled, you can set the Directory URI as a free-form URI. If LDAP Directory Sync is enabled, you can map the Directory URI to the email address (mailid) or the Microsoft OCS/Lync SIP URI (msRTCSIP-PrimaryUserAddress).
- The Directory URI IM address settings are global and apply to all users in the cluster. You cannot set a different Directory URI IM address for individual users in the cluster.
- If you configure directory URI as the IM addressing format, users must have a valid directory URI or the Jabber client will be unable to log in. Please note that the domain portion of the URI cannot start with a number and cannot contain an IP address.

  For example, `joe@5.cisco.com`, `joe@cisco.5com`, and `joe@10.10.10.1` are all invalid directory URIs.

  `joe5@.cisco.com` or `5joe@.cisco.com` are valid directory URIs.

Configure IM Address Task Flow

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

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

Procedure

	Command or Action	Purpose
Step 1	Stop Services, on page 87	You must stop essential IM and Presence services before updating your IM addressing configuration.

	Command or Action	Purpose
Step 2	Assign IM Addressing Scheme, on page 88	Update your IM addressing configuration with new settings such as the default domain and IM addressing scheme.
Step 3	Restart Services, on page 89	Restart essential IM and Presence services. You must restart services before updating user addresses or provisioning users.
Step 4	Update IM user addresses	Update IM user addresses by configuring the corresponding user settings in Cisco Unified Communications Manager. The IM addressing scheme that you configured determines which end user information derives the IM address. • To provision new IM users, see the "Configure End Users" part of the *System Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html. • To edit existing user configurations, see the "Manage End Users" chapter of the *Administration Guide for Cisco Unified Communications Manage*r at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Stop Services

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

Before you begin

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

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

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

Procedure

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

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

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

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

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

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

- Cisco XCP Router

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

What to do next

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

Assign IM Addressing Scheme, on page 88

Assign IM Addressing Scheme

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

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

Before you begin

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

Stop Services, on page 87

Procedure

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

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

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

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

Step 4 Click **Save**.

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

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

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

Note For additional confirmation that there are no duplicate or overlapping directory URIs or userIDs, do the following:

- Run the `utils users validate all` CLI command to check the system for duplicate or overlapping directory URIs and userIDs.
- Verify that the **Cisco IM and Presence Data Monitor** network service is running (the service is running by default). The service runs periodic checks automatically for duplicate and overlapping directory URIs and userIDs. To set the check interval, see Set User Check Interval, on page 269

What to do next

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

Restart Services, on page 89

Restart Services

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

Before you begin

Assign IM Addressing Scheme, on page 88

Procedure

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

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

- **Cisco XCP Router**

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

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

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

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

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

What to do next

If you had High Availability enabled prior to the update, you can re-enable it after all of your Cisco Jabber sessions are recreated. If it has been less than 30 minutes since services restarted, confirm that your Jabber sessions are recreated by running the `show perf query counter "Cisco Presence Engine" ActiveJsmSessions` 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 prior to the upgrade. If it takes more than 30 minutes for your sessions to resume, you have a larger system issue. Once your Jabber sessions are active, re-enable High Availability within your presence redundancy groups.

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

- To provision new IM users, see the "Configure End Users" part of the *System Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.
- To edit existing user configurations, see the "Manage End Users" chapter of the *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.

Domain Management for IM and Presence Service Clusters

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

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

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

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

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

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

IM Domain Management Interactions and Restrictions

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

View IM Address Domains

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

- Domain
- Configured on Local Cluster

- Configured on Peer Cluster(s)

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

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

Procedure

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

Add or Update IM Address Domains

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

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

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

Procedure

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

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

Step 2 Perform one of the following actions:

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

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

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

Delete IM Address Domains

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

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

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

Procedure

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

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

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

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

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

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

Routing Information Configuration on IM and Presence Service

Routing Communication Recommendations

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

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

- If you delete or remove a node, you must restart the Cisco XCP Router on all nodes in your deployment.

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

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

Configure MDNS Routing and Cluster ID

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

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

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

Related Topics

Chat Setup and Management, on page 233

Configure Routing Communication

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

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

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

Before you begin

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

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

Procedure

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

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

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

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

- **Multicast DNS (MDNS)** - Choose Multicast DNS communication if the nodes in your cluster are in the same multicast domain. Multicast DNS communication is enabled by default on IM and Presence Service.
- **Router to Router** - Choose Router-to-Router communication if the nodes in your cluster are not in the same multicast domain.

Step 5 Click **Save**.

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

Related Topics

Restart Cisco XCP Router Service, on page 78

Configure Cluster ID

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

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

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

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

Procedure

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

Step 2 View or edit the Cluster ID value.

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

Step 3 Click **Save**.

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

Related Topics

Chat Setup and Management, on page 233

Configure Throttling Rate for Availability State Change Messages

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

Procedure

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

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

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

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

Step 5 Click **Save**.

IPv6 Configuration

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

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

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

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

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

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

For instructions to configure IPv6 for IM and Presence Service, see *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

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

Related Topics

Important Notes, on page 194

IPv6 Interactions and Restrictions

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

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

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

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

- Connection to an LDAP server.
- Connection to an Exchange server.
- Federation deployments.

Enable IPv6 on Eth0 for IM and Presence Service

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

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

Procedure

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

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

Step 3 Choose the **Address Source**:

- Router Advertisement
- DHCP
- Manual Entry

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

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

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

Step 5 Click **Save**.

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

What to do next

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

Disable IPv6 on Eth0 for IM and Presence Service

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

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

Procedure

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

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

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

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

Step 4 Choose **Save**.

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

Enable IPv6 Enterprise Parameter

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

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

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

Before you begin

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

- Enable IPv6 for ETH0 on each IM and Presence Service node using Cisco Unified CM IM and Presence Administration.

- Set the IPv6 name parameter using Common Topology.

Procedure

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

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

Step 3 Choose **Save**.

What to do next

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

Configure Proxy Server Settings

Procedure

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

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

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

Step 4 Click **Save**.

Services on IM and Presence Service

Turn On Services for IM and Presence Service

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

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

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

Procedure

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

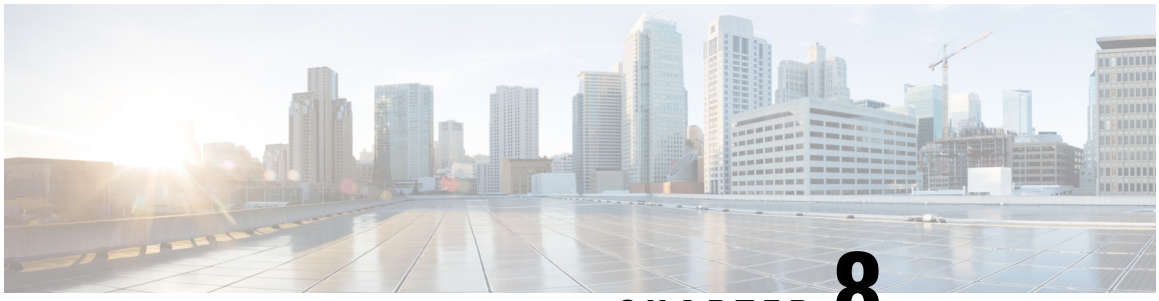
Step 2 Choose the IM and Presence Service node from the Server menu.

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

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

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

Step 4 Click **Save**.



CHAPTER 8

IP Phone Presence Setup

Static Route Configuration on IM and Presence Service

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

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

Route Embed Templates

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

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

Sample Route Embed Template A

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

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

Table 11: Static Routes Set with Embedded Wildcards - Template A

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

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

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

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

Sample Route Embed Template B

Route embed template: **471….xx***

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

Table 12: Static Routes Set with Embedded Wildcards - Template B

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

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

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

Configure Route Embed Templates on IM and Presence Service

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

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

Procedure

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

Step 2 Choose an IM and Presence Service node.

Step 3 Choose the Cisco SIP Proxy service.

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

Step 5 Choose **Save**.

What to do next

Proceed to configure static routes on IM and Presence Service.

Configure Static Routes on IM and Presence Service

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

Table 13: Static Route Parameters Settings for IM and Presence Service

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

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

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

Procedure

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

Step 2 Click **Add New**.

Step 3 Configure the static route settings.

Step 4 Click **Save**.

Presence Gateway Configuration on IM and Presence Service

Presence Gateway Configuration Option

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

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

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

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

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

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

Related Topics

SIP Trunk Configuration on Cisco Unified Communications Manager, on page 52

Configure Presence Gateway

Before you begin

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

Procedure

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

Step 2 Click **Add New**.

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

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

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

Step 6 Click **Save**.

What to do next

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

Related Topics

Configure Authorization Policy on IM and Presence Service, on page 255
Presence Gateway Configuration Option, on page 108

Configure SIP Publish Trunk on IM and Presence Service

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

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

Procedure

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

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

Step 3 Click **Save**.

Configure Cluster-Wide DNS SRV Name for SIP Publish Trunk

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

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

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

Before you begin

Read the cluster-wide DNS SRV topic.

Procedure

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

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

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

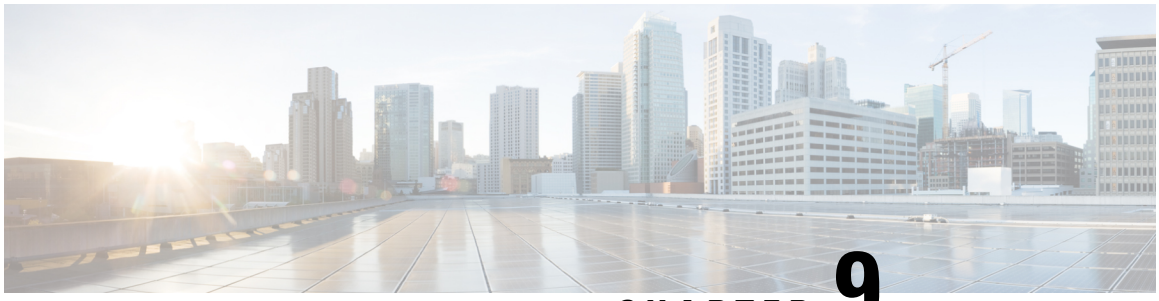
Step 4 Edit the **SRV Cluster Name** field in the General Proxy Parameters (Clusterwide) section.

By default this parameter is empty.

Step 5 Click **Save**.

Related Topics

Cluster-Wide DNS SRV, on page 26
Scalability Options for Deployment, on page 24



CHAPTER 9

LDAP Directory Integration

LDAP Server Name, Address, and Profile Configuration

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

LDAP Directory Integration with Cisco Unified Communications Manager Task List

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

Figure 11: LDAP Directory Integration with Cisco Unified Communications Manager Workflow

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

Table 14: Task List for LDAP Directory Integration

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

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

Secure Connection Between Cisco Unified Communications Manager and LDAP Directory

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

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

- Directory service
- Tomcat service

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

Configure LDAP Synchronization for User Provisioning

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

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

Before you begin

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

Restrictions

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

Procedure

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

Step 2 Click **Add New**.

Step 3 Configure the LDAP server type and attribute.

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

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

Step 6 Configure the following items:

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

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

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

What to do next

Proceed to upload the LDAP authentication server certificates.

Related Topics

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

Upload LDAP Authentication Server Certificates

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

Procedure

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

Step 2 Click **Upload Certificate**.

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

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

Step 5 Click **Upload File**.

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

What to do next

Proceed to configure LDAP authentication.

Configure LDAP Authentication

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

Before you begin

Enable LDAP synchronization on Cisco Unified Communications Manager.

Restrictions

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

Procedure

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

Step 2 Enable LDAP authentication for users.

Step 3 Configure the LDAP authentication settings.

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

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

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

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

What to do next

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

Configure Secure Connection Between IM and Presence Service and LDAP Directory

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

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

Before you begin

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

Procedure

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

Step 2 Click **Upload Certificate**.

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

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

Step 5 Click **Upload File**.

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

What to do next

Proceed to integrate the LDAP directory with Cisco Jabber.

Verify LDAP Directory Connection Using System Troubleshooter

Use the System Troubleshooter in the **Cisco Unified CM IM and Presence Administration** UI to view the status of the system which ensures your connection to the LDAP server is working correctly.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter**.

Step 2 Monitor the status of the connection to the LDAP server in the **LDAP Troubleshooter** area.

The **Problem** column is populated if the system check detects any issues:

- Verify that the LDAP server can be reached.
- Verify that the LDAP server is listening for connections.
- Verify that the LDAP server authentication has been successful.

If any connection problems are detected, perform the recommended solution.

LDAP Directory Integration for Contact Searches on XMPP Clients

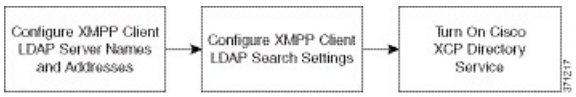
These topics describe how to configure the LDAP settings on IM and Presence Service to allow users of third-party XMPP client to search and add contacts from the LDAP directory.

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

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

Figure 12: LDAP Directory Integration for Contact Searches on XMPP Clients Workflow

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



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

Table 15: Task List for LDAP Directory Integration for Contact Searches on XMPP Clients

Task	Description
Configure XMPP Client LDAP Server Names and Addresses	Upload the root CA certificate to IM and Presence Service as an xmpp-trust-certificate if you enabled SSL and configured a secure connection between the LDAP server and IM and Presence Service. **Tip** The subject CN in the certificate must match the FQDN of the LDAP server.
Configure XMPP Client LDAP Search Settings	You must specify the LDAP search settings that will allow IM and Presence Service to successfully perform contact searches for third-party XMPP clients. You can specify a primary LDAP server and up to two backup LDAP servers. **Tip** Optionally, you can turn on the retrieval of vCards from the LDAP server or allow the vCards to be stored in the local database of IM and Presence Service.
Turn On Cisco XCP Directory Service	You must turn on XCP Directory Service to allow users of a third-party XMPP client to search and add contacts from the LDAP directory. **Tip** Do not turn on the Cisco XCP Directory Service until after you configure the LDAP server and LDAP search settings for third-party XMPP clients; otherwise, the service with stop running.

LDAP Account Lock Issue

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

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

Configure LDAP Server Names and Addresses for XMPP Clients

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

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

You can use IPv6 to connect to the LDAP server even though the connection between IM and Presence Service and Cisco Unified Communications Manager is IPv4. If IPv6 gets disabled for either the enterprise parameter

or for ETH0 on the IM and Presence Service node, the node can still perform an internal DNS query and connect to the external LDAP server if the hostname of the external LDAP server configured for third-party XMPP clients is a resolvable IPv6 address.

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

Before you begin

Obtain the hostnames or IP addresses of the LDAP directories.

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

Procedure

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

Step 2 Click **Add New**.

Step 3 Enter an ID for the LDAP server.

Step 4 Enter the hostname for the LDAP server.

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

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

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

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

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

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

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

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

Step 8 Click **Save**.

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

Tip

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

What to do next

Proceed to configure LDAP search settings for XMPP clients.

Related Topics

Secure Connection Between Cisco Unified Communications Manager and LDAP Directory, on page 112
Configure Secure Connection Between IM and Presence Service and LDAP Directory, on page 115

Configure LDAP Search Settings for XMPP Clients

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

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

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

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

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

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

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

Table 16: LDAP Search Settings for XMPP Clients

Field	Setting
LDAP Server Type	Choose an LDAP server type from this list: • Microsoft Active Directory • Generic Directory Server - Choose this menu item if you are using any other supported LDAP server type (iPlanet, Sun ONE or OpenLDAP).
User Object Class	Enter the User Object Class value appropriate to your LDAP server type. This value must match the User Object Class value configured on your LDAP server. If you use Microsoft Active Directory, the default value is 'user'.
Base Context	Enter the Base Context appropriate to your LDAP server. This value must match a previously configured domain, and/or an organizational structure on your LDAP server.
User Attribute	Enter the User Attribute value appropriate to your LDAP server type. This value must match the User Attribute value configured on your LDAP server. If you use Microsoft Active Directory, the default value is sAMAccountName. If the Directory URI IM address scheme is used and the Directory URI is mapped to either mail or msRTCSIPPrimaryUserAddress, then mail or msRTCSIPPrimaryUserAddress must be specified as the user attribute.
LDAP Server 1	Choose a primary LDAP server.
LDAP Server 2	(Optional) Choose a backup LDAP server.
LDAP Server 3	(Optional) Choose a backup LDAP server.

Before you begin

Specify the LDAP server names and addresses for XMPP clients.

Procedure

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

Step 2 Enter information into the fields.

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

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

Step 5 In the Searchable LDAP Attributes table, map the client user fields to the appropriate LDAP user fields.

If you use Microsoft Active Directory, IM and Presence Service populates the default attribute values in the table.

Step 6 Click **Save**.

Step 7 Start the Cisco XCP Router service (if this service is not already running)

Tip If you make an update to the LDAP search configuration for third-party XMPP clients, restart the Cisco XCP Directory Service. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** to restart this service.

What to do next

Proceed to turn on the Cisco XCP directory service.

Turn On Cisco XCP Directory Service

You must turn on the Cisco XCP Directory Service to allow users of a third-party XMPP client to search and add contacts from the LDAP directory. Turn on the Cisco XCP Directory Service on all nodes in the cluster.

Note Do not turn on the Cisco XCP Directory Service until you configure the LDAP server, and LDAP search settings for third-party XMPP clients. If you turn on the Cisco XCP Directory Service, but you do not configure the LDAP server, and LDAP search settings for third-party XMPP clients, the service will start, and then stop again.

Before you begin

Configure the LDAP server, and LDAP search settings for third-party XMPP clients.

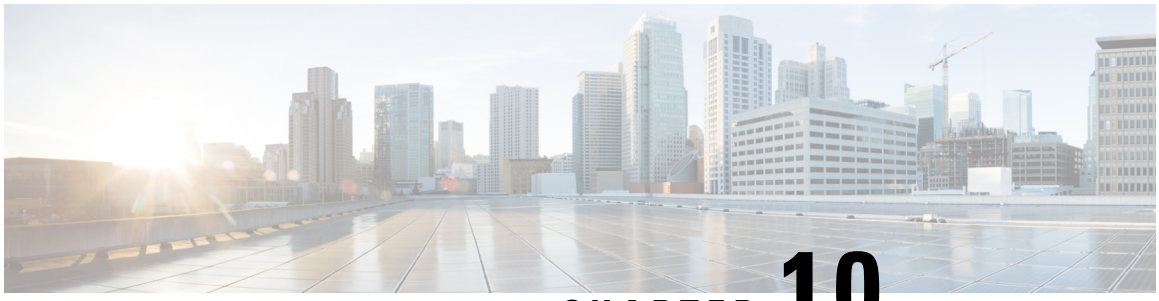
Procedure

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

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

Step 3 Choose **Cisco XCP Directory Service**.

Step 4 Click **Save**.



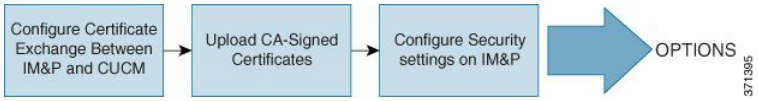
CHAPTER 10

Security Configuration on IM and Presence Service

Security Setup Task List

The following workflow diagram shows the high-level steps to configure security on the IM and Presence Service node deployment.

Figure 13: Security Setup Workflow



The following table lists the tasks to perform to set up security on the IM and Presence Service node deployment. For detailed instructions, see the procedures that are related to the tasks outlined in the workflow.

Note Optionally, you can create a banner that users acknowledge as part of their login to any IM and Presence Service interface.

Table 17: Task List for Security Setup on IM and Presence Service

Task	Description
Configure Certificate Exchange Between IM and Presence Service and Cisco Unified Communications Manager	Perform the following tasks: • Import Cisco Unified Communications Manager certificate to IM and Presence Service node, and then restart the SIP proxy service. **Tip** You can import the certificate using either the Certificate Import Tool or manually using Cisco Unified IM and Presence OS Administration from **Security** > **Certificate Management**. • Download the certificate from IM and Presence Service, and then upload the certificate to Callmanager-trust on Cisco Unified Communications Manager. • Restart the Cisco Unified Communications Manager service. **Note** You must configure a SIP security profile and SIP trunk for IM and Presence Service before you can configure the certificate exchange between Cisco Unified Communications Manager and IM and Presence Service. **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.
Upload CA-Signed Certificates	Upload the Certificate Authority (CA) signed certificates to IM and Presence Service for your deployment, which can be either a single-server or a multi-server deployment. Service restarts are required. See the related tasks for details. • tomcat or tomcat-ECDSA certificate • cup-xmpp or cup-xmpp-ECDSA certificate • cup-xmpp-s2s or cup-xmpp-s2s-ECDSA certificate **Tip** You can upload these certificates on any IM and Presence Service node in the cluster. When this is done, the certificate and the associated signing certificates are automatically distributed to all the other IM and Presence Service nodes in the cluster.
Configure Security Settings on IM and Presence Service	When you import an IM and Presence Service certificate, IM and Presence Service automatically attempts to add the TLS peer subject to the TLS peer subject list, and to the TLS context list. Verify the TLS peer subject and TLS context configuration is set up to your requirements. IM and Presence Service provides increased security for XMPP-based configurations. You can configure the XMPP secure modes on IM and Presence Service using Cisco Unified CM IM and Presence Administration from **System** > **Security** > **Settings**.

Create Login Banner

You can create a banner that users acknowledge as part of their login to any IM and Presence Service interface. You create a .txt file using any text editor, include important notifications they want users to be made aware of, and upload it to the Cisco Unified IM and Presence OS Administration page. This banner will then appear on all IM and Presence Service interfaces notifying users of important information before they login, including legal warnings and obligations. The following interfaces will display this banner before and after a user logs in: Cisco Unified CM IM and Presence Administration, Cisco Unified IM and Presence Operating System Administration, Cisco Unified IM and Presence Serviceability, Cisco Unified IM and Presence Reporting, and IM and Presence Disaster Recovery System.

Procedure

Step 1 Create a .txt file with the contents you want to display in the banner.

Step 2 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 3 Choose **Software Upgrades** > **Customized Logon Message**.

Step 4 Click **Browse** and locate the .txt file.

Step 5 Click **Upload File**.

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

Note The .txt file must be uploaded to each IM and Presence Service node separately.

Enhanced TLS Encryption on IM and Presence Service

This release includes Elliptic Curve Digital Signature Algorithm (ECDSA) support for Tomcat, SIP Proxy, and XMPP interfaces on TLS version 1.2 connections.

We recommended that when you create a certificate, that you configure both an RSA-based certificate and an ECDSA-based certificate. For example, if you configure a tomcat certificate, you should then also configure a tomcat-ECDSA certificate, and vice-versa.

Note If an IM and Presence Service peer does not support TLS version 1.2, then the connection falls back to TLS version 1.0 and the existing behavior is retained.

Note Certificates with a **key length** value of 3072 or 4096 can only be selected for RSA certificates. These options are not available for ECDSA certificates.

Note EC Ciphers on the Tomcat interface are disabled by default. You can enable them using the **HTTPS Ciphers** enterprise parameter on Cisco Unified Communications Manager or on IM and Presence Service. If you change this parameter the Cisco Tomcat service must be restarted on all nodes.

As part of this support four new ciphers have been introduced for use on TLS connections supporting the Tomcat, SIP Proxy, and XMPP interfaces. Two of these new ciphers are RSA-based and two are ECDSA-based.

For further information on ECDSA-based cipher support see, ECDSA Support for Common Criteria for Certified Solutions, in the Release Notes for Cisco Unified Communications Manager and IM and Presence Service, Release 11.0(1).

The new ciphers which are being introduced are:

- ECDHE ECDSA Ciphers
  - **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**
  - **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256**
- ECDHE RSA Ciphers
  - **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384**
  - **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256**

For the RSA-based ciphers, existing security certificates are used. However, the ECDSA-based ciphers require the following additional security certificates:

- `cup-ECDSA`
- `cup-xmpp-ECDSA`
- `cup-xmpp-s2s-ECDSA`
- `tomcat-ECDSA`

If the certificate name ends in `-ECDSA`, then the **certificate/key** type is Elliptic Curve (EC). Otherwise, it is RSA. The Common Name (CN) of an EC certificate has `-EC` appended to the hostname and EC certificates also contain the FQDN or hostname of the server in the SAN field.

Note We recommend that you do not use -EC in the Common Name (CN) field of the RSA-based certificates: Tomcat, XMPP, XMPP-s2s, and CUP. If you do this, the existing EC-based certificate will be overwritten.

For further information on configuring security certificates on IM and Presence Service see, IM and Presence Service Certificate Types, Multi-Server CA Signed Certificate Upload to IM and Presence Service, and Single-Server CA Signed Certificate Upload to IM and Presence Service.

For information on configuring the TLS ciphers see, Configure TLS Cipher Mapping.

RSA Security Certificate Support for Increased Key Lengths

From the current release, new **Key Length** sizes of 3072 bits and 4096 bits have been introduced for self-signed certificates and CSR certificates of certificate/key type RSA.

Multi-Server Certificate Overview

IM and Presence Service supports multi-server SAN based certificates for the certificate purposes of tomcat and tomcat-ECDSA, cup-xmpp and cup-xmpp-ECDSA, and cup-xmpp-s2s and cup-xmpp-s2s-ECDSA. You can select between a single-server or multi-server distribution to generate a Certificate Signing Request (CSR) for the certificate purposes which support multi-server certificates. The resulting signed multi-server certificate and its associated chain of signing certificates are automatically distributed to the other servers in the cluster on upload of the multi-server certificate to any of the individual servers in the cluster. For more information on multi-server certificates, see the New and Changed Features chapter of the *Release Notes for Cisco Unified Communications Manager, Release 10.5(1)*.

IM and Presence Service Certificate Types

This section describes the different certificates required for the clients and services on IM and Presence Service.

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

Table 18: Certificate Types and Services

Certificate Type	Service	Certificate Trust Store	Multi-Server Support	Notes
tomcat tomcat-ECDSA	Cisco Client Profile Agent Cisco AXL Web Service Cisco Tomcat	tomcat- trust	Yes	Presented to a Cisco Jabber client as part of client authentication for IM and Presence Service. Presented to a web browser when navigating the Cisco Unified CM IM and Presence Administration user interface. The associated trust-store is used to verify connections made by IM and Presence Service for the purposes of authenticating user credentials with a configured LDAP server.
ipsec		ipsec-trust	No	Used when an IPSec policy is enabled.
cup cup-ECDSA	Cisco SIP Proxy Cisco Presence Engine	cup-trust	No	

Certificate Type	Service	Certificate Trust Store	Multi-Server Support	Notes
cup-xmpp cup-xmpp-ECDSA	Cisco XCP Connection Manager Cisco XCP Web Connection Manager Cisco XCP Directory service Cisco XCP Router service	cup-xmpp-trust	Yes	Presented to a Cisco Jabber client, Third-Party XMPP client, or a CAXL based application when the XMPP session is being created. 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.
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Cisco XCP XMPP Federation Connection Manager	cup-xmpp-trust	Yes	Presented for XMPP interdomain federation when connecting to externally federated XMPP systems.

Related Topics

XMPP Security Settings Configuration on IM and Presence Service, on page 148
Configure Secure Connection Between IM and Presence Service and LDAP Directory, on page 115

Certificate Exchange Configuration Between IM and Presence Service and Cisco Unified Communications Manager

This module describes the exchange of self-signed certificates between the Cisco Unified Communications Manager node and the IM and Presence Service node. You can use the Certificate Import Tool on IM and Presence Service to automatically import the Cisco Unified Communications Manager certificate to IM and Presence Service. However, you must manually upload the IM and Presence Service certificate to Cisco Unified Communications Manager.

Only perform these procedures if you require a secure connection between IM and Presence Service and Cisco Unified Communications Manager.

Prerequisites for Configuring Security

Configure the following items on Cisco Unified Communications Manager:

- Configure a SIP security profile for IM and Presence Service.
- Configure a SIP trunk for IM and Presence Service:
  - Associate the security profile with the SIP trunk.
  - Configure the SIP trunk with the subject Common Name (CN) of the IM and Presence Service certificate.

Related Topics

SIP Trunk Configuration on Cisco Unified Communications Manager, on page 52

Import Cisco Unified Communications Manager Certificate to IM and Presence Service

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Security** > **Certificate Import Tool**.

Step 2 Choose **IM and Presence (IM/P) Service Trust** from the **Certificate Trust Store** menu.

Step 3 Enter the IP address, hostname or FQDN of the Cisco Unified Communications Manager node.

Step 4 Enter a port number to communicate with the Cisco Unified Communications Manager node.

Step 5 Click **Submit**.

Note After the Certificate Import Tool completes the import operation, it reports whether or not it successfully connected to Cisco Unified Communications Manager, and whether or not it successfully downloaded the certificate from Cisco Unified Communications Manager. If the Certificate Import Tool reports a failure, see the Online Help for a recommended action. You can also manually import the certificate by choosing **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management**.

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

What to do next

Proceed to restart the SIP proxy service.

Restart SIP Proxy Service

Before you begin

Import the Cisco Unified Communications Manager certificate to IM and Presence Service.

Procedure

Step 1 Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** on IM and Presence Service,

Step 2 Choose **Cisco SIP Proxy**.

Step 3 Click **Restart**.

What to do next

Proceed to download the certificate from IM and Presence Service.

Download Certificate from IM and Presence Service

Procedure

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

Step 2 Click **Find**.

Step 3 Choose the **cup.pem** file.

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

Proceed to upload the IM and Presence Service certificate to Cisco Unified Communications Manager.

Upload IM and Presence Service Certificate to Cisco Unified Communications Manager

Before you begin

Download the certificate from IM and Presence Service.

Procedure

Step 1 Choose **Cisco Unified OS Administration** > **Security** > **Certificate Management** on Cisco Unified Communications Manager.

Step 2 Click **Upload Certificate**.

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

Step 4 Browse and choose the certificate (.pem file) previously downloaded from IM and Presence Service.

Note If you want to use an ECDSA certificate, choose the certificate which ends in `-ECDSA.pem`.

Step 5 Click **Upload File**.

What to do next

Proceed to restart the Cisco Unified Communications Manager CallManager service.

Restart Cisco Unified Communications Manager Service

Before you begin

Upload the IM and Presence Service certificate to Cisco Unified Communications Manager.

Procedure

Step 1 Choose **Cisco Unified Serviceability** > **Tools** > **Control Center - Feature Services** on Cisco Unified Communications Manager.

Step 2 Choose **Cisco CallManager**.

Step 3 Click **Restart**.

What to do next

Proceed to configure SIP security settings on IM and Presence Service.

Related Topics

SIP Security Settings Configuration on IM and Presence Service, on page 146

Multi-Server CA Signed Certificate Upload to IM and Presence Service

This section gives further information on uploading the following types of multi-server CA signed certificates:

- tomcat and tomcat-ECDSA certificates
- cup-xmpp and cup-xmpp-ECDSA certificates
- cup-xmpp-s2s and cup-xmpp-s2s-ECDSA certificates

You can upload such certificates on any IM and Presence Service node in the cluster. When this is done the certificate and the associated signing certificates are automatically distributed to all the other IM and Presence Service nodes in the cluster. If a self-signed certificate already exists on any node, for the given certificate purpose (for example, tomcat, cup-xmpp, or cup-xmpp-s2s), it will be overwritten by the new multi-server certificate.

The IM and Presence Service nodes to which a given multi-server certificate and the associated signing certificates are distributed is dependent on the certificate purpose. The cup-xmpp and cup-xmpp-ECDSA, and cup-xmpp-s2s and cup-xmpp-s2s-ECDSA multi-server certificates are distributed to all IM and Presence Service nodes in the cluster. The tomcat multi-server certificate is distributed to all IM and Presence Service nodes in the cluster and to all Cisco Unified Communications Manager nodes in the cluster. For more information on multi-server SAN certificates, see the New and Changed Features chapter of the *Release Notes for Cisco Unified Communications Manager, Release 10.5(1)*.

Single-Server CA Signed Certificate Upload to IM and Presence Service

This section describes how to upload the following types of CA signed certificates to an IM and Presence Service deployment:

- tomcat and tomcat-ECDSA certificates
- cup-xmpp and cup-xmpp-ECDSA certificates
- cup-xmpp-s2s and cup-xmpp-s2s-ECDSA certifiicates

CA-Signed Tomcat Certificate Task List

The high-level steps to upload a CA signed Tomcat or Tomcat-ECDSA certificate to IM and Presence Service are:

1. Upload the Root Certificate and Intermediate Certificate of the signing Certificate Authority to IM and Presence Service.
2. Restart the Cisco Intercluster Sync Agent service.
3. Ensure that the CA certificates have been correctly synced to other clusters.
4. Upload the appropriate signed certificate to each IM and Presence Service node.
5. Restart the Cisco Tomcat service on all nodes.

6. Ensure that intercluster syncing is operating correctly.

Note If you get a Tomcat CSR signed by an EC-based CA or a Tomcat-ECDSA CSR signed by an RSA-based CA, then the TLS connection over the Tomcat interface will fail. We recommend that you use an EC-based CA for signing a tomcat-ECDSA certificate and an RSA-based CA for signing a tomcat certificate.

Upload Root Certificate and Intermediate Certificate of the Signing Certificate Authority

When you upload the Root and Intermediate Certificates, you must upload each certificate in the certificate chain to IM and Presence Service from the Root Certificate down to the last Intermediate Certificate, as follows:

root > intermediate-1 > intermediate-2 > … > intermediate-N

With each certificate that you upload in the chain, you must specify which previously uploaded certificate signed it. For example:

- For intermediate-1, the root cert was used to sign it.
- For intermediate-2, the intermediate-1 cert was used to sign it.

You must upload the Root Certificate and the Intermediate Certificates, if any, to the trust store of the related leaf certificate on the IM and Presence database publisher node. Complete the following procedure to upload the Root Certificate and the Intermediate Certificate of the signing Certificate Authority (CA) to the IM and Presence Service deployment.

Procedure

Step 1 On the IM and Presence database publisher node, choose **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management**.

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

Step 3 From the Certificate Name drop-down list, choose **tomcat-trust**.

Step 4 Enter a description for the signed certificate.

Step 5 Click **Browse** to locate the file for the Root Certificate.

Step 6 Click **Upload File**.

Step 7 Upload each Intermediate Certificate in the same way using the **Upload Certificate/Certificate chain** window.

What to do next

Restart the Cisco Intercluster Sync Agent service.

Restart Cisco Intercluster Sync Agent Service

After you upload the Root and Intermediate certificates to the IM and Presence database publisher node, you must restart the Cisco Intercluster Sync Agent service on that node. This service restart ensures that the CA certificates are synced immediately to all other clusters.

Procedure

Step 1 Log into the Admin CLI.

Step 2 Run the following command: **`utils service restart Cisco Intercluster Sync Agent`**

Note You can also restart the Cisco Intercluster Sync Agent service from the Cisco Unified Serviceability GUI.

What to do next

Verify that the CA certificates have synced to the other clusters.

Verify CA Certificates Have Synchronized to Other Clusters

After the Cisco Intercluster Sync Agent service has restarted, you must ensure that the CA certificate(s) have been correctly synchronized to other clusters. Complete the following procedure on each of the other IM and Presence database publisher nodes.

Note The information in the following procedure also applies to certificates ending in `-ECDSA`.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter**.

Step 2 Under **Inter-clustering Troubleshooter**, find the test **Verify that each TLS-enabled inter-cluster peer has successfully exchanged security certificates** and verify that is has passed.

Step 3 If the test shows an error, note the intercluster peer IP address; it should reference the cluster on which you uploaded the CA certificate(s). Continue with the following steps to resolve the issue.

Step 4 Choose **Presence** > **Inter-Clustering** and click the link associated with the intercluster peer that was identified on the **System Troubleshooter** page.

Step 5 Click **Force Manual Sync**.

Step 6 Allow 60 seconds for the Inter-cluster Peer Status panel to auto-refresh.

Step 7 Verify that the **Certificate Status** field shows "Connection is secure".

Step 8 If the **Certificate Status** field does not show "Connection is secure", restart the Cisco Intercluster Sync Agent service on the IM and Presence database publisher node and then repeat steps 5 to 7.

- To restart the service from the admin CLI run the following command: **`utils service restart Cisco Intercluster Sync Agent`**
- Alternatively, you can restart this service from the Cisco Unified IM and Presence Serviceability GUI.

Step 9 Verify that the **Certificate Status** now shows "Connection is secure". This means that intercluster syncing is correctly established between the clusters and that the CA certificates that you uploaded are synced to the other clusters.

What to do next

Upload the signed certificate to each IM and Presence Service node.

Upload Signed Certificate to Each IM and Presence Service Node

When the CA certificates have correctly synced to all clusters, you can upload the appropriate signed certificate to each IM and Presence Service node.

Note Cisco recommends that you sign all required tomcat certificates for a cluster and upload them at the same time. This process reduces the time to recover intercluster communications.

Note The information in the following procedure also applies to certificates ending in `-ECDSA`.

Procedure

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

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

Step 3 From the Certificate Name drop-down list, choose **tomcat**.

Step 4 Enter a description for the signed certificate.

Step 5 Click **Browse** to locate the file to upload.

Step 6 Click **Upload File**.

Step 7 Repeat for each IM and Presence Service node.

For more information about certificate management, see the *Cisco Unified Communications Operating System Administration Guide*.

What to do next

Restart the Cisco Tomcat service.

Restart Cisco Tomcat Service

After you upload the tomcat certificate to each IM and Presence Service node, you must restart the Cisco Tomcat service on each node.

Procedure

Step 1 Log into the admin CLI.

Step 2 Run the following command: **`utils service restart Cisco Tomcat`**

Step 3 Repeat for each node.

What to do next

Verify that intercluster syncing is operating correctly.

Verify Intercluster Syncing

After the Cisco Tomcat service has restarted for all affected nodes within the cluster, you must verify that intercluster syncing is operating correctly. Complete the following procedure on each IM and Presence database publisher node in the other clusters.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter**.

Step 2 Under **Inter-clustering Troubleshooter**, find the test **Verify that each TLS-enabled inter-cluster peer has successfully exchanged security certificates** test and verify that is has passed.

Step 3 If the test shows an error, note the intercluster peer IP address; it should reference the cluster on which you uploaded the CA certificate(s). Continue with the following steps to resolve the issue

Step 4 Choose **Presence** > **Inter-Clustering** and click the link associated with the intercluster peer that was identified on the **System Troubleshooter** page.

Step 5 Click **Force Manual Sync**.

Step 6 Check the **Also resync peer's Tomcat certificates** checkbox and click **OK**.

Step 7 Allow 60 seconds for the Inter-cluster Peer Status panel to auto-refresh.

Step 8 Verify that the **Certificate Status** field shows "Connection is secure".

Step 9 If the **Certificate Status** field does not show "Connection is secure", restart the Cisco Intercluster Sync Agent service on the IM and Presence database publisher node and then repeat steps 5 to 8.

- To restart the service from the admin CLI run the following command: **`utils service restart Cisco Intercluster Sync Agent`**
- Alternatively, you can restart this service from the Cisco Unified IM and Presence Serviceability GUI.

Step 10 Verify that the **Certificate Status** now shows "Connection is secure". This means that intercluster syncing is now re-established between this cluster and the cluster for which the certificates were uploaded.

CA-Signed cup-xmpp Certificate Upload

The high-level steps to upload a CA signed cup-xmpp or cup-xmpp-ECDSA certificate to IM and Presence Service are:

1. Upload the Root Certificate and Intermediate Certificate of the signing Certificate Authority to IM and Presence Service.
2. Restart the Cisco Intercluster Sync Agent service.
3. Ensure that the CA certificates have been correctly synced to other clusters.
4. Upload the appropriate signed certificate to each IM and Presence Service node.
5. Restart the Cisco XCP Router service on all nodes.

Upload Root Certificate and Intermediate Certificate of the Signing Certificate Authority

When you upload the Root and Intermediate Certificates, you must upload each certificate in the certificate chain to IM and Presence Service from the Root Certificate down to the last Intermediate Certificate, as follows:

root > intermediate-1 > intermediate-2 > … > intermediate-N

With each certificate that you upload in the chain, you must specify which previously uploaded certificate signed it. For example:

- For intermediate-1, the root cert was used to sign it.
- For intermediate-2, the intermediate-1 cert was used to sign it.

You must upload the Root Certificate and the Intermediate Certificates, if any, to the **cup-xmpp-trust** store on the IM and Presence database publisher node. Complete the following procedure to upload the Root Certificate and the Intermediate Certificate of the signing Certificate Authority (CA) to the IM and Presence Service deployment.

Procedure

Step 1 On the IM and Presence database publisher node, choose **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management**.

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

Step 3 From the Certificate Name drop-down list, choose **cup-xmpp-trust**.

Step 4 Enter a description for the signed certificate.

Step 5 Click **Browse** to locate the file for the Root Certificate.

Step 6 Click **Upload File**.

Step 7 Upload each Intermediate Certificate in the same way using the **Upload Certificate/Certificate chain** window.

What to do next

Restart the Cisco Intercluster Sync Agent service.

Restart Cisco Intercluster Sync Agent Service

After you upload the Root and Intermediate certificates to the IM and Presence database publisher node, you must restart the Cisco Intercluster Sync Agent service on that node. This service restart ensures that the CA certificates are synced immediately to all other clusters.

Procedure

Step 1 Log into the Admin CLI.

Step 2 Run the following command: **`utils service restart Cisco Intercluster Sync Agent`**

Note You can also restart the Cisco Intercluster Sync Agent service from the Cisco Unified Serviceability GUI.

What to do next

Verify that the CA certificates have synced to the other clusters.

Verify CA Certificates Have Synchronized to Other Clusters

After the Cisco Intercluster Sync Agent service has restarted, you must ensure that the CA certificate(s) have been correctly synchronized to other clusters. Complete the following procedure on each of the other IM and Presence database publisher nodes.

Note The information in the following procedure also applies to certificates ending in `-ECDSA`.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter**.

Step 2 Under **Inter-clustering Troubleshooter**, find the test **Verify that each TLS-enabled inter-cluster peer has successfully exchanged security certificates** and verify that is has passed.

Step 3 If the test shows an error, note the intercluster peer IP address; it should reference the cluster on which you uploaded the CA certificate(s). Continue with the following steps to resolve the issue.

Step 4 Choose **Presence** > **Inter-Clustering** and click the link associated with the intercluster peer that was identified on the **System Troubleshooter** page.

Step 5 Click **Force Manual Sync**.

Step 6 Allow 60 seconds for the Inter-cluster Peer Status panel to auto-refresh.

Step 7 Verify that the **Certificate Status** field shows "Connection is secure".

Step 8 If the **Certificate Status** field does not show "Connection is secure", restart the Cisco Intercluster Sync Agent service on the IM and Presence database publisher node and then repeat steps 5 to 7.

- To restart the service from the admin CLI run the following command: **`utils service restart Cisco Intercluster Sync Agent`**
- Alternatively, you can restart this service from the Cisco Unified IM and Presence Serviceability GUI.

Step 9 Verify that the **Certificate Status** now shows "Connection is secure". This means that intercluster syncing is correctly established between the clusters and that the CA certificates that you uploaded are synced to the other clusters.

What to do next

Upload the signed certificate to each IM and Presence Service node.

Upload Signed Certificate to Each IM and Presence Service Node

When the CA certificates have correctly synced to all clusters, you can upload the appropriate signed cup-xmpp certificate to each IM and Presence Service node.

Note Cisco recommends that you sign all required cup-xmpp certificates for a cluster and upload them at the same time so that service impacts can be managed within a single maintenance window.

Note The information in the following procedure also applies to certificates ending in `-ECDSA`.

Procedure

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

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

Step 3 From the Certificate Name drop-down list, choose **cup-xmpp**.

Step 4 Enter a description for the signed certificate.

Step 5 Click **Browse** to locate the file to upload.

Step 6 Click **Upload File**.

Step 7 Repeat for each IM and Presence Service node.

For more information about certificate management, see the *Cisco Unified Communications Operating System Administration Guide* .

What to do next

Restart the Cisco XCP Router service on all nodes.

Restart Cisco XCP Router Service On All Nodes

Caution A restart of the Cisco XCP Router affects service.

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

Procedure

Step 1 Log into the admin CLI.

Step 2 Run the following command: **`utils service restart Cisco XCP Router`**

Step 3 Repeat for each node.

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

CA-Signed cup-xmpp-s2s Certificate Upload

The high-level steps to upload a CA signed cup-xmpp-s2s or cup-xmpp-s2s-ECDSA certificate to IM and Presence Service are:

1. Upload the Root Certificate and Intermediate Certificate of the signing Certificate Authority to IM and Presence Service.
2. Ensure that the CA certificates have been correctly synced to other clusters.
3. Upload the appropriate signed certificate to IM and Presence Service federation nodes (this certificate is not required on all IM and Presence Service nodes, only those used for federation).
4. Restart the Cisco XCP XMPP Federation Connection Manager service on all affected nodes.

Upload Root Certificate and Intermediate Certificate of Signing Certificate Authority

When you upload the Root and Intermediate Certificates, you must upload each certificate in the certificate chain to IM and Presence Service from the Root Certificate down to the last Intermediate Certificate, as follows:

root > intermediate-1 > intermediate-2 > … > intermediate-N

With each certificate that you upload in the chain, you must specify which previously uploaded certificate signed it. For example:

- For intermediate-1, the root cert was used to sign it.
- For intermediate-2, the intermediate-1 cert was used to sign it.

You must upload the Root Certificate and the Intermediate Certificates, if any, to the **cup-xmpp-trust** store on the IM and Presence database publisher node. Complete the following procedure to upload the Root Certificate and the Intermediate Certificate of the signing Certificate Authority (CA) to the IM and Presence Service deployment.

Procedure

Step 1 On the IM and Presence database publisher node, choose **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management**.

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

Step 3 From the Certificate Name drop-down list, choose **cup-xmpp-trust**.

Step 4 Enter a description for the signed certificate.

Step 5 Click **Browse** to locate the file for the Root Certificate.

Step 6 Click **Upload File**.

Step 7 Upload each Intermediate Certificate in the same way using the **Upload Certificate/Certificate chain** window.

What to do next

Verify that the CA certificates have synced to other clusters.

Verify CA Certificates Have Synchronized to Other Clusters

After the Cisco Intercluster Sync Agent service has restarted, you must ensure that the CA certificate(s) have been correctly synchronized to other clusters. Complete the following procedure on each of the other IM and Presence database publisher nodes.

Note The information in the following procedure also applies to certificates ending in `-ECDSA`.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter**.

Step 2 Under **Inter-clustering Troubleshooter**, find the test **Verify that each TLS-enabled inter-cluster peer has successfully exchanged security certificates** and verify that is has passed.

Step 3 If the test shows an error, note the intercluster peer IP address; it should reference the cluster on which you uploaded the CA certificate(s). Continue with the following steps to resolve the issue.

Step 4 Choose **Presence** > **Inter-Clustering** and click the link associated with the intercluster peer that was identified on the **System Troubleshooter** page.

Step 5 Click **Force Manual Sync**.

Step 6 Allow 60 seconds for the Inter-cluster Peer Status panel to auto-refresh.

Step 7 Verify that the **Certificate Status** field shows "Connection is secure".

Step 8 If the **Certificate Status** field does not show "Connection is secure", restart the Cisco Intercluster Sync Agent service on the IM and Presence database publisher node and then repeat steps 5 to 7.

- To restart the service from the admin CLI run the following command: **`utils service restart Cisco Intercluster Sync Agent`**
- Alternatively, you can restart this service from the Cisco Unified IM and Presence Serviceability GUI.

Step 9 Verify that the **Certificate Status** now shows "Connection is secure". This means that intercluster syncing is correctly established between the clusters and that the CA certificates that you uploaded are synced to the other clusters.

What to do next

Upload the signed certificate to each IM and Presence Service node.

Upload Signed Certificate to Federation Nodes

When the CA certificates have correctly synced to all clusters, you can upload the appropriate signed certificate to each IM and Presence Service federation node. You do not need to upload the certificate to all nodes, only nodes for federation.

Note The information in the following procedure also applies to certificates ending in `-ECDSA`.

Note Cisco recommends that you sign all required cup-xmpp-s2s certificates for a cluster and upload them at the same time.

Procedure

Step 1 Choose **Cisco Unified IM and Presence OS AdministrationSecurityCertificate Management**.

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

Step 3 From the Certificate Name drop-down list, choose **cup-xmpp**.

Step 4 Enter a description for the signed certificate.

Step 5 Click **Browse** to locate the file to upload.

Step 6 Click **Upload File**.

Step 7 Repeat for each IM and Presence Service federation node.

For more information about certificate management, see the *Cisco Unified Communications Operating System Administration Guide*.

What to do next

Restart the Cisco XCP XMPP Federation Connection Manager service on the affected nodes.

Restart Cisco XCP XMPP Federation Connection Manager Service

After you upload the cup-xmpp-s2s 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

Step 1 Log into the admin CLI.

Step 2 Run the following command: **utils service restart Cisco XCP XMPP Federation Connection Manager**

Step 3 Repeat for each federation node.

Delete Self-Signed Trust Certificates

Note The information in the following section also applies to certificates ending in `-ECDSA`.

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

When CA-signed certificates are generated to replace the original self-signed trust certificates on either IM and Presence Service or Cisco Unified Communications Manager the original self-signed trust certificates persist in the service trust store of both nodes. If you want to delete the self-signed trust certificates, you must delete them on both the IM and Presence Service and Cisco Unified Communications Manager nodes.

Delete Self-Signed Trust Certificates from IM and Presence Service

Before you begin

Important You have configured the IM and Presence Service nodes with CA-signed certificates, and waited 30 minutes for the Cisco Intercluster Sync Agent Service to perform its periodic clean-up task on a given IM and Presence Service node.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Operating System Administration** user interface, choose **Security** > **Certificate Management**.

Step 2 Click **Find**.
The **Certificate List** appears.

Note The certificate name is composed of two parts, the service name and the certificate type. For example tomcat-trust where tomcat is the service and trust is the certificate type.

The self-signed trust certificates that you can delete are:

- Tomcat 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 only appears for certificates you have the authority to delete.

What to do next

Repeat the above procedure for each IM and Presence Service node in the cluster and on any intercluster peers to ensure complete removal of unnecessary self-signed trust certificates across the deployment.

If the service is Tomcat, you must check for the IM and Presence Service node's self signed tomcat-trust certificate on the Cisco Unified Communications Manager node. See, Delete Self-Signed Tomcat-Trust Certificates from Cisco Unified Communications Manager, on page 145.

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 Log in to the **Cisco Unified Operating System Administration** user interface, choose **Security** > **Certificate Management**.

The **Certificate List** window appears.

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

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

Step 4 Click the link to an IM and Presence Service node's self-signed tomcat-trust certificate.
A new window appears that shows the tomcat-trust certificate details.

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

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

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

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

SIP Security Settings Configuration on IM and Presence Service

Configure TLS Peer Subject

When you import an IM and Presence Service certificate, IM and Presence Service automatically attempts to add the TLS peer subject to the TLS peer subject list, and to the TLS context list. Verify the TLS peer subject and TLS context configuration is set up to your requirements.

Procedure

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

Step 2 Click **Add New**.

Step 3 Perform one of the following actions for the Peer Subject Name:

a) Enter the subject CN of the certificate that the node presents.
b) Open the certificate, look for the CN and paste it here.

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

Step 5 Click **Save**.

What to do next

Proceed to configure the TLS context.

Configure TLS Context

When you import an IM and Presence Service certificate, IM and Presence Service automatically attempts to add the TLS peer subject to the TLS peer subject list, and to the TLS context list. Verify the TLS peer subject and TLS context configuration is set up to your requirements.

Before you begin

Configure a TLS peer subject on IM and Presence Service.

Procedure

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

Step 2 Click **Find**.

Step 3 Choose **Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context**.

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

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

Step 6 Click **Save**.

Step 7 Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Service Activation**.

Step 8 Restart the Cisco SIP Proxy service.

Troubleshooting Tip

You must restart the SIP proxy service before any changes that you make to the TLS context take effect.

Related Topics

Restart SIP Proxy Service, on page 131

Configure TLS Cipher Mapping

Configure the TLS cipher suite for a TLS context.

From the current release, the following new RSA-based and ECDSA-based ciphers have been added:

- ECDHE ECDSA Ciphers
  - `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`
  - `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`
- ECDHE RSA Ciphers
  - `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
  - `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`

For further TLS encryption information see, Enhanced TLS Encryption on IM and Presence Service.

Procedure

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

Step 2 Click **Find**.

Step 3 Choose a context configuration from the list.

Step 4 To add an available cipher to the suite of selected TLS ciphers, in the **TLS Cipher Mapping** pane select a cipher in the **Available TLS Ciphers** list, and click the right arrow to move it to the **Selected TLS Ciphers** list.

You can unselect a TLS cipher by clicking the left arrow to move the cipher from the **Selected TLS Ciphers** list, back to the **Available TLS Ciphers** list.

Step 5 To order the priority of the ciphers in the **Selected TLS Ciphers** list, use the up and down arrows to the right of that list.

Note Click **Reset To Default** if you want to return to the default configuration for this context.

Step 6 Click **Save**.

XMPP Security Settings Configuration on IM and Presence Service

XMPP Security Modes

IM and Presence Service provides increased security for XMPP-based configuration. The following table describes these XMPP security modes. To configure the XMPP security modes on IM and Presence Service, choose **Cisco Unified CM IM and Presence Administration** > **System** > **Security** > **Settings**.

Table 19: XMPP Secure Mode Descriptions

Secure Mode	Description
Enable XMPP Client To IM/P Service Secure Mode	If you turn on this setting, IM and Presence Service establishes a secure TLS connection between the IM and Presence Service nodes and XMPP client applications in a cluster. IM and Presence Service turns on this secure mode by default. We recommend that you do not turn off this secure mode unless the XMPP client application can protect the client login credentials in nonsecure mode. If you do turn off the secure mode, verify that you can secure the XMPP client-to-node communication in some other way.

Secure Mode	Description
Enable XMPP Router-to-Router Secure Mode	If you turn on this setting, IM and Presence Service establishes a secure TLS connection between XMPP routers in the same cluster, or in different clusters. IM and Presence Service automatically replicates the XMPP certificate within the cluster and across clusters as an XMPP trust certificate. An XMPP router will attempt to establish a TLS connection with any other XMPP router that is in the same cluster or a different cluster, and is available to establish a TLS connection.
Enable Web Client to IM/P Service Secure Mode	If you turn on this setting, IM and Presence Service establishes a secure TLS connection between the IM and Presence Service nodes and XMPP-based API client applications. If you turn on this setting, upload the certificates or signing certificates for the web client in the cup-xmpp-trust repository on IM and Presence Service. **Caution** If your network and IM and Presence Service node support IPv6, and you enable secure TLS connections to XMPP-based API client applications, you must enable the IPv6 enterprise parameter for the node and enable the IPv6 Ethernet IP setting for Eth0 on each IM and Presence Service node using Cisco Unified IM and Presence Operating System Administration; otherwise, the node attempts to use IPv4 for IP traffic. Any packets that are received from an XMPP-based API client application that has an IPv6 address will not be delivered. The node cannot revert to using IPv4 if the node is configured to use an IPv6 connection to an external database, LDAP server, or Exchange server, or if a federation deployment using IPv6 is configured for the node.

If you update the XMPP security settings, restart the services. Perform one of these actions:

- Restart the Cisco XCP Connection Manager if you edit **Enable XMPP Client To IM/P Service Secure Mode**. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** to restart this service.
- Restart the Cisco XCP Router if you edit the **Enable XMPP Router-to-Router Secure Mode**. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Network Services** to restart this service.

- Restart the Cisco XCP Web Connection Manager if you edit **Enable Web Client To IM/P Service Secure Mode**. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** to restart this service.

Related Topics

Configure Secure Connection Between IM and Presence Service and XMPP Clients, on page 150

Configure Secure Connection Between IM and Presence Service and XMPP Clients

Procedure

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

Step 2 Perform one of the following tasks:

- To establish a secure TLS connection between IM and Presence Service and XMPP client applications in a cluster, choose **Enable XMPP Client To IM/P Service Secure Mode**.

  Cisco recommends that you do not turn off this secure mode unless the XMPP client application can protect the client login credentials in a nonsecure mode. If you do turn off the secure mode, verify that you can secure the XMPP client-to-node communication in some other way.

- To establish a secure TLS connection between IM and Presence Service and XMPP-based API client applications in a cluster, choose **Enable Web Client To IM/P Service Secure Mode**.

  If you turn on this setting, upload the certificates or signing certificates for the web client in the cup-xmpp-trust repository on IM and Presence.

  Caution If your network and IM and Presence Service node support IPv6, and you enable secure TLS connections to XMPP-based API client applications, you must enable the IPv6 enterprise parameter for the node and enable the IPv6 Ethernet IP setting for Eth0 on each IM and Presence Service node in the cluster. If the enterprise parameter and Eth0 are not configured for IPv6, the node attempts to use IPv4 for any IPv6 packets that are received from an XMPP-based API client application and those IPv6 packets are not delivered.

  The node cannot revert to using IPv4 if the node is configured to use an IPv6 connection to an external database, LDAP server, or an Exchange server, or if a federation deployment using IPv6 is configured for the node.

Step 3 Click **Save**.

If you update the XMPP security settings, restart the following service using one of the following actions:

- Restart the Cisco XCP Connection Manager if you edit **Enable XMPP Client To IM/P Service Secure Mode**. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** to restart this service.
- Restart the Cisco XCP Web Connection Manager if you edit **Enable Web Client To IM/P Service Secure Mode**. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** to restart this service.

What to do next

Proceed to turn on the services that support XMPP clients on the IM and Presence Service node.

Related Topics

Third-Party Client Integration, on page 16

Turn On IM and Presence Service Services to Support XMPP Clients

Perform this procedure on each node in your IM and Presence Service cluster.

Procedure

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

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

Step 3 Turn on the following services:

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

Step 4 Click **Save**.

Tip For XMPP clients to function correctly, make sure you turn on the Cisco XCP Router on all nodes in your cluster.

Related Topics

Third-Party Client Integration, on page 16

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”.

Tip 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

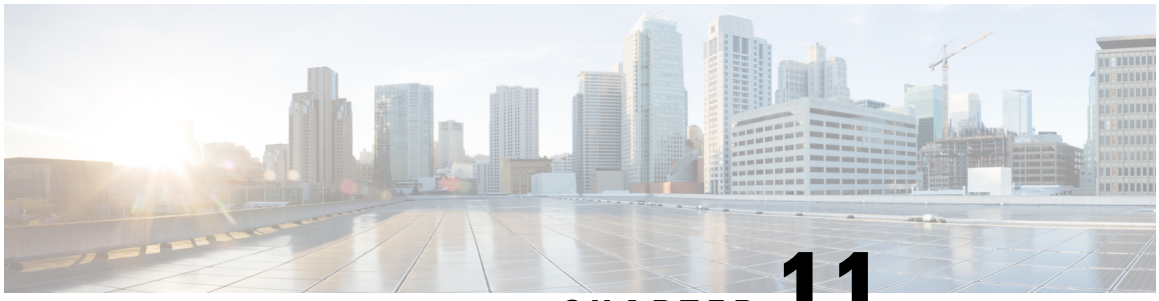
Step 1 Choose **System** > **Security Settings**.

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.



CHAPTER 11

Configure Intercluster Peers

Prerequisites for Intercluster Deployment

You configure an intercluster peer between the IM and Presence database publisher nodes in standalone IM and Presence Service clusters. No configuration is required on the IM and Presence Service subscriber nodes in a cluster for intercluster peer connections. Before you configure IM and Presence Service intercluster peers in your network, note the following:

- The intercluster peers must each integrate with a different Cisco Unified Communications Manager cluster.
- You must complete the required multinode configuration in both the home IM and Presence Service cluster, and in the remote IM and Presence Service cluster:
  - Configure the system topology and assign your users as required.
  - Activate the services on each IM and Presence Service node in the cluster.
- You must turn on the AXL interface on all local IM and Presence nodes, and on all remote IM and Presence nodes. IM and Presence Service creates, by default, an intercluster application user with AXL permissions. To configure an intercluster peer, you will require the username and password for the intercluster application user on the remote IM and Presence Service node.
- You must turn on the Sync Agent on the local IM and Presence database publisher node, and on the remote IM and Presence database publisher node. Allow the Sync Agent to complete the user sychronization from Cisco Unified Communications Manager before you configure the intercluster peers.

For sizing and performance recommendations for intercluster deployments, including information on determining a presence user profile, see the IM and Presence Service SRND.

Intercluster Peer Configuration

Configure Intercluster Peer

Perform this procedure on the database publisher node of the local IM and Presence Service cluster, and on the database publisher node of the remote IM and Presence Service cluster (with which you want your local cluster to form a peer relationship).

Before you begin

- Activate the AXL interface on all local IM and Presence Service nodes and confirm that the AXL interface is activated on all remote IM and Presence Service nodes.
- Confirm that the Sync Agent has completed the user synchronization from Cisco Unified Communications Manager on the local and remote cluster.
- Acquire the AXL username and password for the intercluster application user on the remote IM and Presence Service node.
- If you do not use DNS in your network, see topics related to IM and Presence Service default domain and node name values for intercluster deployments.
- Resolve any invalid or duplicate userIDs before proceeding. For more information, see topics related to end-user management and handling.

Note For the intercluster peer connection to work properly, the following ports must be left open if there is a firewall between the two clusters:

- 8443 (AXL)
- 7400 (XMPP)
- 5060 (SIP) Only if SIP federation is being used

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Inter-Clustering**.

Step 2 Enter the IP address, FQDN, or hostname of the database publisher node of a remote IM and Presence Service cluster.

Step 3 Enter the username of the application user on the remote IM and Presence Service node that has AXL permissions.

Step 4 Enter the associated password of the application user on the remote IM and Presence Service node that has AXL permissions.

Step 5 Enter the preferred protocol for SIP communication.

Note Cisco recommends that you use **TCP** 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.

Step 6 Click **Save**.

Step 7 Check your notifications in the top right of the GUI header. If a notification advises you to restart the **Cisco XCP Router**, then restart the **Cisco XCP Router** on all cluster nodes. Otherwise, you can skip this step.

Step 8 Repeat this procedure on the database publisher node of the remote intercluster peer.

Tip If you configure the intercluster peer connection before the Sync Agent completes the user synchronization from Cisco Unified Communications Manager (on either the local or remote cluster), the status of the intercluster peer connection will display as Failed.

If you choose TLS as the intercluster transport protocol, IM and Presence Service attempts to automatically exchange certificates between intercluster peers to establish a secure TLS connection. IM and Presence Service indicates whether the certificate exchange is successful in the intercluster peer status section.

What to do next

Proceed to turn on the Intercluster Sync Agent.

Related Topics

Restart Cisco XCP Router Service, on page 78
Node Name Value for Intercluster Deployments, on page 29
IM and Presence Default Domain Value for Intercluster Deployments, on page 30
Default Domain Value for Intercluster Deployments

Turn On Intercluster Sync Agent

By default, IM and Presence Service turns on the Intercluster Sync Agent parameter. Use this procedure to either verify that the Intercluster Sync Agent parameter is on, or to manually turn on this service.

The Intercluster Sync Agent uses the AXL/SOAP interface for the following:

- to retrieve user information for IM and Presence Service to determine if a user is a local user (on the local cluster), or a user on a remote IM and Presence Service cluster within the same domain.
- to notify remote IM and Presence Service clusters of changes to users local to the cluster.

Note You must turn on the Intercluster Sync Agent on all nodes in the IM and Presence Service cluster because in addition to synchronizing user information from the local IM and Presence database publisher node to the remote IM and Presence database publisher node, the Intercluster Sync Agent also handles security between all nodes in the clusters.

Procedure

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

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

Step 3 Choose **Cisco Intercluster Sync Agent**.

Step 4 Click **Start**.

What to do next

Proceed to verify the intercluster peer status.

Related Topics

Multinode Scalability Feature, on page 23

Verify Intercluster Peer Status

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Inter-Clustering**.

Step 2 Choose the peer address from the search criteria menu.

Step 3 Click **Find**.

Step 4 Choose the peer address entry that you wish to view.

Step 5 In the **Intercluster Peer Status** window:

a) Verify that there are check marks beside each of the result entries for the intercluster peer.

b) Make sure that the Associated Users value equals the number of users on the remote cluster.

c) If you choose TLS as the intercluster transport protocol, the Certificate Status item displays the status of the TLS connection, and indicates if IM and Presence Service successfully exchanged security certificates between the clusters. If the certificate is out-of-sync, you need to manually update the tomcat trust certificate (as described in this module). For any other certificate exchange errors, check the Online Help for a recommended action.

Step 6 Choose **Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter**.

Step 7 Verify that there are check marks beside the status of each of the intercluster peer connection entries in the InterClustering Troubleshooter section.

Update Intercluster Sync Agent Tomcat Trust Certificates

If the tomcat certificate status for an intercluster peer is out-of-sync, you need to update the Tomcat trust certificate. In an intercluster deployment this error can occur if you reuse the existing Intercluster Peer Configuration to point to a new remote cluster. Specifically, in the existing Intercluster Peer Configuration window, you change the Peer Address value to point to a new remote cluster. This error can also occur in a fresh IM and Presence Service installation, or if you change the IM and Presence Service host or domain name, or if you regenerate the Tomcat certificate.

This procedure describes how to update the Tomcat trust certificate when the connection error occurs on the local cluster, and the corrupt Tomcat trust certificates are associated with the remote cluster.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Inter-Clustering.**

Step 2 Click **Force Sync** to synchronize certificates with the remote cluster.

Step 3 In the confirmation window that displays, choose **Also resync peer's Tomcat certificates**.

Step 4 Click **OK**.

Note If there are any certificates that have not synced automatically, go to the Intercluster Peer Configuration window and all certificates marked with an x are the missing certificates which you need to manually copy.

Delete Intercluster Peer Connections

Use this procedure if you want to remove an intercluster peer relationship.

Procedure

Step 1 Log in to the IM and Presence Service database publisher node.

Step 2 From Cisco Unified CM IM and Presence Administration, choose **Presence** > **Inter-Clustering**.

Step 3 Click **Find** and select the intercluster peer that you want to remove.

Step 4 Click **Delete**.

Step 5 Restart the **Cisco XCP Router**:

a) Log in to Unified IM and Presence Serviceability and choose **Tools** > **Control Center - Network Services**.
b) From the **Server** list, choose the database publisher node and click **Go**.
c) Under **IM and Presence Services**, select **Cisco XCP Router** and click **Restart**.

Step 6 Repeat these steps on the peer cluster.

Note If you are removing an intercluster peer from an intercluster network with multiple clusters, you must repeat this procedure for each peer cluster that remains in the intercluster network. This means that, on the cluster that is being removed, there will be as many cycles of **Cisco XCP Router** restarts as there are peer cluster connections that are being broken.

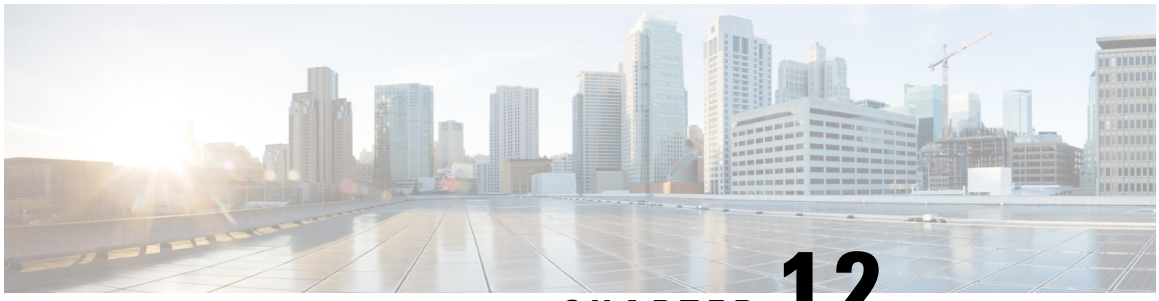
Intercluster Peering Interactions and Restrictions

Feature	Interactions and Restrictions
Cisco Business Edition 6000	Intercluster peering is not supported when the IM and Presence Service is deployed on a Cisco Business Edition 6000 server.

Feature	Interactions and Restrictions
Cluster Limit	With intercluster peering, you can deploy up to 30 IM and Presence Service clusters in the intercluster mesh, irrespective of whether those clusters are centralized or decentralized.

PART III

Feature Configuration



CHAPTER 12

Availability and Instant Messaging on IM and Presence Service Configuration

Availability Setup on IM and Presence Service

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

This procedure describes how to turn on or off availability sharing for all client applications in a IM and Presence Service cluster.

Availability sharing is turned on by default on IM and Presence Service.

Procedure

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

Step 2 Configure the availability setting. Perform one of the following actions:

- To turn on availability sharing in the IM and Presence Service cluster, check **Enable availability sharing**. If you turn on this setting, IM and Presence Service shares availability information for a user amongst all users in the cluster, based on the policy settings for that user.

  The default policy setting for a user is to allow all other users view their availability. Users configure their policy settings from the Cisco Jabber client.

- To turn off availability sharing for all clients in the IM and Presence Service cluster, uncheck **Enable availability sharing.**. If you turn off this setting, IM and Presence Service does not share any availability to other users in the IM and Presence Service cluster, nor does it share availability information it receives from outside the cluster. Users can only view their own availability status.

Step 3 Click **Save**.

Step 4 Restart the following services:

a) Cisco XCP Router

b) Cisco Presence Engine

Tip
- When you turn off availability sharing, a user can view their own availability status on the client application; the availability status for all other users are greyed out.
- When you turn off availability sharing, when a user enters a chat room, their availability status shows a status of "Unknown" with a green icon.

Configure Ad-Hoc Presence Subscription Settings

Note These settings allow users to initiate ad-hoc presence subscriptions to users that are not on their contact list.

Procedure

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

Step 2 Check **Enable ad-hoc presence subscriptions** to turn on ad-hoc presence subscriptions for Cisco Jabber users.

Step 3 Set the maximum number of active ad-hoc subscriptions that IM and Presence Service permits at one time. If you configure a value of zero, IM and Presence Service permits an unlimited number of active ad-hoc subscriptions.

Step 4 Set the time-to-live value (in seconds) for the ad-hoc presence subscriptions.

When this time-to-live value expires, IM and Presence Service drops any ad-hoc presence subscriptions and no longer temporarily monitors the availability status for that user.

Note If the time-to-live value expires while the user is still viewing an instant message from a ad-hoc presence subscription, the availability status that displays may not be current.

Step 5 Click **Save**.

You do not have to restart any services on IM and Presence Service for this setting, however Cisco Jabber users will have to sign out, and sign back in to retrieve the latest ad-hoc presence subscriptions settings on IM and Presence Service.

Configure Maximum Contact List Size Per User

You can configure the maximum contact list size for a user; this is the number of contacts the user can add to their contact list. This setting applies to the contact list on Cisco Jabber client applications and on third-party client applications.

Users who reach the maximum number of contacts are unable to add new contacts to their contact list, nor can other users add them as a contact. If a user is close to the maximum contact list size, and the user adds a group of contacts that pushes the contact list over the maximum number, IM and Presence Service does not add the surplus contacts. For example, if the maximum contact list size on IM and Presence Service is 200. A user has 195 contacts and attempts to add 6 new contacts to the list, IM and Presence Service adds five contacts and does not add the sixth contact.

Tip The System Troubleshooter in Cisco Unified CM IM and Presence Administration indicates if there are users who have reached the contact list limit.

If you are migrating users to IM and Presence Service, Cisco recommends that you set the Maximum Contact List Size and Maximum Watchers settings to Unlimited while importing user contact lists. This ensures that each migrated user contact list is fully imported. After all users have migrated, you can reset the Maximum Contact List Size and Maximum Watchers settings to the preferred values.

Procedure

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

Step 2 Edit the value of the **Maximum Contact List Size (per user)** setting.

The default value is 200.

Tip Check the **No Limit** check box to allow an unlimited contact list size.

Step 3 Click **Save**.

Step 4 Restart the Cisco XCP Router service.

Related Topics

Restart Cisco XCP Router Service, on page 78

Configure Maximum Number of Watchers Per User

You can configure the number of watchers for a user, specifically the maximum number of people that can subscribe to see the availability status for a user. This setting applies to the contact list on Cisco Jabber clients and on third-party clients.

If you are migrating users to IM and Presence Service, Cisco recommends that you set the Maximum Contact List Size and Maximum Watchers settings to Unlimited while importing user contact lists. This ensures that each migrated user contact list is fully imported. After all users have migrated, you can reset the Maximum Contact List Size and Maximum Watchers settings to the preferred values.

Procedure

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

Step 2 Edit the value of the **Maximum Watchers (per user)** setting.

The default value is 200.

Tip Check the **No Limit** check box to allow an unlimited number of watchers.

Step 3 Click **Save**.

Step 4 Restart the Cisco XCP Router service.

IM Setup On IM and Presence Service

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

This procedure describes how to turn on or off instant message capabilities for all client applications in a IM and Presence Service cluster. Instant message capabilities is turned on by default on IM and Presence Service.

⚠

Caution When you turn off instant message capabilities on IM and Presence Service, all group chat functionality (ad hoc and persistent chat) will not work on IM and Presence Service. We recommend that you do not turn on the Cisco XCP Text Conference service or configure an external database for persistent chat on IM and Presence Service.

Procedure

Step 1 Log in to **Cisco Unified CM IM and Presence Administration**, choose **Messaging** > **Settings**.

Step 2 Configure the instant messaging setting. Do one of the following actions:

- To turn on instant message capabilities for client applications in the IM and Presence Service cluster, check **Enable instant messaging.**. If you turn on this setting, local users of client applications can send and receive instant messages.
- To turn off instant message capabilities for client applications in the IM and Presence Service cluster, uncheck **Enable instant messaging.**.

  Note If you turn off this setting, local users of client applications cannot send and receive instant messages. Users can only use the instant messaging application for availability and phone operations. If you turn off this setting, users do not receive instant messages from outside the cluster.

Step 3 Click **Save**.

Step 4 Restart the Cisco XCP Router service.

Turn On or Off Offline Instant Messaging

By default IM and Presence Service stores (locally) any instant messages that are sent to a user when they are offline, and IM and Presence Service delivers these instant messages to the user the next time they sign in to

the client application. You can turn off (suppress) this feature so IM and Presence Service does not store offline instant messages.

Note IM and Presence Service limits offline messages to 100 per user up to a maximum of 30000 per node.

Procedure

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

Step 2 Configure the offline instant messaging. Perform one of the following actions:

- To turn off the storage of offline instant messages on IM and Presence Service, check **Suppress Offline Instant Messaging.**. If you check this setting, any instant messages that are sent to a user when they are offline, IM and Presence Service does not deliver these instant messages to the user the next time they sign in to the client application.
- To turn on the storage of offline instant messages on IM and Presence Service, uncheck **Suppress Offline Instant Messaging.**. If you uncheck this setting, any instant messages that are sent to a user when they are offline, IM and Presence Service delivers these instant messages to the user the next time they sign in to the client application.

Step 3 Click **Save**.

Allow Clients to Log Instant Message History

You can prevent or allow users to log instant message history locally on their computer. On the client side, the application must support this functionality; it must enforce the prevention of instant message logging.

Procedure

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

Step 2 Configure the log instant message history setting as follows:

- To allow users of client applications to log instant message history on IM and Presence Service, check **Allow clients to log instant message history (on supported clients only)**.
- To prevent users of client applications from logging instant message history on IM and Presence Service, uncheck **Allow clients to log instant message history (on supported clients only)**.

Step 3 Click **Save**.

Allow Cut and Paste in Instant Messages

You can prevent or allow users to log instant message history locally on their computer. On the client side, the application must support this functionality; it must enforce the prevention of instant message logging.

Procedure

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

Step 2 Configure the cut and paste in instant messages setting as follows:

- To allow users of client applications to cut and paste in instant messages, check **Allow cut & paste in instant messages**.
- To prevent users of client applications from cutting and pasting in instant messages, uncheck **Allow cut & paste in instant messages**.

Step 3 Click **Save**.

Stream Management

The IM and Presence Service supports Stream Management for instant messaging. Stream Management is implemented using the XEP-0198 specification, which defines an Extensible Messaging and Presence Protocol (XMPP) extension for active management of an XML stream between two XMPP entities, including features for stanza acknowledgements and stream resumption. For more information about XEP-0198, see the specification at http://xmpp.org/extensions/xep-0198.html

If there is a temporary loss of communication between IM and Presence Service and Cisco Jabber, Stream Management ensures that any instant messages that are sent during the communications outage are not lost. A configurable timeout period determines how such messages are handled:

- If Cisco Jabber reestablishes communication with IM and Presence Service within the timeout period, the messages are resent.
- If Cisco Jabber does not reestablish communication with IM and Presence Service within the timeout period, the messages are returned to the sender.
- Messages that are sent after the timeout period lapses are stored offline and delivered when Cisco Jabber resumes communication with IM and Presence Service.

Stream Management is enabled by default on a cluster-wide basis. However, you can use the Stream Management service parameters to configure the feature.

Configure Stream Management

Use this procedure to cofigure Stream Management (XEP-0198) on the IM and Presence Service.

Procedure

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

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

Step 3 From the **Service** drop-down, choose **Cisco XCP Router**.

Step 4 Set the **Enable Stream Management** service parameter to **Enabled**.

Step 5 Under **Stream Management Parameters (Clusterwide)**, configure any of the Stream Management parameters:

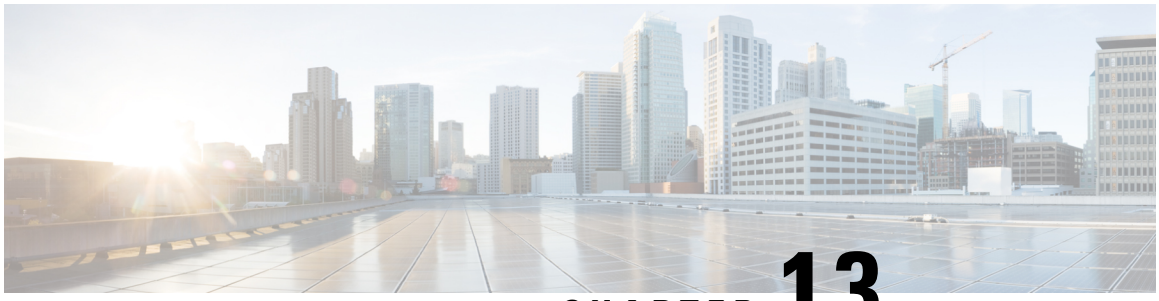
Table 20: Stream Management Service Parameters

Service Parameter	Description
Enable Stream Management	Enables or disables Stream Management cluster-wide. The default setting is Enabled.
Stream Management Timeout	The timeout controls how long a session (whose connection has been severed) will allow for a resume (in seconds) before giving up. If the client attempts to negotiate a longer timeout (or does not specify a desired timeout) this maximum will apply. Any messages that are sent after this timeout ends and before Cisco Jabber logs in again with IM and Presence Service are stored offline and resent after relogin. The range is 30 seconds—90 seconds. The default value is 60 seconds.
Stream Management Buffer	Defines the maximum number of packets (packet history) that will be kept in buffer for a stream management-enabled session. A stream resume will fail if the client needs more history than what is available in the buffer. The range is 5—150 packets with a default value of 100 packets.
Acknowledgement Request Rate	Defines the number of stanzas that the server sends before asking the client to provide the count of the last stanza received. A smaller number makes for more network traffic, but helps the server prune the stanza history buffer and reduces memory used. The range is 1—64 stanzas with a default value of 5. **Note** A smaller Acknowledgement Request Rate leads to increased network traffic, but reduced memory use.

Step 6 Click **Save**.

Availability and Instant Messaging Interactions and Restrictions

Feature	Interactions and Restrictions
Block Everyone	When a Cisco Jabber user enables the "Block Everyone" feature from within their Cisco Jabber policy settings, the block prevents other Jabber users from viewing or exchanging IMs and Presence with the blocking user, unless they are listed as a contact in the blocking user's contact list. For example, a Cisco Jabber user (Andy) has enabled Block everyone within his personal Jabber settings. The following list breaks down how Andy's block affects other Jabber users whom may or may not be included in Andy's personal contact list. In addition to the block, Andy has a personal contact list that: • Includes Bob—Because Bob is in Andy's personal contact list, he can still send IMs and view Andy's presence despite the block. • Omits Carol—Carol cannot view Andy's presence or send IMs due to the block.. • Omits Deborah as a personal contact. However, Deborah is a member of an enterprise group that Andy has listed as a contact—Deborah is blocked from viewing Andy's presence or sending IMs to Andy. Note that Deborah is blocked from viewing Andy's presence, or sending IMs to Andy, despite the fact that she is a member of an enterprise group in Andy's contact list. For additional details on enterprise group contacts behavior, see CSCvg48001.



CHAPTER 13

Configure Ad Hoc and Persistent Chat

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

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

Persistent Chat Rooms

Persistent chat rooms are group chat sessions that remain in existence even 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 Turn On or Off Instant Messaging for IM and Presence Service Cluster, on page 164.

Persistent Chat Prerequisites

If you are deploying persistent chat rooms:

- Make sure that instant messaging is enabled. For details, see Turn On or Off Instant Messaging for IM and Presence Service Cluster, on page 164.
- You must deploy an external database. For database setup and support information, see the *Database Setup Guide for IM and Presence Service* at http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html.
- 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.
- For Persistent Chat deployments, we recommend that you deploy a minimum OVA of 15,000 users.

Group Chat and Persistent Chat Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Group Chat System Administrators, on page 171	Add system administrators to manage the persistent chat system.
Step 2	Configure Chat Room Settings, on page 171	Configure basic chat room settings. Optionally, enable Persistent Chat.
Step 3	Restart the Cisco XCP Text Conference Manager, on page 172	If you are deploying Persistent Chat, make sure that the Cisco XCP Text Conference Manager service is running.
Step 4	Set up External Database for Persistent Chat, on page 173	For Persistent Chat, you must configure a unique external database instance for each node.

	Command or Action	Purpose
		Note If you are deploying High Availability for Persistent Chat, you can skip the remaining tasks in this chapter as the database requirements are slighlty different when HA is deployed.
Step 5	Add External Database Connection, on page 173	In the IM and Presence Service, set up a connection to your external database.

Configure Group Chat System Administrators

Add system administrators to manage the persistent chat system.

Procedure

Step 1 Choose **Messaging** > **Group Chat System Administrators**.

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 171

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

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Messaging** > **Group Chat and Persistent Chat**

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 partipants 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 172

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, proceed to the High Availability for Persistent Chat chapter of this guide.

Otherwise, Set up External Database for Persistent Chat, on page 173.

Set up External Database for Persistent Chat

Note 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.
- Use the External Database Cleanup Utility to set up jobs that monitor the database size and delete expired records automatically.
- 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.

For instructions on how to set up an external database, see *External Database Setup Guide for IM and Presence Service* at http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html.

What to do next

Add External Database Connection, on page 173

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

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.

Group Chat and Persistent Chat Interactions and Restrictions

Table 21: Group Chat and Persistent Chat Interactions and Restrictions

Feature Interaction	Restriction
Archiving room joins	Archiving room joins and leaves is optional because it will increase traffic and consume space on the external database server.
Chat with anonymous rooms	If you are deploying chat via Cisco Jabber (either group chat or persistent chat), make sure that the **Rooms are anonymous by default** and **Room owners can change whether or not rooms are anonymous** options are not selected in the **Group Chat and Persistent Chat Settings** window. If either check box is checked, chat will fail
Database Connection Issues	If the connection with the external database fails after the Text Conference Manager service has started, the Text Conference Manager service will remain active and functional, however, messages will no longer be written to the database and new persistent rooms cannot be created until the connection recovers.
OVA Requirements	If you are deploying Persistent Chat or Intercluster Peering, the minimum OVA size that you can deploy for these features is the 5000 user OVA. It's recommended that you deploy at least the 15,000 user OVA. Centralized Deployments may require the 25,000 user OVA, depending on the size of the user base. For additional details on OVA options and user capacities, refer to the following site: **Note** It's strongly recommended to deploy at least the 15,000 user OVA on all IMP nodes. https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html

Feature Interaction	Restriction
Persistent chat character limit with Microsoft SQL Server	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.
Persistent Chat for Jabber Mobile where a peer cluster is running a non-supported release	Persistent chat for Jabber mobile is introduced with 11.5(1)SU5 and is not supported on earlier 11.5(1)SU releases. This feature is also not supported for 12.0(1) or 12.0(1)SU1. If you have Persistent Chat for Jabber mobile deployed in this release, and you also have intercluster peering set up with peer clusters that do not support persistent chat rooms for Jabber Mobile, the following conditions apply for Jabber mobile clients: If the persistent chat room is hosted on a non-supported release, such as 11.5(1): • A Jabber mobile client that is homed from the supported cluster can join persistent chat rooms hosted on the non-supported cluster, but will have no option to mute the room. They will see a Global Mute option, but it will not work. • A Jabber mobile client that is homed on the non-supported peer cluster will be unable to join any persistent chat rooms. If the persistent chat room is hosted on a supported release, such as 11.5(1)SU5: • A Jabber mobile client participant that is homed on the supported cluster will have all persistent chat on mobile functionality. • A Jabber mobile client from a non-supported peer cluster will be unable to join persistent chat rooms. **Note** The search feature for Persistent Chat does not work when the Jabber Configuration file *(jabber-config.xml)* is set to disable the IM History.
External Database connectivity and Cisco XCP Text Conferencing service	In a split-brain scenario, When the subscriber or publisher detects its peer Text Conferencing service or any node is down, then the subscriber or publisher attempts a transition from normal to backup. During this operation if loading of the peer's chat rooms fails to connect to external database, then the Cisco XCP Text Conferencing service will shutdown.

Feature Interaction	Restriction
Number of Persistent chat rooms supported if High Availability is configured	The maximum number of Persistent Chat Rooms supported on an IM&P deployment is 5000 per subcluster. If High Availability is enabled, it is recommended to create a maximum of 2500 rooms per node. (though the system allows to create upto maximum of 5000 rooms per node). If more than 2500 rooms are configured per node in a High Availability deployment, then during failover, there would be more than 5000 rooms hosted on the backup node. This might result in unexpected performance issues depending on the traffic load. The load of 5000 rooms on the system also depends on the number of participants in the room, the rate of message exchange in the rooms and the size of messages. Use Cisco Collaboration Sizing tool to ensure you have the right OVA setup for your Persistent Chat Deployment. For Information on Collaboration Sizing tool, Please refer: https://cucst.cloudapps.cisco.com/landing It is recommended to have your rooms balanced equally among both the nodes in a subcluster. And if you have more than one subcluster in a IM&P Cluster, it is recommended to also load balance the rooms across all the subclusters. Currently IM&P doesn't have a mechanism to automatically load balance the rooms. The responsibility of load balancing the room lies with the users creating the rooms. During room creation, users have to ensure that they use the jabber feature to automatically select a random node for a room creation.
Making ad hoc chat rooms private	Ad hoc chat rooms are public by default, but can be configured to be for members only with the following configuration: 1. From Cisco Unified CM IM and Presence Administration, choose **Messaging** > **Group Chat and Persistent Chat**. 2. Check the **Rooms are for members only by default** check box. 3. Uncheck the **Room owners can change whether or not rooms are for members onl**y check box. 4. Uncheck the **Only moderators can invite people to members-only rooms** check box. 5. Click **Save**. 6. Restart the Cisco XCP Text Conference service.

Persistent Chat Examples (without HA)

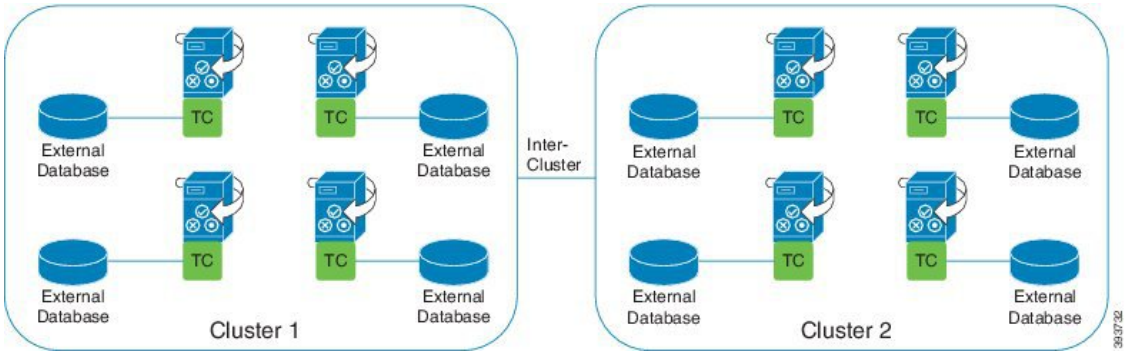
The following two examples illustrate the Persistent Chat feature along with intercluster peering where High Availability for Persistent Chat is not deployed.

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.

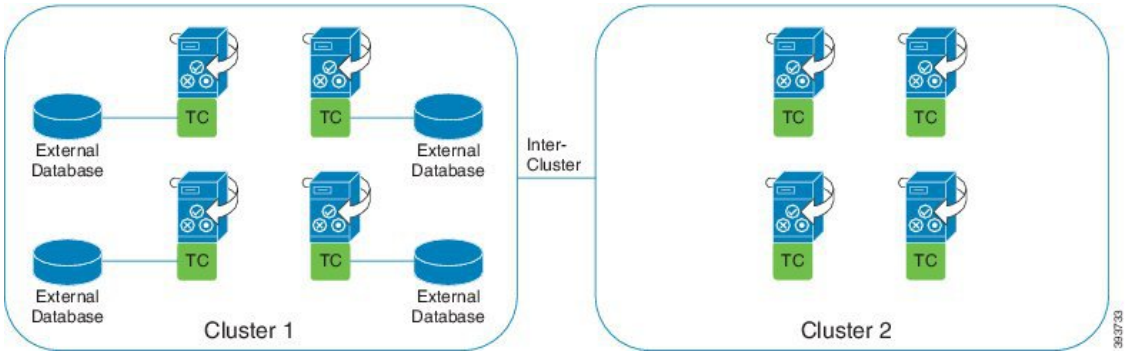
The Cisco Text Conferencing service is running on all nodes in either cluster, allowing all users in either cluster to join persistent chat rooms that are hosted on any node in either cluster.



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.



Persistent Chat Boundaries in IM and Presence

This section describes the matrix representing persistent chat (PChat) boundaries in IM and Presence with examples to clarify various dependencies.

The following assumptions are made for deriving the persistent chat boundaries:

1. With respect to the number of rooms per alias/server/subcluster/cluster:
   a. The server may contain several text conferencing aliases.
   b. A subcluster contains two servers (nodes).
   c. A cluster may have up to three subclusters.
2. If high availabilty (HA) is enabled, all supported room numbers are halved. The maximum allowed value for the **Maximum number of persistent chat rooms allowed** is 2500.
3. Example: Assuming 100 users per rooms in average, the IM and Presence service can support:
   a. 3500 persistent chat rooms per server without HA, or
   b. 1750 persistent chat rooms per server with HA.
   c. Assuming one message per room per minute, up to 273 persistent chat rooms can be active per server.

The following are some examples to clarify these dependencies:

Rooms supported per time slice can be increased at the expense of the total number of rooms supported by using the following formula:

New Number of Rooms Supported = Current Number of Rooms Supported * Current Number of Rooms Supported Per Time Slice (%) / New Rooms Supported Per Time Slice (%)

Table 22: 25K OVA Persistent Chat Capacity Table (Per Server)

Average Number of Users per Room	Number of PChat Rooms Supported	Rooms Supported Per Time Slice Message Frequency = 1/min	Rooms Supported Per Time Slice Message Frequency = 3/min
2	5000	100%	100%
5	5000	100%	58%
10	5000	99%	33%
15	5000	69%	23%
20	5000	53%	18%
30	5000	36%	12%
50	5000	22%	7%
100	3497	16%	5%
200	2064	14%	5%
500	926	12%	4%
1,000	482	12%	4%

Note It is assumed that 30% of the users have two devices/clients.

Example for 25K OVA:

Average Number of Users per Room = 10

Message frequency = 3/ min

Current Number of Rooms Supported = 5000

Current Rooms Supported per Time Slice = 33%

New Rooms Supported per Time Slice = 50%

Result:

New Rooms Supported = 5000 * 33/50 =3300

Table 23: 15K OVA Persistent Chat Capacity Table (Per Server)

Average Number of Users per Room	Number of PChat Rooms Supported	Rooms Supported Per Time Slice Message Frequency = 1/min	Rooms Supported Per Time Slice Message Frequency = 3/min
2	5000	100%	80%
5	5000	100%	41%
10	5000	67%	22%
15	5000	46%	15%
20	5000	35%	12%
30	5000	24%	8%
50	5000	14%	5%
100	3497	10%	3%
200	2064	9%	3%
500	926	8%	3%
1,000	482	7%	2%

Note It is assumed that 30% of the users have two devices/clients.

Example for 15K OVA:

Average Number of Users per Room = 5

Message frequency = 3/ min

Current Number of Rooms Supported = 5000

Current Rooms Supported per Time Slice = 41%

New Rooms Supported per Time Slice = 50%

Result:

New Rooms Supported = 5000 * 41/50 =4100

Table 24: 5K OVA Persistent Chat Capacity Table (Per Server)

Average Number of Users per Room	Number of PChat Rooms Supported	Rooms Supported Per Time Slice Message Frequency = 1/min	Rooms Supported Per Time Slice Message Frequency = 3/min
2	5000	94%	31%
5	5000	53%	18%
10	4654	33%	11%
15	4261	26%	9%
20	3929	21%	7%
30	3399	17%	6%
50	2677	13%	4%
100	1748	10%	3%
200	1032	9%	3%
500	463	8%	3%
1,000	241	7%	2%

Note It is assumed that 30% of the users have two devices/clients.

Example for 5K OVA:

Average Number of Users per Room = 2

Message frequency = 3/ min

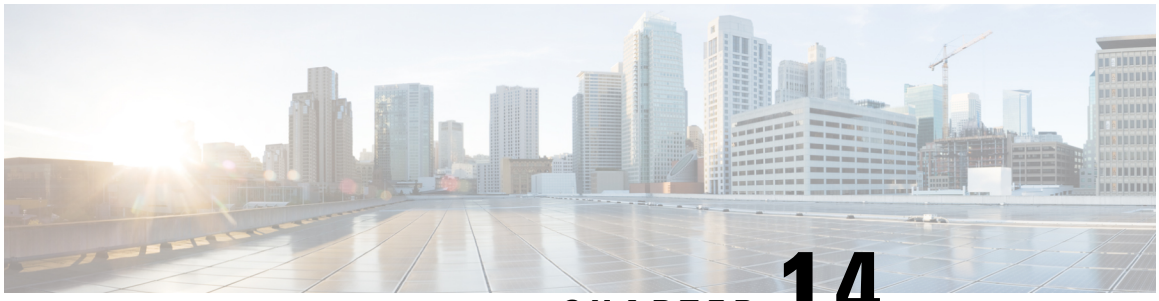
Current Number of Rooms Supported = 5000

Current Rooms Supported per Time Slice = 31%

New Rooms Supported per Time Slice = 50%

Result:

New Rooms Supported = 5000 * 31/50 =3100



CHAPTER 14

High Availability for Persistent Chat on IM and Presence Service

High Availability for Persistent Chat Overview

From the current release the persistent chat feature is highly available. In the event of 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 TC service. After failover jabber clients can seamlessly continue to use the persistent chat rooms.

For further information on high availability, see the Configure Presence Redundancy Groups chapter of the System Configuration Guide for Cisco Unified Communications Manager.

For this example there are three users: A, B, and C and three IM and Presence Service nodes: 1A, 2A, and 1B. Node 1A and Node 1B are part of the same Presence Redundancy Group and form a High Availability (HA) pair. The users are assigned to the following nodes:

- User A is on Node 1A
- User B is on Node 2A
- User C is on Node 1B

1. Users A, B, and C are in a chat room hosted on Node 1A.
2. The Text Conferencing (TC) service fails on Node 1A.
3. The IM and Presence Service administrator starts a manual fallback.
4. Node 1B transitions to the HA state **Failed Over with Critical Services not Running**, before transitioning to the HA state **Running in Backup Mode**.
5. In line with the HA Failover Model, User A is signed out automatically and is signed in to the backup Node 1B.
6. Users B and C are not affected but continue to post messages to the chat room hosted on Node 2A.

7. Node 1A transitions to **Taking Back** and Node 1B transitions to **Falling Back**.
8. User A is signed out of Node 1B. Users B and C 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 **Taking Back** to **Normal** and it unloads its peer node rooms.
10. Node 1A moves from the HA state **Failing Over** to **Normal** and it reloads rooms associated with pubalias.cisco.com.
11. User A signs in again to Node 1A, enters the persistent chat room and continues to read or post messages to the room.

Table 25: Group Chat and Persistent Chat Restrictions

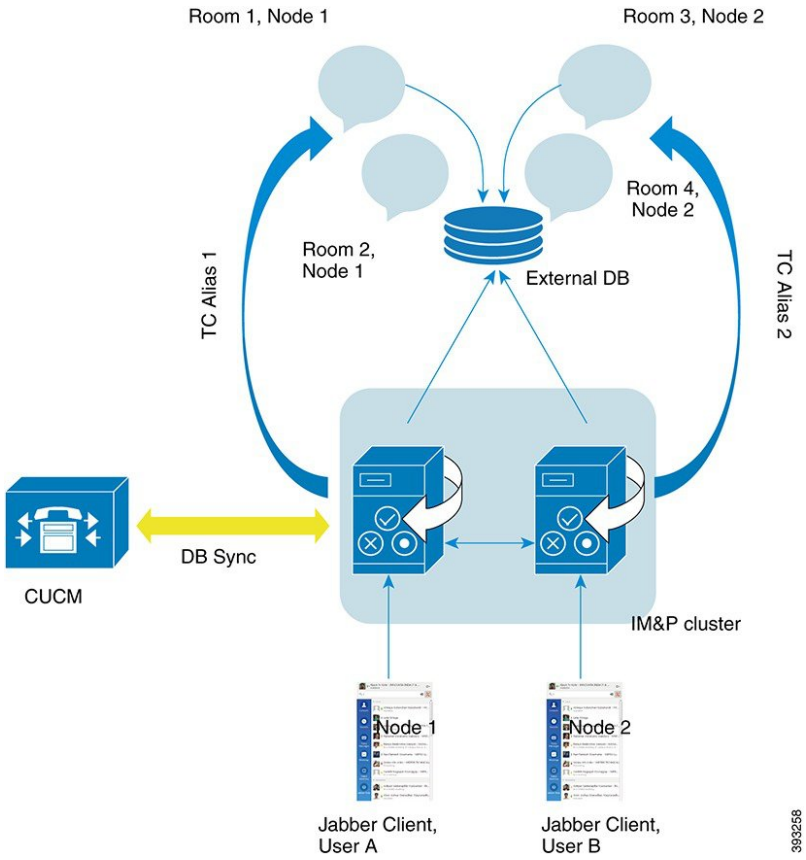
Feature	Restriction
Chat with anonymous rooms	If you are deploying chat via Cisco Jabber (either group chat or persistent chat), make sure that the **Rooms are anonymous by default** and **Room owners can change whether or not rooms are anonymous** options are not selected in the **Group Chat and Persistent Chat Settings** window. If either check box is checked, chat will fail

High Availability for Persistent Chat Flows

The following flows demonstrate the high availability for persistent chat flows for failover and failback.

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.

Figure 14: High Availability for Persistent Chat Structure



High Availability for Persistent Chat Failover Flow

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:

Subcluster 1	Subcluster 2
• Andy is on Node 1A—Node 1A hosts the chat room • Bob is on Node 1B	• Catherine is on Node 2A • Deborah is on Node 2B

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 for Persistent Chat Fallback Flow

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:

Subcluster 1	Subcluster 2
• Andy is on Node 1A—Node 1A hosts the chat room • Bob is on Node 1B	• Catherine is on Node 2A • Deborah is on Node 2B

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.

Enable and Verify High Availability for Persistent Chat

To enable and verify that high availability for persistent chat is working correctly, carry out the steps in the following procedure:

Procedure

Step 1 Ensure that high availability is enabled in the presence redundancy group:

a) From **Cisco Unified CM Administration**, click **System** > **Presence Redundancy Groups**.
b) On the **Find and List Presence Redundancy Groups** window, click **Find** and choose the Presence Redundancy Group you want to check.
c) On the **Presence Redundancy Group Configuration** window, ensure that the **Enable High Availability** check box is checked.

Step 2 Ensure that persistent chat is enabled on the presence redundancy group:

a) From **Cisco Unified CM IM and Presence Administration UI**, click **Messaging** > **Group Chat and Persistent Chat**.
b) On the **Group Chat and Persistent Chat Settings** window, ensure that the **Enable Persistent Chat** check box is checked.

Step 3 Ensure that both presence redundancy group nodes are assigned to to the same external database. See image.

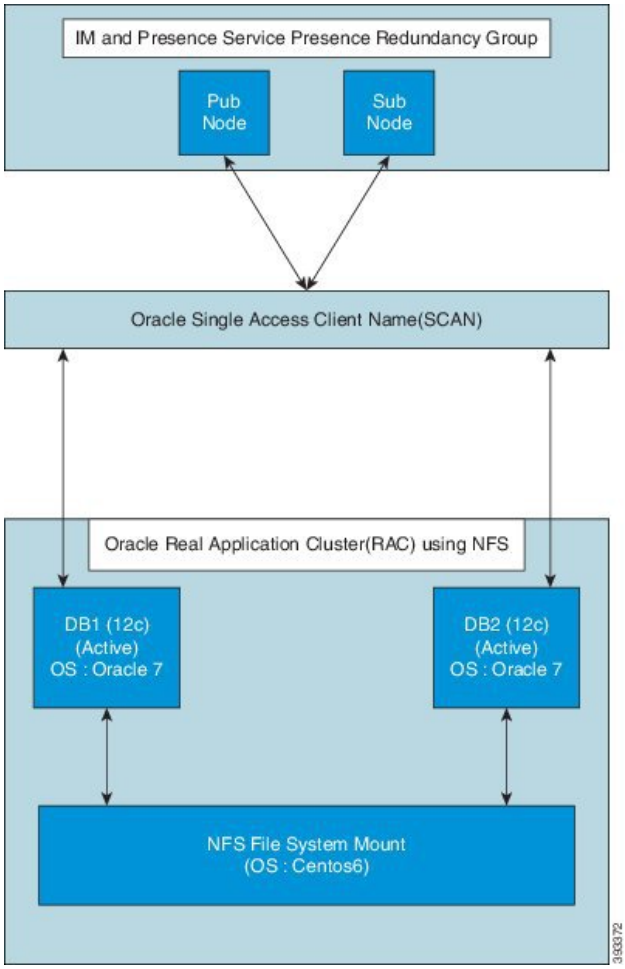
Step 4 To verify that high availability for persistent chat is enabled, check the **System** > **Presence Topology** window. In the Node Status section of the **Node Detail** pane, in the **Service Column**, check that the **Cisco XCP Text Conference Manager** entry has Yes in its **Monitored** column.

If it is a monitored service, this means that it is a critical service and that high availability has been successfully enabled. If it is not, then check that your presence redundancy group has been configured correctly.

External Database for Persistent Chat High Availability

For information on supported versions, refer to the External Database Setup Requirements section of the *Database Setup Guide for IM and Presence Service*.

Figure 15: Oracle High Availability Setup



Merge External Database Tables

The External Database Merge Tool allows persistent chat data which is stored on multiple external database partitions to be merged into a single database.

On earlier versions, each IM and Presence Service node in a presence redundancy group was assigned to a unique external database. From the current release, to enable High Availability for Persistent Chat, nodes in a presence redundancy group must be assigned to only one external database. The External Database Merge Tool allows you to quickly combine these two databases.

The External Database Merge Tool can be used on Oracle and Postgres databases.

Note To use the External Database Merge Tool on an Oracle database, the **Oracle SID** field must have the same value as the **Database Name** field. Otherwise, the merge will fail. For more information, see CSCva08935.

External Database Merge Tool

Use this procedure to merge the two databases in an IM and Presence Service presence redundancy group.

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 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>;`

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**.

Note 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**.

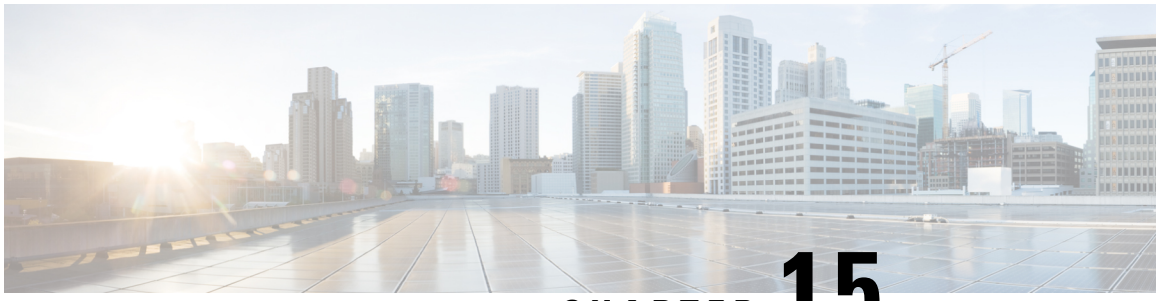
Step 9 When merging has completed successfully, the **Find And List External Database Jobs** window is loaded. Click **Find** to refresh the window and view the new job.

Click the **ID** of the job if you want to view its details.

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.



CHAPTER 15

Managed File Transfer

Managed File Transfer

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.

This configuration is specific to file transfers and has no impact on the message archiver feature for regulatory compliance.

Supported Software

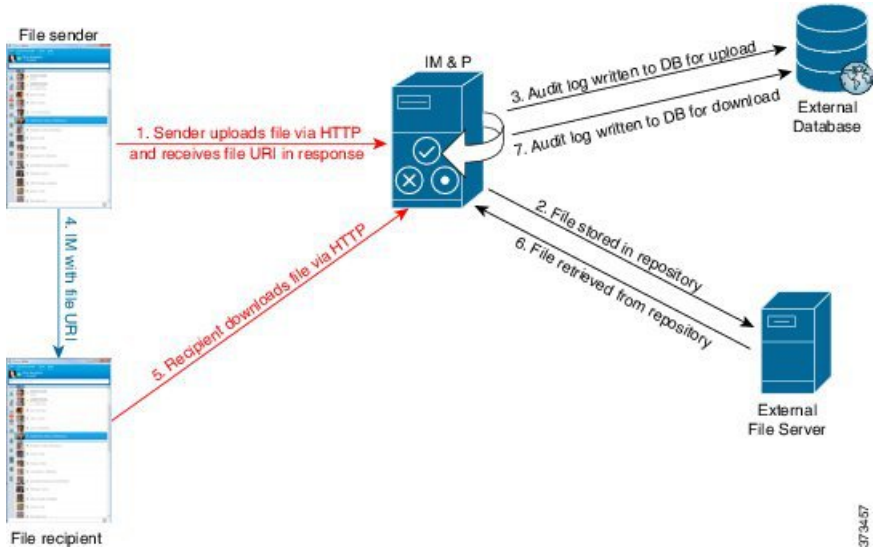
For detailed information on supported databases for Managed File Transfer, refer to the "External Database Requirements" chapter of the *Database Seup Guide for the IM and Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Related Topics

PostgreSQL documentation

Oracle documentation

File Transfer Flow



1. The sender's client uploads the file via HTTP, and the server responds with a URI for the file.
2. The file is stored in the repository on the file server.
3. An entry is written to the external database log table to record the upload.
4. The sender’s client sends an IM to the recipient; the IM includes the URI of the file.
5. The recipient’s client requests the file via HTTP. After reading the file from the repository (6) and recording the download in the log table (7), the file is downloaded 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.

Important Notes

Before you enable managed file transfer on an IM and Presence Service node consider these points:

- If you deploy any combination of the persistent group chat, message archiver, or managed file transfer features on an IM and Presence Service node, you can assign the same physical external database installation and external file server to all of these features. However, you should consider the potential IM traffic, the number of file transfers, and the file size when you determine the server capacity.

- Ensure that all clients can resolve the full FQDN of the IM and Presence Service node to which they are assigned. For the managed file transfer feature to work, it is not enough for the clients to resolve the hostname; they must be able to resolve the FQDN.
- 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.
- The Cisco XCP File Transfer Manager service must be active on each node where managed file transfer is enabled.

You can configure one of the following options on the **File Transfer** window:

- **Disabled**—file transfer is disabled for the cluster.
- **Peer-to-Peer**—one-to-one file transfers are allowed, but files are not archived or stored on a server. Group chat file transfer is not supported.
- **Managed File Transfer**—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.
- **Managed and Peer-to-Peer File Transfer**—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.

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.

External Database

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 logs the metadata associated with a file transfer, including:

- AFT index—the sequence number that identifies the transaction.
- JID—the Jabber ID of the user who uploaded or downloaded a file.
- To JID—the Jabber ID of the user, group chat, or persistent room that is the intended recipient of the file transfer.
- File name—the autogenerated encoded resource name assigned to the uploaded file.
- Real file name—the real name of the uploaded file.
- File server—the hostname or IP address of the file server where the file is stored.
- File path—the absolute path to the file (including the file name) on the file server.

- File size—the size of the file in bytes.
- Time stamp value—the date and time (UTC) the file was uploaded or downloaded.

Note For a full list of the logged metadata, see *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* at this link.

Important Notes

- The external database requirements and restrictions differ depending on the features you want to deploy on IM and Presence Service:
  - Managed file transfer—you require one unique logical external database instance for each IM and Presence Service node in an IM and Presence Service cluster.
  - Persistent group chat—you require one unique logical external database instance for each IM and Presence Service node in an IM and Presence Service cluster.

Note Each node requires its own logical database instance, but nodes can share the same physical database installation.

  - Message archiver—we highly recommend that you configure at least one logical external database instance for an IM and Presence Service cluster. However, you may require more than one external database for a cluster depending on your IM traffic and server capacity.
- If IM and Presence Service connects to an external database server using IPv6, ensure that the enterprise parameter is configured for IPv6 and that the Ethernet interface is set for IPv6 on each node in the deployment. Otherwise, the connection to the external database server fails and the Cisco XCP Message Archiver and Cisco XCP Text Conference Manager services are unable to connect to the external database and fail. For information about configuring IPv6 on IM and Presence Service, see the Related Topics.
- For information about database size and scalability for the managed file transfer feature, see the *Cisco Collaboration System Solution Reference Network Designs (SRND)* document at this link: http://www.cisco.com/c/en/us/solutions/enterprise/unified-communication-system/index.html

Related Topics

IPv6 Configuration, on page 96

External Database Disk Usage

You are responsible for managing the database disk usage. You must ensure that the disks or tablespaces do not become full, otherwise the managed file transfer feature may stop working. There are counters and alerts to help you manage database disk usage. See Cisco XCP File Transfer Manager RTMT Alarms and Counters, on page 200.

The following are sample SQL commands that you can use to purge records from the external database:

- to remove all records of files that were uploaded, run the following command:

DELETE

FROM *aft_log*

WHERE *method* = `'Post'`;

- to remove records of all files that were downloaded by a specific user, run the following command:

  DELETE

  FROM *aft_log*

  WHERE *jid* LIKE `'<userid>@<domain>%'` AND *method* = `'Get'`;

- to remove records of all files that were uploaded after a specific time, run the following command:

  DELETE

  FROM *aft_log*

  WHERE *method* = `'Post'` AND *timestampvalue* > `'2014-12-18 11:58:39'`;

See *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* at this link for sample SQL queries that you can adapt to purge records from the external database.

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.

External File Server

The file server is the repository for files transferred by the managed file transfer feature. Metadata associated with a managed file transfer is stored in an external database.

Note Files are stored on an external Linux file server, not on the IM and Presence Service node.

External File Server Requirements

Note the following requirements for the external file server.

- Subject to file server capacity, each IM and Presence Service node requires its own unique logical 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.

Recommendations for File Storage Partitions

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.

Important Notes

- You provide and maintain the external file server.
- You are responsible for managing file storage and disk usage. For more information about file server management, see the Related References.

  There are counters and alerts to help you manage file server disk usage. For more information about the managed file transfer alarms and counters, see the Related References.
- A file server partition/directory is mounted in the IM and Presence Service directory that is used to store files.
- The connection to the file server is encrypted using SSHFS, so the content of all files is encrypted.

Related Topics

Prerequisites, on page 204
File Server Management, on page 198
Cisco XCP File Transfer Manager RTMT Alarms and Counters, on page 200

User Authentication

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.
- 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 minimize man-in-the-middle attacks.

Public and Private Keys

When a server private/public key pair is generated the private key is usually written to `/etc/ssh/ssh_host_rsa_key`

The public key is written to `/etc/ssh/ssh_host_rsa_key.pub`

If these files do not exist, complete the following procedure:

1. Enter the following command:

   ```
   $ ssh-keygen -t rsa -b 2048
   ```

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*

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.

Note While checking the status from the publisher node to the subscriber node, and vice verse 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.

File Server Directories

You can create any directory structure 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.

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[1].
- 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.

File Server Management

You are responsible for managing file storage and disk usage. To manage the size of the external database, you can automatically purge files by combining queries with shell scripting. Your queries can use the metadata that is created when files are transferred including transfer type, file type, timestamp, absolute path on the file server to the file, and other information.

Note Do not purge files that were created during the current UTC hour.

[1] Remember to create this directory structure on every other node that will have managed file transfer enabled.

When choosing how to handle 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.

Sample Query and Output

You can perform queries on the AFT_LOG table and then use the output of the queries to purge unwanted files from the external file server.

For example, the following query returns records for every file that was uploaded after a specific date:

SELECT *file_path*

FROM *aft_log*

WHERE *method* = `'Post'` AND *timestampvalue* > `'2014-12-18 11:58:39'`;

The output of this query would be something like this:

```
/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
```

You can then write a script that uses the **rm** command and this output to remove these files from the external file server. See *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* at this link for more sample SQL queries that you can use to purge records from the external file server.

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.

Managed File Transfer Service Parameters

To help you to manage the external file server disk space, you can define the thresholds at which an RTMT alarm is generated with the following service parameters (for the Cisco XCP File Transfer Manager service):

- **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 for this service parameter 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 for this service parameter is 15%.

You must restart the Cisco XCP Router service after you change either of these parameters. To configure these parameters, log in to the **Cisco Unified CM IM and Presence Administration** interface, choose **System** > **Service Parameters**, and select the **Cisco XCP File Transfer Manager** service for the node.

Tip 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.

Related Topics

Cisco XCP File Transfer Manager RTMT Alarms and Counters, on page 200

Cisco XCP File Transfer Manager RTMT Alarms and Counters

Alerts

When an IM and Presence Service node is integrated with an external server and external database for managed file transfers, the transferred files are delivered to users 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 to the external database, IM and Presence Service does not deliver the file to the recipient.

To ensure that you are notified if the connections are lost, you should verify that the following RTMT alarm settings are properly configured.

Note Any files that were uploaded before the connection to the external file server was lost and were in the process of being downloaded, 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.

Alarm	Problem	Solution
XcpMFTExtFsMountError	Cisco XCP File Transfer Manager has lost its connection to the external file server.	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.
XcpMFTExtFsFreeSpaceWarn	Cisco XCP File Transfer Manager has detected that the available disk space on the external file server is low.	Free up space on the external file server by deleting unwanted files from the partition used for file transfer.

Alarm	Problem	Solution
XcpMFTDBConnectError	Cisco XCP data access layer was unable to connect to the database.	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.
XcpMFTDBFullError	Cisco XCP File Transfer Manager cannot insert or modify data in the external database because either the disk or tablespace is full.	Check the database and assess if you can free up or recover any disk space. Consider adding additional database capacity.

Cisco XCP MFT Counters

To help you administer managed file transfer, one new folder (Cisco XCP MFT Counters) and six new counters have been added to the RTMT.

Counter	Description
MFTBytesDownloadedLastTimeslice	This counter represents the number of bytes downloaded during the last reporting interval (typically 60 seconds).
MFTBytesUpoadedLastTimeslice	This counter represents the number of bytes uploaded during the last reporting interval (typically 60 seconds).
MFTFilesDownloaded	This counter represents the total number of files downloaded.
MFTFilesDownloadedLastTimeslice	This counter represents the number of files downloaded during the last reporting interval (typically 60 seconds).
MFTFilesUploaded	This counter represents the total number of files uploaded.
MFTFilesUploadedLastTimeslice	This counter represents the number of files uploaded during the last reporting interval (typically 60 seconds).

Configure XCP File Transfer Manager Alarms

Procedure

Step 1 Log in to **Cisco Unified IM and Presence Serviceability**.

Step 2 Choose **Alarm** > **Configuration**.

Step 3 Choose the server (node) to configure the alarm from the Server drop-down list, and click **Go**.

Step 4 Choose IM and Presence Services from the Service Group drop-down list, and click **Go**.

Step 5 Choose Cisco XCP File Transfer Manager (Active) from the Service drop-down list, and click **Go**.

Step 6 Configure the alarm settings as preferred and click **Save**.

Managed File Transfer Workflow

Procedure

	Command or Action	Purpose
Step 1	Set up an external database, see *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* at this link.	The external database is a repository that stores the metadata associated with archived files.
Step 2	Configure an External Database Instance on IM and Presence Service, on page 202	Provides the steps required to connect the IM and Presence Service node to an external database.
Step 3	Set Up an External File Server, on page 204	Provides the steps to configure an external Linux file server.
Step 4	Configure an External File Server Instance on IM and Presence Service, on page 208	Provides the steps required to connect the IM and Presence Service node to an external file server.
Step 5	Enable Managed File Transfer on IM and Presence Service, on page 210	Contains the set of instructions to enable the managed file transfer feature on the IM and Presence Service node. Provides ways to link the node to the external database and to link the node to the external file server.

Configure an External Database Instance on IM and Presence Service

Perform this configuration on the IM and Presence Service database publisher node of your cluster.

Before you begin

- Install and configure an external database, see *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* at this link.
- Obtain the hostname or IP address of the external database.
- If using Oracle as your database, retrieve the tablespace value.

  To determine the tablespace available for your Oracle database, execute the following query as sysdba:

```
SELECT DEFAULT_TABLESPACE FROM DBA_USERS WHERE USERNAME = 'UPPER_CASE_USER_NAME';
```

Procedure

Step 1 Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Messaging** > **External Server Setup** > **External Databases**.

Step 2 Click **Add New**.

Step 3 In the **External Database Settings** window, enter the following fields and click **Save**.

Field	Description
Database Name	Enter the name of the database that was defined during the external database installation. **Note** If you are using Oracle, this value must match the Windows service name.
Database Type	From the drop-down list choose the database type: Postgres or Oracle. **Note** If Oracle is chosen as the database type, the Enable SSL check box and the Tablespace field become active.
Tablespace	Enter the tablespace value.
User Name	Enter the user name for the database user (owner) that you defined during external database installation.
Password	Enter and confirm the password for the database user.
Hostname	Enter the hostname or IP address for the external database.
Port Number	Enter a port number for the external database. **Note** The default port numbers for Postgres (5432), Oracle (1521), and Oracle with SSL enabled (2484) are prepopulated in the **Port Number** field. You can choose to enter a different port number if required.
Enable SSL	Check the check box if you want to enable SSL. • The check box becomes enabled when Oracle is chosen as the Database Type. The option is not available with Postgres databases. • When you change either the **Enable SSL** check box, or the **Certificate Name** drop-down field, or both, a notification to restart the corresponding service (Cisco XCP Message Archiver or Cisco XCP Text Conference Manager) assigned to the external database is sent.

Field	Description
Certificate Name	From the drop-down list, choose a certificate. • The drop-down list becomes active when the Enable SSL check box is checked. • The certificate you need to enable SSL must be uploaded to the cup-xmpp-trust store. • After the certificate is uploaded to the cup-xmpp-trust store, you must wait 15 minutes for the certificate to propagate to all the nodes of the IM and Presence Service cluster. If you do not wait, the SSL connection on nodes where the certificate has not propagated fails. • If the certificate is missing or deleted from the cup-xmpp-trust store, an alarm XCPExternalDatabaseCertificateNotFound is raised in the Cisco Unified Communications Manager Real Time Monitoring Tool (RTMT).

After you click **Save**, IM and Presence Service provides the following status information on an external database:

- Database reachability—verifies that IM and Presence Service can ping an external database.
- Database connectivity—verifies that IM and Presence Service has successfully established an Open Database Connectivity (ODBC) connection with the external database.
- Database schema verification—verifies that the external database schema is valid.

Postgres only: If you make a configuration change in the `install_dir/data/pg_hba.conf` file or the `install_dir/data/postgresql.conf` file after you assign the external database, you should verify the external database connection.

What to do next

Set Up an External File Server, on page 204

Related Topics

http://www.postgresql.org/docs/manuals/
http://www.oracle.com/pls/db111/portal.portal_db?selected=11

Set Up an External File Server

Prerequisites

Tasks to complete before you begin to set up an external file server:

- Install and configure an external database, see *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* at this link.
- Configure an External Database Instance on IM and Presence Service, on page 202

Before setting up users, directories, ownership, permissions and other tasks on the file server, complete these steps.

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. See the *External File Server Requirements* topic for more information.

Related Topics

External File Server Requirements, on page 195

Set Up a User

Procedure

Step 1 On the file server as root, create a user who owns the file storage directory structure (our example uses *mftuser*) and force creation of the home directory (**-m**).

```
# useradd -m mftuser
```

```
# passwd mftuser
```

Step 2 Switch to the *mftuser*.

```
# su mftuser
```

Step 3 Create a `.ssh` directory under the *~mftuser* home directory that is used as a key store.

```
$ 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.

```
$ touch ~mftuser/.ssh/authorized_keys
```

Step 5 Set the correct permissions for passwordless SSH to function.

```
$ 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 Directories, on page 206

Set Up Directories

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 are used in the **External File Server Directory** field that you enter in the *Deploy an External File Server on IM and Presence Service* task.
- 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 the Public Key, on page 207

Obtain the Public Key

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.

Note
- 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 AAAQEAzRevlQCH1KFAnXwhd5UvEFzJs...

...a7y49d+/Am6+ZxkLc4ux5xXZueL3GSGt4rQUy3rp/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. It is used in the *Enable Managed File Transfer on IM and Presence Service* procedure.

What to do next

Configure an External File Server Instance on IM and Presence Service, on page 208

Configure an External File Server Instance on IM and Presence Service

The following procedure describes how to configure an external file server instance 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

- Install and configure an external database, see *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* at this link.
- Configure an External Database Instance on IM and Presence Service, on page 202
- Set Up an External File Server, on page 204
- Obtain the following external file server information:
  - Hostname, FQDN, or IP address
  - Public key
  - Path to the file storage directory
  - User name

Procedure

Step 1 Log in to the **Cisco Unified CM IM and Presence Administration** user interface. 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.

Field	Description
Name	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.
Host/IP Address	Enter the hostname or IP address of the file server. **Note** • 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). • If you change this setting, you must restart the Cisco XCP Router service.
External File Server Public Key	Paste the file server's public key (the key you were instructed to save to a text file) in to this field. If you did not save the key it can be retrieved from the file server by running the command: `$ ssh-keyscan -t rsa host` on the file server. Where *host* is the IP address, hostname, or FQDN of the file server. You must copy and paste the entire key text starting with the hostname, FQDN, or IP address to the end. For example, copy: extFileServer.cisco.com ssh-rsa AAAQEAzRevlQCH1KFAnXwhd5UvEFzJs... ...a7y49d+/Am6+ZxkLc4ux5xXZueL3GSGt4rQUy3rp/sdug+/+N9MQ== (ellipses added). **Important** This value must begin with the hostname, FQDN, or IP address that you entered for the Host/IP Address field. For example, if extFileServer is used in the Host/IP Address field, then this field must begin with extFileServer followed by the entire rsa key.
External File Server Directory	The path to the top of the file server directory hierarchy. For example, `/opt/mftFileStore/node_1/`
User Name	The user name of the external file server administrator.

Step 4 Repeat these steps to create an external file server instance for each node in the cluster that will have managed file transfer enabled.

Step 5 Click **Save**.

File Server Troubleshooting Tests

After the file server is assigned, the following tests are automatically executed. This occurs when you enable managed file transfer in the next procedure Enable Managed File Transfer on IM and Presence Service, on page 210. When the file server is assigned and you have started the Cisco XCP File Transfer Manager service, you should return to this section to verify the connection to the file server is trouble free.

The External File Server Status area displays a list of file server tests and results:

- Verify external file server reachability (pingable)
- Verify that external file server is listening for connections
- Verify external file server public key is correct
- Verify node public key is configured correctly on the external file server
- Verify external file server directory is valid
- Verify external file server has been mounted successfully
- Verify that free disk space is available on the file server

Tip

- You can change the name of the file server configuration, not the file server itself, after it is assigned.
- If you had managed file transfer configured and you change existing settings, restarting the Cisco XCP Router service restarts managed file transfer.
- If you change any other settings without changing them on the file server itself, file transfer stops working and you receive a notification to restart the Cisco XCP Router service.
- If a database or file server failure occurs, a message is generated that specifies the failure. However, the error response does not distinguish between database, file server, or some other internal failure. The RTMT also generates an alarm if there is a database or file server failure, this alarm is independent of whether a file transfer is occurring.

What To Do Next

Enable Managed File Transfer on IM and Presence Service, on page 210

Enable Managed File Transfer on IM and Presence Service

Before you begin

Complete the following tasks before you enable managed file transfer:

- Set up an external database, see *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* at this link.
- Configure an External Database Instance on IM and Presence Service, on page 202
- Set Up an External File Server, on page 204
- Configure an External File Server Instance on IM and Presence Service, on page 208

Procedure

Step 1 Log in to **Cisco Unified CM IM and Presence Administration**, choose **Messaging** > **File Transfer**.

Step 2 In the File Transfer Configuration area of the **The File Transfer** window, choose either **Managed File Transfer** or **Managed and Peer-to-Peer File Transfer**, depending on your deployment.

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
yc2EAAAABIwAAAQEAp2g+S2XDEzptN11S5h5nwVleKBnfG2pdW6KiLfzu/sFLegioIIqA8jBguNY/...

...5s+tusrtBBuciCkH5gfXwrsFS0O0AlfFvwnfq1xmKmIS9W2rf0Qp+A+G4MVpTxHgaonw==
imp@imp_node

(ellipses added).

Note
- 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 Ensure that the Cisco XCP File Transfer Manager service is active on all nodes where managed file transfer is enabled.

This service 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. Complete the following steps to check that the Cisco XCP File Transfer Manager service is active on all managed file transfer enabled nodes:

a) On any node in the cluster, log in to the **Cisco Unified IM and Presence Serviceability** user interface.

b) Choose **Tools** > **Service Activation**.
c) Choose a server (node) and click **Go**.
d) Ensure the check box next to Cisco XCP File Transfer Manager is checked and that the Activation Status is Activated.

   If the above conditions are not met click **Refresh**. If the Activation Status remains the same after a **Refresh**, go to Step 8.

e) Repeat steps c and d on all nodes where managed file transfer is enabled.

Step 8 If you are configuring the managed file transfer feature on a node for the first time, you must manually start the Cisco XCP File Transfer Manager service, as follows:

a) On any node in the cluster, log in to the **Cisco Unified IM and Presence Serviceability** user interface.
b) Choose **Tools** > **Control Center - Feature Activation**
c) Choose a server (node) and click **Go**.
d) In the IM and Presence Services area, click the radio button next to Cisco XCP File Transfer Manager.
e) Click **Start**.
f) Repeat steps c-e for all nodes where managed file transfer is enabled. This should be the same as step f) in step 9 below.

Step 9 (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.

a) Log in to the node's **Cisco Unified CM IM and Presence Administration** user interface.
b) Choose **System** > **Service Parameters**.
c) Choose the **Cisco XCP File Transfer Manager** service for the node.
d) Enter the required percentage values for the **External File Server Available Space Lower Threshold** and **External File Server Available Space Upper Threshold** service parameters.
e) Choose **Save**.

Step 10 Restart the Cisco XCP Router service.

a) On any node in the cluster, log in to the **Cisco Unified IM and Presence Serviceability** user interface.
b) Choose **Tools** > **Control Center - Network Services**.
c) Choose a server (node) and click **Go**.
d) In the IM and Presence Services area, click the radio button next to Cisco XCP Router.
e) Click **Restart**.
f) Repeat steps c-e for all nodes where managed file transfer is enabled.

Step 11 Verify that there are no problems with the external database setup and with the external file server setup.

- For the external database:
  a. Log in to the node's **Cisco Unified CM IM and Presence Administration** user interface.
  b. Choose **Messaging** > **External Server Setup** > **External Databases**.
  c. Check the information provided in the External Database Status area.
- On the node where you need to verify that the external file server is assigned:
  a. Log in to the node's **Cisco Unified CM IM and Presence Administration** user interface.
  b. Choose **Messaging** > **External Server Setup** > **External File Servers**.

c. Check the information provided in the External File Server Status area.

Troubleshooting Managed File Transfer

If managed file transfer fails to start or you are experiencing problems with the feature, do the following:

1. Check the Cisco XCP File Transfer Manager service logs. Go to the IM and Presence Service Command Line Interface (CLI) and enter the following command: `file view activelog epas/trace/xcp/log/AFTStartup.log`
2. If the Cisco RTMT plugin is installed, check it for traces and syslog messages.

Cisco Jabber Client Interoperability

There are a number of configuration options for file transfers. You can configure one of the following file transfer types on IM and Presence Service:

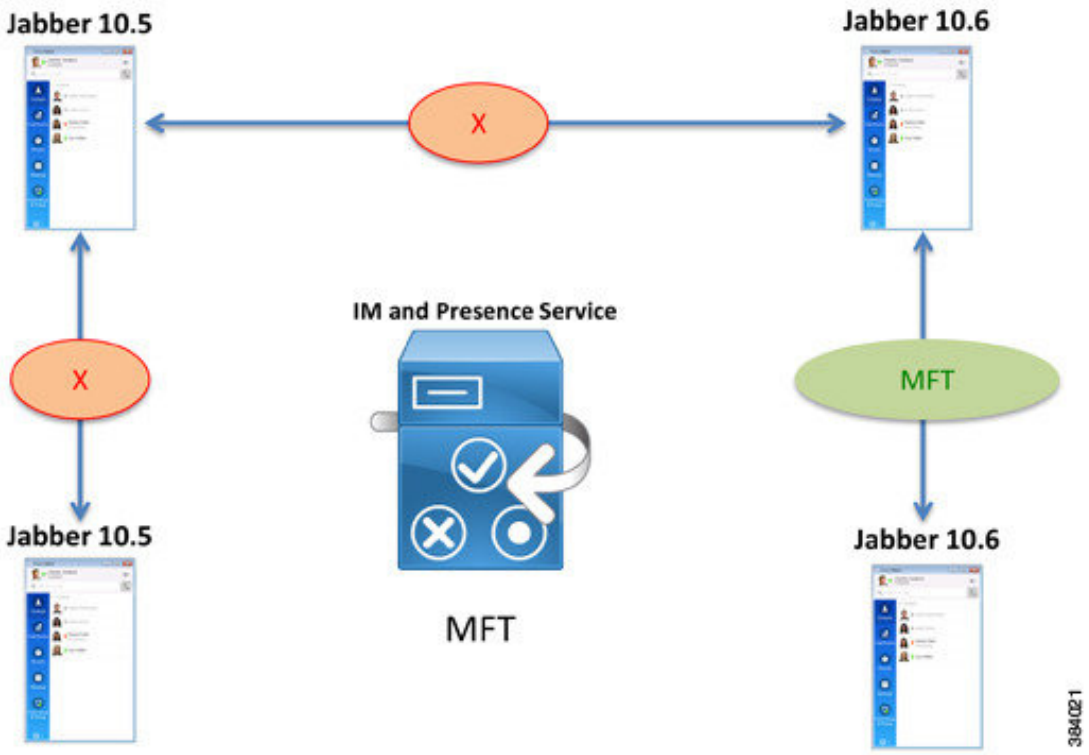
- **Disabled**—no file transfers are allowed.
- **Peer-to-Peer**—one-to-one file transfers are allowed, but files are not archived or stored on a server. Group chat file transfer is not supported.
- **Managed File Transfer**—one-to-one and group file transfers are allowed. File transfers are logged to 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.
- **Managed and Peer-to-Peer File Transfer**—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.

This section describes the file transfer functionality between Cisco Jabber pre-10.6 clients, or third party clients, and Cisco Jabber 10.6 and later clients in the following scenarios:

- Single node deployment where **Managed File Transfer** is enabled.
- Single node deployment where **Managed and Peer-to-Peer File Transfer** is enabled.
- 2-node cluster deployment, where one node has **Managed and Peer-to-Peer File Transfer** enabled and the other node has **Peer-to-Peer** enabled.
- 2-cluster deployment, where a node in one cluster has **Managed and Peer-to-Peer File Transfer** enabled and a node in the other cluster has **Peer-to-Peer** enabled (for simplicity, this scenario assumes one node per cluster).
- Group Chat in a 2-cluster deployment, where a node in one cluster has either **Managed File Transfer** or **Managed and Peer-to-Peer File Transfer**enabled and a node in the other cluster has **Peer-to-Peer** enabled (for simplicity, this scenario assumes one node per cluster).

Single Node - Managed File Transfer

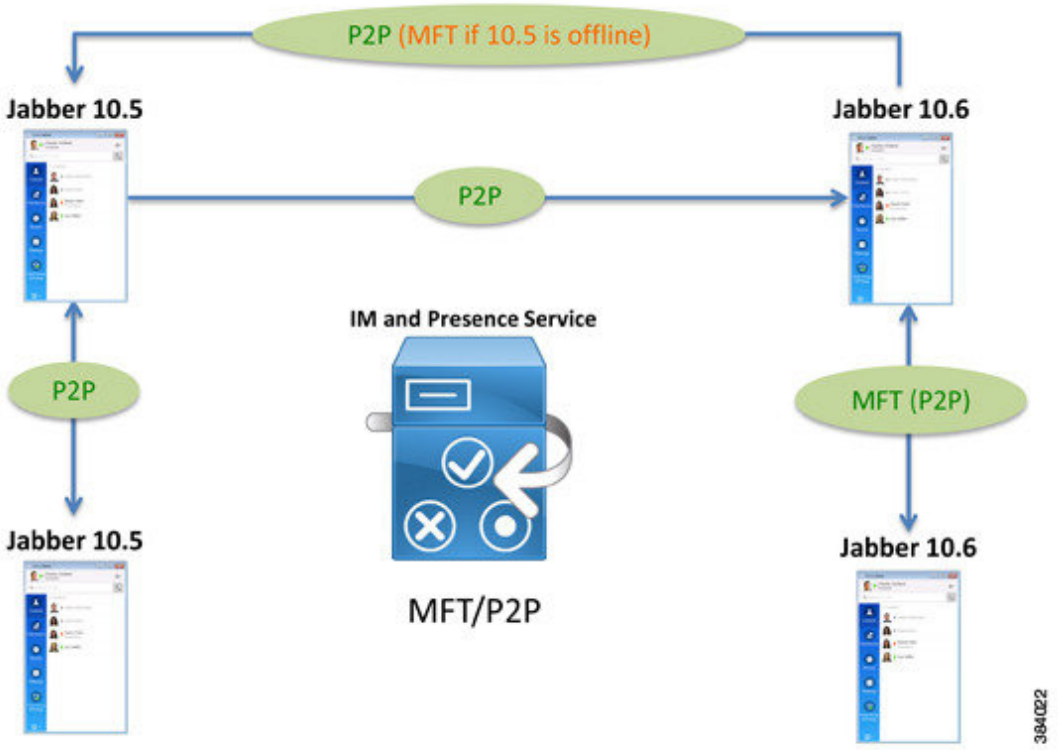
The following figure shows a single IM and Presence Service node that has **Managed File Transfer** (MFT) enabled. Cisco Jabber Release 10.5 clients and Cisco Jabber Release 10.6 clients are registered to the IM and Presence Service node.



In this deployment model, managed file transfers are only supported between Cisco Jabber Release 10.6 clients. Peer-to-peer file transfers are not allowed, regardless of the client release.

Single Node - Managed and Peer-to-Peer File Transfer

The following figure shows a single IM and Presence Service node that has **Managed and Peer-to-Peer File Transfer** (MFT/P2P) enabled. Cisco Jabber Release 10.5 clients and Cisco Jabber Release 10.6 clients are registered to the IM and Presence Service node.

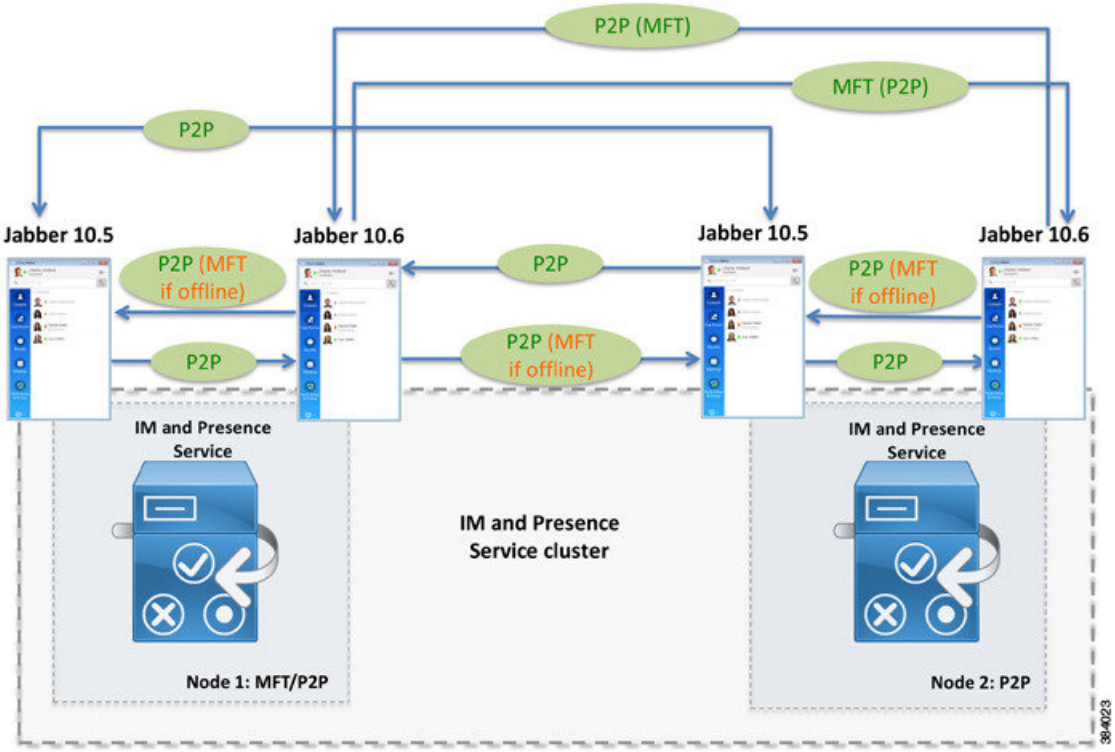


In this deployment model, file transfers are allowed and are treated as either managed file transfers or peer-to-peer file transfers depending on the client:

- File transfers between Cisco Jabber 10.5 clients are treated as peer-to-peer transfers.
- File transfers between Cisco Jabber 10.6 clients are treated as managed file transfers if the clients are configured to support managed file transfers. However, you can change the client settings to treat file transfers as peer-to-peer transfers.
- If a Cisco Jabber 10.5 client sends a file to a Cisco Jabber 10.6 client, it is treated as a peer-to-peer file transfer.
- If a Cisco Jabber 10.6 client sends a file to a Cisco Jabber 10.5 client, it is treated as a peer-to-peer file transfer if peer-to-peer is the default client preference and the Cisco Jabber 10.5 client is online. If the 10.5 client is offline, the file transfer is treated as a managed file transfer but the 10.5 client cannot receive it.

Single Cluster - Mixed Nodes

The following figure shows a cluster with two IM and Presence Service nodes. Node 1 has **Managed and Peer-to-Peer File Transfer** (MFT/P2P) enabled and Node 2 has **Peer-to-Peer** (P2P) enabled. Both nodes have Cisco Jabber Release 10.5 clients and Cisco Jabber Release 10.6 clients registered to them.



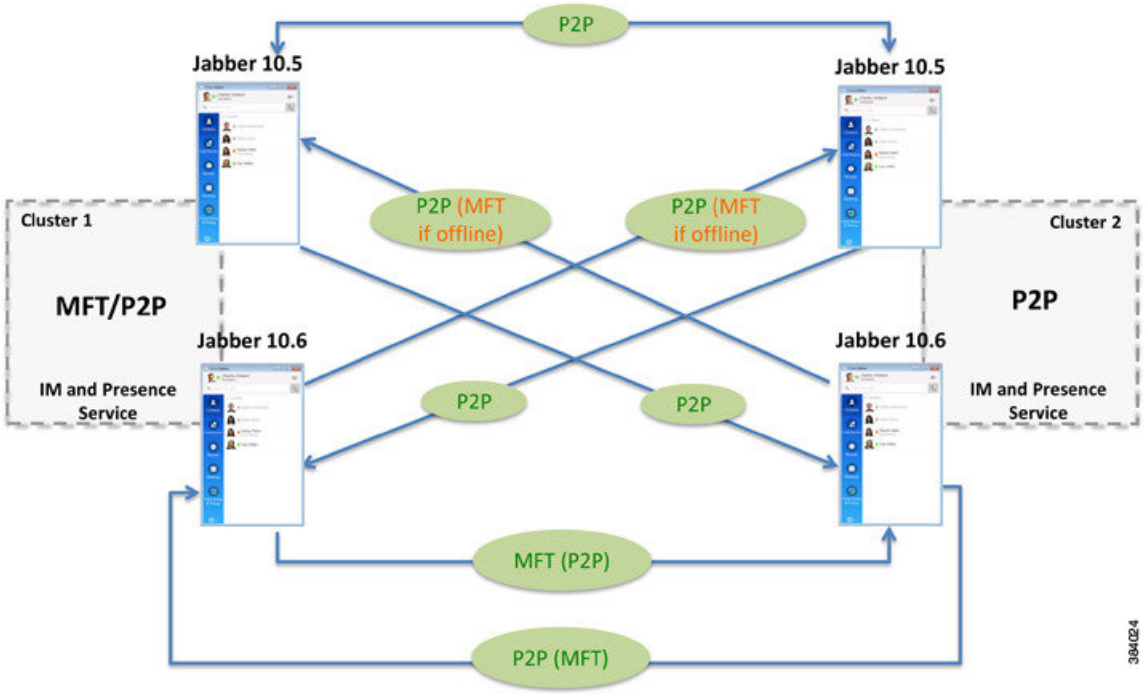
In this deployment model, file transfers are allowed and are treated as either managed file transfers or peer-to-peer file transfers depending on the client. Use the following legend to interpret the different file transfer behaviours:

- P2P—file transfers are treated as peer-to-peer file transfers.
- MFT (P2P)—managed file transfer is the default client preference. However you can reconfigure the clients to use peer-to-peer file transfers.
- P2P (MFT)—peer-to-peer is the default client preference. However, you can reconfigure the clients to use managed file transfers.
- P2P (MFT if offline)—peer-to-peer is the default client preference and the recipient is online. If the recipient is offline, it is treated as a managed file transfer by the sender but the recipient cannot receive it.

Note A node that has **Managed File Transfer** enabled should not be deployed in a cluster with a node that has **Peer-to-Peer** enabled. The recommended migration path is to configure the **Peer-to-Peer** nodes as **Managed and Peer-to-Peer File Transfer** nodes and then change them to **Managed File Transfer** nodes.

Multiple Cluster - Mixed Nodes

The following figure shows a deployment with two clusters where a node in Cluster 1 has **Managed and Peer-to-Peer File Transfer** (MFT) enabled and a node in Cluster 2 has **Peer-to-Peer** (P2P) enabled. Both nodes have Cisco Jabber Release 10.5 clients and Cisco Jabber Release 10.6 clients registered to them.

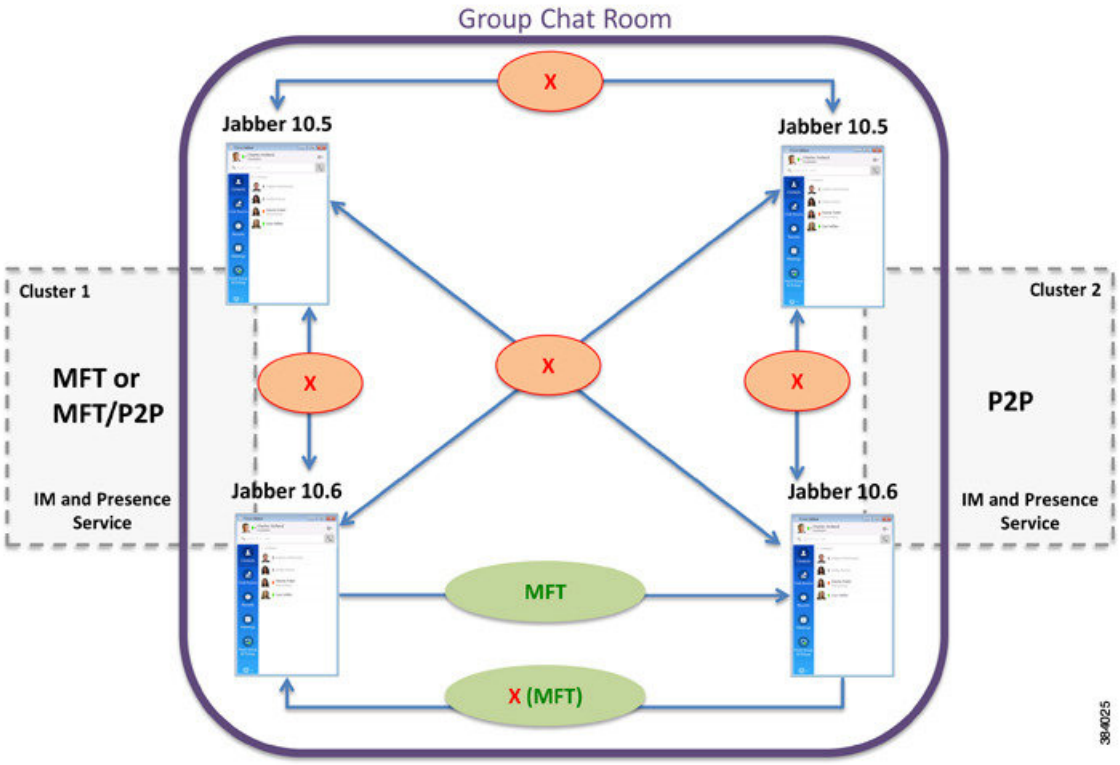


In this deployment model, file transfers are allowed and are treated as either managed file transfers or peer-to-peer file transfers depending on the client. Use the following legend to interpret the different file transfer behaviours:

- P2P—file transfers are treated as peer-to-peer file transfers.
- MFT (P2P)—managed file transfer is the default client preference. However you can reconfigure the clients to use peer-to-peer file transfers.
- P2P (MFT)—peer-to-peer is the default client preference. However, you can reconfigure the clients to use managed file transfers.
- P2P (MFT if offline)—peer-to-peer is the default client preference and the recipient is online. If the recipient is offline, it is treated as a managed file transfer by the sender but the recipient cannot receive it.

Group Chat

The following figure shows a group chat scenario between two clusters, where a node in Cluster 1 has either **Managed File Transfer** (MFT) or **Managed and Peer-to-Peer File Transfer** (MFT/P2P) enabled and a node in Cluster 2 has **Peer-to-Peer** (P2P) enabled. Both nodes have Cisco Jabber Release 10.5 clients and Cisco Jabber Release 10.6 clients registered to them.



In this scenario, managed file transfers are only supported between Cisco Jabber Release 10.6 clients. Peer-to-peer file transfers are not allowed, regardless of the client release. Use the following legend to interpret the different file transfer behaviours:

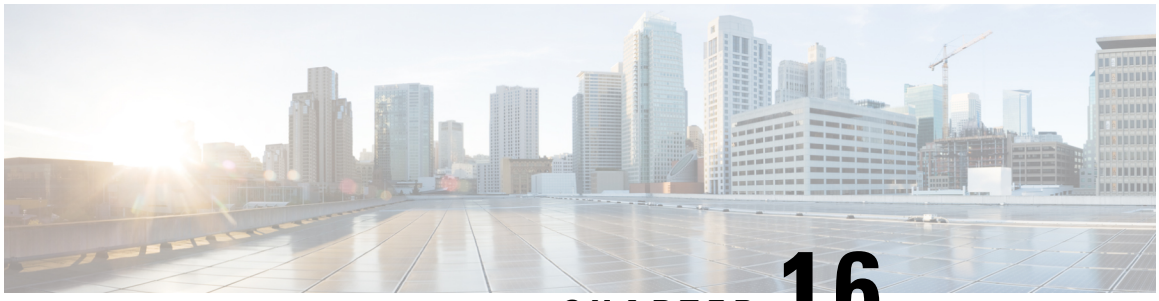
- MFT—managed file transfers are supported and the external file server of the sender's home node is used to serve the file upload and all the file downloads, regardless of which node the recipient is homed on.
- X (MFT)—the default client preference is to not allow any file transfers. However, you can reconfigure the client to support managed file transfers.

Mobile and Remote Access for Jabber Clients

For on-premise deployments, Managed File Transfer is the only supported file transfer option for Mobile and Remote Access clients. To use Managed File Transfer or MRA, you must be running a Restricted version of

the IM and Presence Service. Managed File Transfer will not work over MRA if you are running an Unrestricted version of the IM and Presence Service.

For more information about Mobile and Remote Access, see this link: http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html



CHAPTER 16

Multiple Device Messaging

Multiple Device Messaging Overview

With Multiple Device Messaging (MDM), you can have your 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, which are both 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.

For example, if you start an IM conversation on your desktop computer, you can continue the conversation on your mobile device after moving away from your desk. See Multiple Device Messaging Flow, on page 222.

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.

MDM maintains compatibility with the Cisco XCP Message Archiver service and other third-party clients which do not support MDM.

MDM is supported by all Jabber clients from version 11.7 and higher.

The following limitations apply:

- Clients must be signed-in - Signed-out clients do not display sent or received IMs or notifications.
- File transfer is only available on the active device which sent or received the file.
- Group chat is only available on the device which joined the chat room.
- MDM is not supported on clients which connect to IM and Presence Service from the cloud through Cisco Expressway, on Expressway versions prior X8.8.

For further information on how MDM operates, see the following two flows:

Multiple Device Messaging Flow

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 Flow

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.

Enable Multiple Device Messaging

Multiple Device Messaging is enabled by default. You can use this procedure to disable or enable the feature.

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 Choose Enabled or Disabled, from the **Enable Multi-Device Messaging** drop-down list.
Step 5 Click **Save**.
Step 6 Restart the Cisco XCP Router service.

Counters for Multiple Device Messaging

Multiple Device Messaging (MDM) uses the following counters from the Cisco XCP MDM Counters Group:

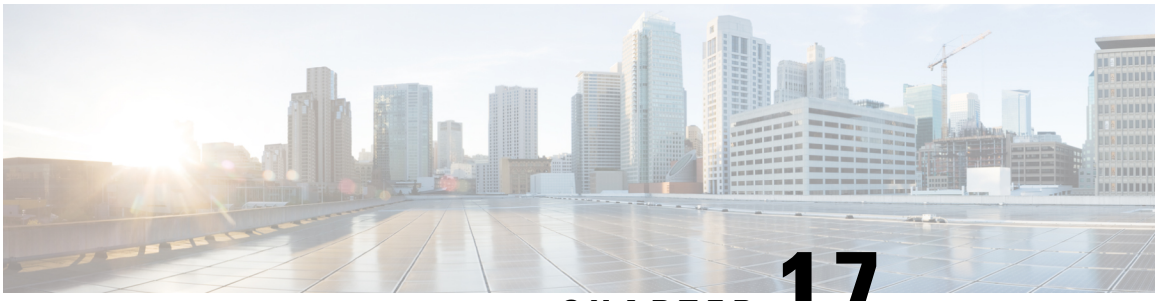
Table 26: Counter Group: Cisco XCP MDM Counters

Counter Name	Description
MDMSessions	The current number of MDM enabled sessions.
MDMSilentModeSessions	The current number of sessions in silent mode.
MDMQuietModeSessions	The current number of sessions in quiet mode.
MDMBufferFlushes	The total number of MDM buffer flushes.
MDMBufferFlushesLimitReached	The total number of MDM buffer flushes due to reaching the overall buffer size limit.

Counter Name	Description
MDMBufferFlushPacketCount	The number of packets flushed in the last timeslice.
MDMBufferAvgQueuedTime	The average time in seconds before the MDM buffer is flushed.

Multiple Device Messaging Interactions and Restrictions

Feature	Interaction
Server Recovery Manager	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.



CHAPTER 17

Configure Push Notifications

Push Notifications Overview

When your cluster is enabled for Push Notifications, and the IM and Presence Service use Google and Apple's cloud-based Push Notification service to push notifications for voice and video calls, instant message notification to Cisco Jabber or Cisco Webex on Android and iOS clients that are running in suspended mode (also known as background mode). Push Notifications allows your system to maintain a persistent communication with Cisco Jabber or Cisco Webex. Push Notifications is required both for Cisco Jabber and Cisco Webex on Android and iOS clients that connect from within the enterprise network, and for clients that register to an on-premise deployment through Expressway's Mobile and Remote Access (MRA) feature.

How Push Notifications Work

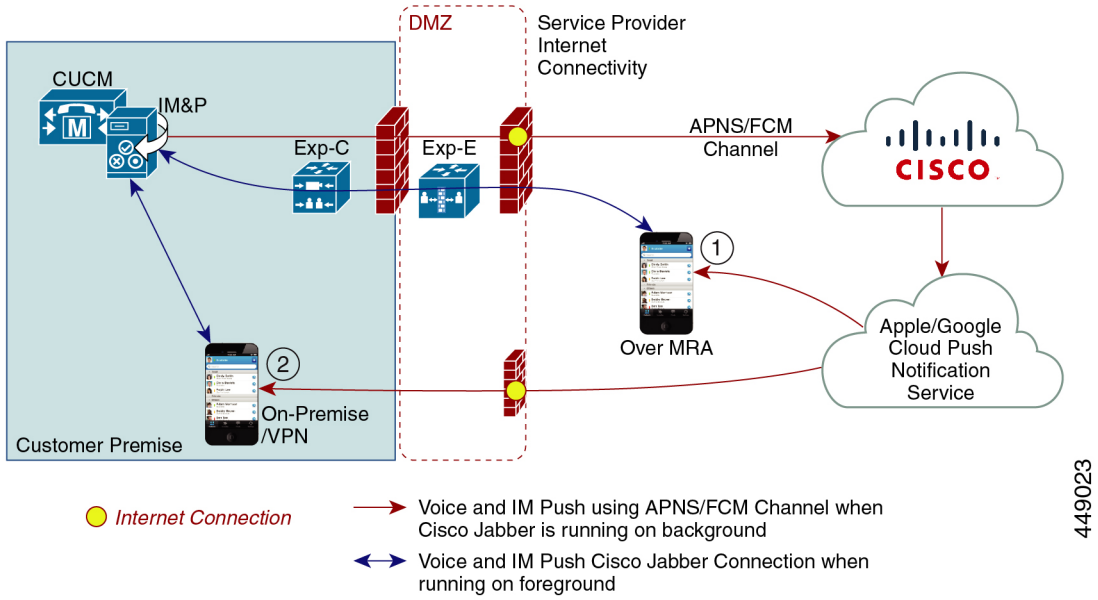
At startup, clients that are installed on Android and iOS platform devices register to , the IM and Presence Service and to the Google and Apple cloud. With MRA deployments, the clients registers to the on-premises servers through Expressway. So as long as the Cisco Jabber and Cisco Webex client remains in foreground mode, and the IM and Presence Service can send calls and instant messages to the clients directly.

However, once the Cisco Jabber or Cisco Webex clients moves to suspended mode (for example, to maintain battery life), the standard communication channel is unavailable, preventing and IM and Presence Service from communicating directly with the clients. Push Notifications provides another channel to reach the clients through the partner clouds.

Note Cisco Jabber and Cisco Webex is considered to be running in suspended mode if any of the following conditions are true:

- the Cisco Jabber or Cisco Webex application is running off-screen (in the background)
- the Android or iOS device is locked
- the Android or iOS device screen is turned off

Figure 16: Push Notifications Architecture



The above diagram displays what happens when Cisco Jabber or Cisco Webex for Android and iOS clients run in the background or are stopped. The figure illustrates: (1) an MRA deployment where the clients that connects with an on-premises Cisco Unified Communications Manager and IM and Presence Service deployment through Expressway, and (2) a Cisco Jabber or Cisco Webex for Android and iOS clients that connects directly to the on-premises deployment from within the enterprise network.

Note As of iOS13 for Apple clients and supported Android clients, voice calls and messages use separate Push Notifications channels ('VoIP' and 'Message') to reach a client that is running in background mode. However, the general flow is the same for both channels. With iOS 12, voice calls and messages are delivered using the same channel.

Push Notifications Behavior for Cisco Jabber and Cisco Webex

The following table describes the behavior under iOS 12 and iOS 13 for Cisco Jabber or Cisco Webex iOS clients that are registered to and the IM and Presence Service.

Cisco Jabber or Cisco Webex client is running in...	Cisco Jabber is running on an iOS12 Device	Cisco Jabber is running on an iOS13 Device or Android Device
Foreground Mode	**Voice and Video Calls** sends voice and video calls to Cisco Jabber or Cisco Webex clients directly using the standard SIP communications channel. For calls, also sends Push Notifications to Cisco Jabber or Cisco Webex clients that are in foreground mode. However, the standard SIP channel gets used to establish the call, rather than the Push Notifications channel. **Messages** The IM and Presence Service sends messages to the client directly using the standard SIP communication channel. For messages, Push Notifications are not sent to clients that are in foreground mode.	The behaviour is the same as with iOS12.

Cisco Jabber or Cisco Webex client is running in...	Cisco Jabber is running on an iOS12 Device	Cisco Jabber is running on an iOS13 Device or Android Device
Suspended Mode (Background mode)	**Voice or Video Calls** Standard communication channel is unavailable. Unified CM uses the Push Notifications channel. Upon receiving the notification, the Cisco Jabber or Cisco Webex client re-enters foreground mode automatically, and the client rings. **Messaging** Standard communication channel is 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 Cisco Jabber or Cisco Webex client and a notification appears on the Cisco Jabber or Cisco Webex client. 3. When the user clicks the notification, the Cisco Jabber or Cisco Webex client moves back the foreground. The Cisco Jabber or Cisco Webex client resumes the session with the IM and Presence Service and downloads the instant message. **Note** While the Cisco Jabber or Cisco Webex client is in suspended mode, the user's Presence status displays as **Away**.	With iOS13, call traffic and message traffic is split into separate Push Notifications channels: a 'VoIP' channel for calls, and a "Message" channel for messaging. **Voice or Video Calls** Standard communication channel is unavailable. Unified CM uses Push Notifications 'VoIP' channel. Upon receiving the VoIP notification, Jabber launches CallKit with Caller ID. This behavior holds for Cisco Jabber or Cisco Webex iOS clients. **Messaging** Standard communication channel is unavailable. IM and Presence Service uses Push Notifications 'Message' channel. 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 Cisco Jabber or Cisco Webex client. 3. When the user clicks the notification, Cisco Jabber or Cisco Webex client moves to foreground mode. Cisco Jabber or Cisco Webex client resumes the session with the IM and Presence Service and downloads the message. **Note** While Cisco Jabber or Cisco Webex client is in suspended mode, the user Presence displays as **Away**.

Supported Clients for Push Notifications

Client	OS	Platform Cloud	Cloud Service
Cisco Jabber on iPhone and iPad	iOS	Apple	Apple Push Notification Service (APNS)
Cisco Jabber on Android	Android	Google	Android PNS Service
Webex on iOS	iOS	Apple	Apple Push Notification Service (APNS)

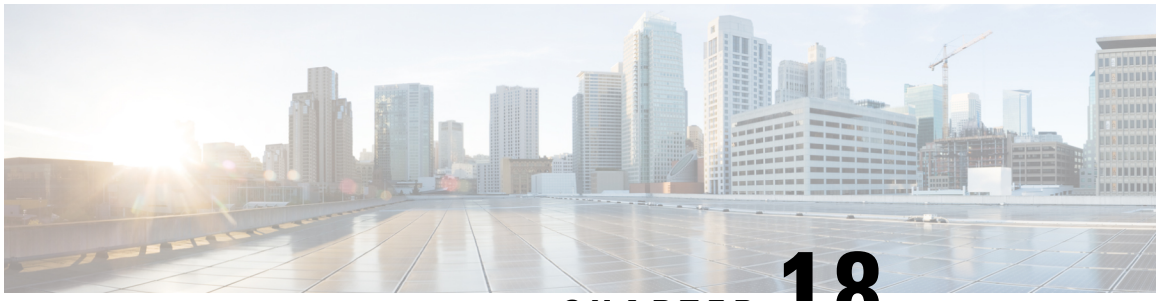
Client	OS	Platform Cloud	Cloud Service
Webex on Android	Android	Google	Android PNS Service

Push Notifications Configuration

For details on how to configure and deploy Push Notifications, refer to *Deploying Push Notifications for Cisco Jabber on iPhone and iPad* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

PART IV

Administration



CHAPTER 18

Chat Setup and Management

Chat Deployments

You can set up chat for different deployment scenarios. Sample deployment scenarios are available.

Chat Deployment Scenario 1

Deployment Scenario:	You do not want to include the Cluster ID in the chat node alias. Instead of the system-generated alias `conference-1-mycup.cisco.com`, you want to use the alias `primary-conf-server.cisco.com`.
Configuration Steps:	**1.** Choose **Messaging** > **Group Chat and Persistent Chat** to turn off the system-generated alias. (This is on by default). **2.** Edit the alias and change it to `primary-conf-server.cisco.com`.
Notes:	When you turn off the old system-generated alias, `conference-1-mycup.cisco.com` reverts to a standard, editable alias listed under Group Chat Server Aliases. This maintains the old alias and the chat room addresses associated with that alias.

Chat Deployment Scenario 2

Deployment Scenario:	You want to: • change the Domain from cisco.com to linksys.com and use conference-1-mycup.linksys.com instead of conference-1-mycup.cisco.com. • maintain the address of existing persistent chat rooms in the database so that users can still find old chat rooms of type xxx@conference-1-mycup.cisco.com.

Configuration Steps:	1. Log in to **Cisco Unified CM IM and Presence Administration**, choose **Presence** > **Settings Topology** > **Advanced Configuration**. 2. See the related topics for more information about how to edit the default IM and Presence Service domain.
Notes:	When you change the domain, the fully qualified cluster name (FQDN) automatically changes from conference-1-mycup.cisco.com to conference-1-mycup.linksys.com. The old system-generated alias conference-1-mycup.cisco.com reverts to a standard, editable alias listed under Group Chat Server Aliases. This maintains the old alias and the chat room addresses associated with that alias.

Related Topics

IM and Presence Service Default Domain Configuration

Chat Deployment Scenario 3

Deployment Scenario:	You: • want to change the Cluster ID from mycup to ireland to use conference-1-ireland.cisco.com instead of conference-1-mycup.cisco.com. • do not need to maintain the address of existing persistent chat rooms in the database.
Configuration Steps:	1. Choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Settings** > **Standard Configuration**. 2. Edit the Cluster ID and change it to ireland. 3. Choose **Messaging** > **Group Chat Server Alias Mapping**. 4. Delete the old alias conference-1-mycup.cisco.com.
Notes:	When you change the Cluster ID, the fully qualified cluster name (FQDN) automatically changes from conference-1-mycup.cisco.com to conference-1-ireland.cisco.com. The old system-generated alias conference-1-mycup.cisco.com reverts to a standard, editable alias listed under Group Chat Server Aliases. This maintains the old alias and the chat room addresses associated with that alias. Because (in this example) the Administrator has no need to maintain the old alias address, it is appropriate to delete it.

Chat Deployment Scenario 4

Deployment Scenario:	You want to: • delete a node associated with an existing alias from the System Topology, for example, conference-3-mycup.cisco.com. • add a new node with a new node ID (node id: 7) to the System Topology, for example, conference-7-mycup.cisco.com. • maintain the address of chat rooms that were created using the old alias.

Configuration Steps:	Option 1 1. Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **Group Chat Server Alias Mapping**. 2. Click **Add New** to add the additional alias, conference-3-mycup.cisco.com. Option 2 1. Choose **Messaging** > **Group Chat and Persistent Chat** and turn off the default system-generated alias, conference-7-mycup.cisco.com. (This is on by default). 2. Edit the alias and change it to conference-3-mycup.cisco.com.
Notes:	When you add the new node to the System Topology, the system automatically assigns this alias to the node: conference-7-mycup.cisco.com. Option 1 • If you add an additional alias, the node is addressable via both aliases, conference-7-mycup.cisco.com and conference-3-mycup.cisco.com. Option 2 • If you turn off the old system-generated alias, conference-7-mycup.cisco.com reverts to a standard, editable alias listed under Group Chat Server Aliases.

Chat Administration Settings

Change IM Gateway Settings

You can configure IM Gateway settings for IM and Presence Service.

The SIP-to-XMPP connection on the IM and Presence Service IM Gateway is enabled by default. This allows IM interoperability between SIP and XMPP clients so that users of SIP IM clients can exchange bi-directional IMs with users of XMPP IM clients. We recommend that you leave the IM Gateway Status parameter on; however, you can turn off the IM Gateway Status parameter to prevent XMPP and SIP clients from communicating with each other.

You can also change the default inactive timeout interval of IM conversations, as well as select the error message that gets displayed if the IM fails to get delivered.

Restriction

SIP clients cannot participate in chat rooms because this is an XMPP-specific feature.

Procedure

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

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

Step 3 Choose **Cisco SIP Proxy** as the service on the **Service Parameter Configuration** window.

Step 4 Do one of the following actions:

a) Set IM Gateway Status to **On** in the SIP XMPP IM Gateway (Clusterwide) section to enable this feature.

b) Set IM Gateway Status to **Off** in the SIP XMPP IM Gateway (Clusterwide) section to disable this feature.

Step 5 Set the Inactive Timeout interval (in seconds) of IM conversations maintained by the gateway. The default setting is 600 seconds, which is appropriate to most environments.

Step 6 Specify the error message that you want users to see if the IM fails to deliver. Default error message: Your IM could not be delivered.

Step 7 Click **Save**.

What to do next

Proceed to configure the persistent chat room settings.

Limit Number Of Sign-In Sessions

Administrators can limit the number of sign-in sessions per user on the Cisco XCP Router. This parameter is applicable to XMPP clients only.

Procedure

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

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

Step 3 Choose **Cisco XCP Router** as the service in the **Service Parameter Configuration** window.

Step 4 Enter a parameter value in the **Maximum number of logon sessions per user** in the **XCP Manager Configuration Parameters (Clusterwide)** area.

Step 5 Click **Save**.

Step 6 Restart the Cisco XCP Router Service.

Related Topics

Restart Cisco XCP Router Service, on page 78

Configure Persistent Chat Room Settings

You need only configure persistent chat settings if you use persistent chat rooms as opposed to temporary (ad-hoc) chat rooms. This configuration is specific to persistent chat and has no impact on IM archiving for regulatory compliance.

Restriction

SIP clients cannot participate in chat rooms because this is an XMPP-specific feature.

Before you begin

- To use persistent chat rooms, you must configure a unique external database instance per node.

- If you use an external database for persistent chat logging, consider the size of your database. Archiving all the messages in a chat room is optional, and will increase traffic on the node and consume space on the external database disk. In large deployments, disk space could be quickly consumed. Ensure that your database is large enough to handle the volume of information.
- Before you configure the number of connections to the external database, consider the number of IMs you are writing offline and the overall volume of traffic that results. The number of connections that you configure will allow the system to scale. While the default settings on the UI suit most installations, you may want to adapt the parameters for your specific deployment.
- The heartbeat interval is typically used to keep connections open through firewalls. Do not set the Database Connection Heartbeat Interval value to zero without contacting Cisco support.

Procedure

Step 1 Select **Cisco Unified Communications Manager IM and Presence Administration** > **Messaging** > **Group Chat and Persistent Chat**.

Step 2 Check **Enable Persistent Chat**.

Note This is a cluster-wide setting. If persistent chat is enabled on any node in the cluster, clients in any cluster will be able to discover the Text Conference instance on the node and chat rooms hosted on that node.

Users on a remote cluster can discover Text Conference instances and rooms on the local cluster even if Persistent Chat is not enabled on the remote cluster.

Step 3 (Optional) Specify how to store chat room messages, if required:

a) Check **Archive all room messages** if you want to archive all the messages that are sent in the room. This is a cluster-wide setting that applies to all persistent chat rooms.
b) Enter the number of connections to the database that you to want to use for processing requests. This is a cluster-wide setting that applies to all connections between chat nodes and associated databases.
c) Enter the number of seconds after which the database connection should refresh. This is a cluster-wide setting that applies to all connections between chat nodes and associated databases.

Step 4 Select from the list of preconfigured external databases and assign the appropriate database to the chat node.

Tip Click the hyperlink if you need to edit the chat node details in the **Cluster Topology Details** window.

Step 5 If you are deploying Cisco Jabber, leave the **Rooms are anonymous by default** and **Room owners can change whether or not rooms are anonymous** check boxes unchecked. Chat fails with Cisco Jabber if either option is selected.

Step 6 If you update any of the Persistent Chat settings, choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** to restart the Cisco XCP Text Conference Manager service.

- If you turn on the **Archive all messages in a room** setting, Cisco recommends that you monitor the performance of each external database used for persistent chat. You should anticipate an increased load on the database server(s).
- If you enable persistent chat rooms, but do not establish the correct connection with the external database, the TC service will shut down. Under these circumstances, you will lose the functionality of all chat

rooms - both temporary and persistent. If a chat node establishes a connection (even if other chat nodes fail), it will still start.

What to do next

Proceed to turn on Cisco XCP Text Conference Manager.

Related Topics

Change IM Gateway Settings, on page 235
Chat Node Alias Management, on page 241

Enable Persistent Chat

Configure persistent chat settings only if you use persistent chat rooms as opposed to temporary (ad hoc) chat rooms. This configuration is specific to persistent chat and has no impact on IM archiving for regulatory compliance.

Before you begin

- To use persistent chat rooms, you must configure a unique external database instance for each node.

Important You must have an external database assigned for each node.

- If you are using an Oracle external database, you need to update the patch for the known Oracle defect: ORA-22275. If this is not done persistent chat rooms will not work properly.
- If you use an external database for persistent chat logging, consider the size of your database. Archiving all the messages in a chat room is optional, and will increase traffic on the node and consume space on the external database disk. In large deployments, disk space could be quickly consumed. Ensure that your database is large enough to handle the volume of information.
- Archiving all room joins and leaves is optional, because it increases traffic and consumes space on the external database server.
- Before you configure the number of connections to the external database, consider the number of IMs you are writing and the overall volume of traffic that results. The number of connections that you configure will allow the system to scale. While the default settings on the UI suit most installations, you may want to adapt the parameters for your specific deployment.
- The heartbeat interval is typically used to keep connections open through firewalls. Do not set the Database Connection Heartbeat Interval value to zero without contacting Cisco support.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **Group Chat and Persistent Chat**.

Step 2 Check the check box to **Enable Persistent Chat**.

Step 3 (Optional) Check the check box **Archive all room joins and exits**, if you want to log all instances of users joining and leaving a room. This is a cluster-wide setting that applies to all persistent chat rooms.

Step 4 (Optional) Check the check box **Archive all room messages**, if you want to archive all the messages that are sent in the room. This is a cluster-wide setting that applies to all persistent chat rooms.

Step 5 (Optional) Check the check box **Allow only group chat system administrators to create persistent chat rooms**, if you want to ensure that persistent chat rooms are created only by group chat system administrators. This is a cluster-wide setting that applies to all persistent chat rooms.

To configure group chat system administrators, choose **Messaging** > **Group chat system administrators**.

Step 6 Enter the maximum number of persistent chat rooms that are allowed in the **Maximum number of persistent chat rooms allowed** field. The default value is set to 1500.

Important You must ensure that there is sufficient space on the external database. Having a large number of chat rooms impacts resources on the external database.

Step 7 Enter the number of connections to the database that you to want to use for processing requests in the **Number of connections to the database** field. The default is set to 5. This is a cluster-wide setting that applies to all connections between chat nodes and associated databases.

Step 8 Enter the number of seconds after which the database connection should refresh in the **Database connection heartbeat interval (seconds)** field. The default is set to 300. This is a cluster-wide setting that applies to all connections between chat nodes and associated databases.

Step 9 Enter the number of minutes after which the chat room should time out in the **Timeout value for persistent chat rooms (minutes)** field. The default is set to 0. The timeout is used to check whether a chat room is idle and empty. If the room is found to be idle and empty, the room is closed. With the default value set to 0, the idle check is disabled.

Step 10 Choose from the list of preconfigured external databases and assign the appropriate database to the chat node.

- If you turn on the **Archive all room joins and exits** setting, Cisco recommends that you monitor the performance of each external database that is used for persistent chat. Expect an increased load on the database servers.
- If you turn on the **Archive all room messages** setting, Cisco recommends that you monitor the performance of each external database that is used for persistent chat. Expect an increased load on the database servers.
- If you enable persistent chat rooms but do not establish the correct connection with the external database, the chat node will fail. Under these circumstances, you will lose the functionality of all chat rooms, both temporary and persistent. If a chat node establishes a connection (even if other chat nodes fail), it will still start.
- To edit the Cisco Unified Communications Manager IM and Presence Service node details in the **Cluster Topology Details** window, click the hyperlink.

Step 11 Click **Save**.

Step 12 Restart the Cisco XCP Router on all nodes in the cluster by choosing **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Network Services**.

Note the following:

- If the Cisco XCP Text Conference Manager service was already running, it will automatically restart when you restart the Cisco XCP Router.

- If the Cisco XCP Text Conference Manager service was not already running, you must start it after the Cisco XCP Router has restarted. To start the Cisco XCP Text Conference Manager service, choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services**.

Note After you have enabled persistent chat, if you subsequently want to update any of the persistent chat settings, only the following non-dynamic settings require a Cisco XCP Text Conference Manager restart:

- Number of connections to the database
- Database connection heartbeart interval (seconds)

Related Topics

Restart Cisco XCP Text Conference Manager Service

Configure Group Chat System Administration

Procedure

Step 1 Choose **Messaging** > **Group Chat System Administrators**.

Step 2 Check **Enable Group Chat System Administrators**.

You must restart the Cisco XCP Router when the setting is enabled or disabled. Once the System Administrator setting is enabled, you can add system administrators dynamically.

Step 3 Click **Add New**.

Step 4 Enter an IM address.

Example:

The IM address must be in the format of name@domain .

Step 5 Enter a nickname.

Step 6 Enter a description.

Step 7 Click **Save**.

Group Chat and Persistent Chat Default Settings Configuration and Reversion

You can change the default enhanced ad hoc and persistent chat settings. To revert all settings back to their default values, click **Set to Default**.

Note To allow chat room owners to change a setting, check the **Room owners can change** check box on the node. The room owner can then configure such settings as they wish and those settings are applicable to the room they are creating. The availability of configuring these settings from the client also depends on the client implementation and whether the client is providing an interface in which to configure these settings.

Chat Node Alias Management

Chat Node Aliases

Aliases create a unique address for each chat node so that users (in any domain) can search for specific chat rooms on specific nodes, and join chat in those rooms. Each chat node in a system must have a unique alias.

Note This chat node alias, `conference-3-mycup.cisco.com`, for example, will form part of the unique ID for each chat room created on that node, `roomjid@conference-3-mycup`.cisco.com

You can assign your aliases cluster-wide, in these ways:

- System-generated - allows the system to automatically assign a unique alias to each chat node.You do not have do to anything further to address your chat node if you enable the system-generated aliases. The system will auto-generate one alias per chat node by default using the following naming convention: `conference-x-clusterid.domain`, where:
  - conference - is a hardcoded keyword
  - x- is the unique integer value that denotes the node ID
  - Example: `conference-3-mycup.cisco.com`
- Manually - You may choose to override the default system-generated alias if the `conference-x-clusterid.domain` naming convention does not suit your customer deployment, for example, if you do not want to include the Cluster ID in your chat node alias. With manually-managed aliases, you have complete flexibility to name chat nodes using aliases that suit your specific requirements.
- Additional Aliases - You can associate more than one alias with each chat node on a per-node basis. Multiple aliases per node allows users to create additional chat rooms using these aliases. This applies whether you assign a system-generated alias or manage your aliases manually.

Key Considerations

Changing chat node aliases can make the chat rooms in the database unaddressable and prevent your users from finding existing chat rooms.

Note these results before you change the constituent parts of aliases or other node dependencies:

- Cluster ID - This value is part of the fully qualified cluster name (FQDN). Changing the Cluster ID (choose **System** > **Presence Topology: Settings**) causes the FQDN to incorporate the new value and

the system-managed alias to automatically change across the cluster. For manually-managed aliases, it is the responsibility of the Administrator to manually update the alias list if the Cluster ID changes.

- Domain - This value is part of the FQDN. Changing the Domain (choose **Presence** > **Presence Settings**) causes the FQDN to incorporate the new value and the system-managed alias to automatically change across the cluster. For manually-managed aliases, it is the responsibility of the Administrator to manually update the alias list if the Domain changes.
- Connection between the chat node and external database - The chat node will not start if persistent chat is enabled and you do not maintain the correct connection with the external database.
- Deletion of a chat node — If you delete a node associated with an existing alias from the Presence Topology, chat rooms created using the old alias may not be addressable unless you take further action.
- To ensure that the user has access to all the old chat rooms, take a backup of all the existing aliases before deleting a node and assign the same alias to a new node.

We recommend that you do not change existing aliases without considering the wider implications of your changes, namely:

- Make sure that you maintain the address of old chat nodes in the database so that users can locate existing chat rooms via the old alias, if required
- If there is federation with external domains, you may need to publish the aliases in DNS to inform the users in those domains that the aliases have changed and new addresses are available. This depends on whether or not you want to advertise all aliases externally.

Related Topics

Chat Deployment Scenario 1, on page 233

Turn On or Off System-Generated Chat Node Aliases

Chat node aliases allow users in any domain to search for specific chat rooms on specific nodes, and join in those chat rooms. IM and Presence Service automatically assign a unique, system-generated alias to each chat node by default. No further configuration is needed to address your chat node when system-generated aliases are used. The system automatically generates one alias per chat node using the default naming convention `conference-x-clusterid.domain`.

If you want to manually assign chat node aliases, you must turn off the default system-generated alias setting. If you turn off a system-generated alias, the existing alias (`conference-x-clusterid.domain`) reverts to a standard, editable alias listed under Conference Server Aliases. See topics related to manually managed chat node aliases for more information. For best practice guidelines, see the sample chat deployment scenarios

Before you begin

- Review the topics about chat node aliases and key considerations.
- You cannot edit or delete a system-generated alias, for example, `conference-3-mycup.cisco.com`.

Procedure

Step 1 Log in to **Cisco Unified CM IM and Presence Administration**, choose **Messaging** > **Group Chat and Persistent Chat**.

Step 2 Enable or disable system-generated aliases:

a) To enable the system to automatically assign chat room aliases to nodes using the naming convention `conference-x-clusterid.domain`, check **System Automatically Manages Primary Group Chat Server Aliases**

Tip Choose **Messaging** > **Group Chat Server Alias Mapping** to verify that the system-generated alias is listed under Primary Group Chat Server Aliases.

b) To disable system-generated aliases, uncheck **System Automatically Manages Primary Group Chat Server Aliases**.

What to do next

- Even if you configure a system-generated alias for a chat node, you can associate more than one alias with the node if required.
- If you are federating with external domains, you may want to inform federated parties that the aliases have changed and new aliases are available. To advertise all aliases externally, configure DNS and publish the aliases as DNS records.
- If you update any of the system-generated alias configuration, perform one of these actions:
- Restart the Cisco XCP Text Conference Manager. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** to restart this service

Related Topics

Chat Deployment Scenario 1, on page 233
Configure Persistent Chat Room Settings, on page 236

Manage Chat Node Aliases Manually

You can manually add, edit, or delete chat node aliases. To manually manage chat node aliases, you must turn off the default setting, which uses system-generated aliases. If you turn off a system-generated alias, the existing alias (**conference-x-clusterid.domain**) reverts to a standard, editable alias listed under Conference Server Aliases. This maintains the old alias and the chat room addresses associated with that alias.

You can manually assign multiple aliases to chat nodes. Even if a system-generated alias already exists for a chat node, you can associate additional aliases to the node manually.

For manually-managed aliases, it is the responsibility of the administrator to manually update the alias list if the Cluster ID or domain changes. System-generated aliases will incorporate the changed values automatically.

Note Although it is not mandatory, we recommend that you always include the domain when you assign a new chat node alias to a node. Use this convention for additional aliases, newalias.domain. Choose **Presence Settings** > **Advanced Settings** in **Cisco Unified CM IM and Presence Administration** to see the domain.

Before you begin

Review topics related to chat node aliases and key considerations.

Procedure

Step 1 Log in to **Cisco Unified CM IM and Presence Administration**, choose **Messaging** > **Group Chat and Persistent Chat**.

Step 2 Uncheck **System Automatically Manages Primary Group Chat Server Aliases**.

Step 3 All the existing chat node aliases are listed together under Group Chat Server Aliases. To view the alias list, perform these actions:

a) Choose **Messaging** > **Group Chat Server Alias Mapping**.
b) Click **Find**.

Step 4 Complete one or more of the following actions as required:

Edit an existing alias (old system-generated or user-defined alias)

a) Click the hyperlink for any existing alias that you want to edit.
b) Edit the alias for the node in the Group Chat Server Alias field. Make sure the alias is unique for the node.
c) Choose the appropriate node to which you want to assign this changed alias.

Add a new chat node alias

a) Click **Add New**.
b) Enter a unique alias for the node in the Group Chat Server Alias field.
c) Choose the appropriate node to which you want to assign the new alias.

Delete an existing alias

a) Check the check box for the alias that you want to delete.
b) Click **Delete Selected**.

Troubleshooting Tips

- Every chat node alias must be unique. The system will prevent you from creating duplicate chat node aliases across the cluster.
- A chat node alias name cannot match the IM and Presence domain name.
- Delete old aliases only if you no longer need to maintain the address of chat rooms via the old alias.
- If you are federating with external domains, you may want to inform federated parties that the aliases have changed and new aliases are available. To advertise all aliases externally, configure DNS and publish the aliases as DNS records.
- If you update any of the chat node alias configuration, restart the Cisco XCP Text Conference Manager.

What to do next

- Proceed to turn on the Cisco XCP Text Conference Manager.

Related Topics

Chat Deployments, on page 233

Turn on Cisco XCP Text Conference Manager

This procedure applies if you configure the persistent chat room settings, or manually add one or more aliases to a chat node. You must also turn on this service if you want to enable ad hoc chat on a node.

Before you begin

If persistent chat is enabled, an external database must be associated with the Text Conference Manager service, and the database must be active and reachable or the Text Conference Manager will not start. If the connection with the external database fails after the Text Conference Manager service has started, the Text Conference Manager service will remain active and functional, however, messages will no longer be written to the database and new persistent rooms cannot be created until the connection recovers.

Procedure

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

Step 2 Choose the node from the Server drop-down list and click **Go**.

Step 3 Click the radio button next to the Cisco XCP Text Conference Manager service in the IM and Presence Service section to turn it on or click **Restart** to restart the service.

Step 4 Click **OK** when a message indicates that restarting may take a while.

Step 5 (Optional) Click **Refresh** if you want to verify that the service has fully restarted.

Related Topics

Configure Persistent Chat Room Settings, on page 236

Chat Room Management

Set Number of Chat Rooms

Use room settings to limit the number of rooms that users can create. Limiting the number of chat rooms will help the performance of the system and allow it to scale. Limiting the number of rooms can also help mitigate any possible service-level attacks.

Procedure

Step 1 To change the maximum number of chat rooms that are allowed, enter a value in the field for **Maximum number of rooms allowed**. The default is set to 5500.

Step 2 Click **Save**.

Configure Member Settings

Member settings allow system-level control over the membership in chat rooms. Such a control is useful for users to mitigate service-level attacks that can be prevented by administrative actions such as banning. Configure the member settings as required.

Procedure

Step 1 Check **Rooms are for members only by default** if you want rooms to be created as members-only rooms by default. Members-only rooms are accessible only by users on a white list configured by the room owner or administrator. The checkbox is unchecked by default.

Note The white list contains the list of members who are allowed in the room. It is created by the owner or administrator of the members-only room.

Step 2 Check **Room owners can change whether or not rooms are for members only** if you want to configure the room so that room owners are allowed to change whether or not rooms are for members only. The check box is checked by default.

Note A room owner is the user who creates the room or a user who has been designated by the room creator or owner as someone with owner status (if allowed). A room owner is allowed to change the room configuration and destroy the room, in addition to all other administrator abilities.

Step 3 Check **Only moderators can invite people to members-only rooms** if you want to configure the room so that only moderators are allowed to invite users to the room. If this check box is unchecked, members can invite other users to join the room. The check box is checked by default.

Step 4 Check **Room owners can change whether or not only moderators can invite people to members-only rooms** if you want to configure the room so that room owners can allow members to invite other users to the room. The check box is checked by default.

Step 5 Check **Users can add themselves to rooms as members** if you want to configure the room so that any user can request to join the room at any time. If this check box is checked, the room has an open membership. The check box is unchecked by default.

Step 6 Check **Room owners can change whether users can add themselves to rooms as members** if you want to configure the room so that room owners have the ability to change the setting that is listed in Step 5 at any time. The check box is unchecked by default.

Step 7 Click **Save**.

Configure Availability Settings

Availability settings determine the visibility of a user within a room.

Procedure

Step 1 Check **Members and administrators who are not in a room are still visible in the room** if you want to keep users on the room roster even if they are currently offline. The check box is checked by default.

Step 2 Check **Room owners can change whether members and administrators who are not in a room are still visible in the room** if you want to allow room owners the ability to change the visibility of a member or administrator. The check box is checked by default.

Step 3 Check **Rooms are backwards-compatible with older clients** if you want the service to function well with older Group Chat 1.0 clients. The check box is unchecked by default.

Step 4 Check **Room owners can change whether rooms are backwards-compatible with older clients** if you want to allow room owners the ability to control backward compatibility of the chat rooms. The check box is unchecked by default.

Step 5 Check **Rooms are anonymous by default** if you want the room to display the user nickname but keep the Jabber ID private. The check box is unchecked by default.

Step 6 Check **Room owners can change whether or not rooms are anonymous** if you want to allow room owners to control the anonymity level of the user Jabber ID. The check box is unchecked by default.

Step 7 Click **Save**.

Configure Invite Settings

Invite settings determine who can invite users to a room based on the user's role. Roles exist in a moderator-to-visitor hierarchy so, for instance, a participant can do anything a visitor can do, and a moderator can do anything a participant can do.

Procedure

Step 1 From the drop-down list for **Lowest participation level a user can have to invite others to the room**, choose one:

- **Visitor** allows visitors, participants, and moderators the ability to invite other users to the room.
- **Participant** allows participants and moderators the ability to invite other users to the room. This is the default setting.
- **Moderator** allows only moderators the ability to invite other users to the room.

Step 2 Check **Room owners can change the lowest participation level a user can have to invite others to the room** to allow room owners to change the settings for the lowest participation level that is allowed to send invitations. The check box is unchecked by default.

Step 3 Click **Save**.

Configure Occupancy Settings

Procedure

Step 1 To change the system maximum number of users that are allowed in a room, enter a value in the field for **How many users can be in a room at one time**. The default value is set to 1000.

Note The total number of users in a room should not exceed the value that you set. The total number of users in a room includes both normal users and hidden users.

Step 2 To change the number of hidden users that are allowed in a room, enter a value in the field for **How many hidden users can be in a room at one time**. Hidden users are not visible to others, cannot send a message to the room, and do not send presence updates. Hidden users can see all messages in the room and receive presence updates from others. The default value is 1000.

Step 3 To change the default maximum number of users that are allowed in a room, enter a value in the field for **Default maximum occupancy for a room**. The default value is set to 50 and cannot be any higher than the value that is set in Step 1.

Step 4 Check **Room owners can change default maximum occupancy for a room** if you want to allow room owners to change the default maximum room occupancy. The check box is checked by default.

Step 5 Click **Save**.

Configure Chat Message Settings

Use Chat Message settings to give privileges to users based on their role. For the most part, roles exist in a visitor-to-moderator hierarchy. For example, a participant can do anything a visitor can do, and a moderator can do anything a participant can do.

Procedure

Step 1 From the drop-down list for **Lowest participation level a user can have to send a private message from within the room**, choose one:

- **Visitor** allows visitors, participants, and moderators to send a private message to other users in the room. This is the default setting.
- **Participant** allows participants and moderators to send a private message to other users in the room.
- **Moderator** allows only moderators to send a private message to other users in the room.

Step 2 Check **Room owners can change the lowest participation level a user can have to send a private message from within the room** if you want to allow room owners to change the minimum participation level for private messages. The check box is checked by default.

Step 3 From the drop-down list for **Lowest participation level a user can have to change a room's subject**, choose one:

a) **Participant** allows participants and moderators to change the room's subject. This is the default setting.
b) **Moderator** allows only moderators to change the room's subject.

Visitors are not permitted to change the room subject.

Step 4 Check **Room owners can change the lowest participation level a user can have to change a room's subject** if you want to allow room owners to change the minimum participation level for updating a room's subject. The check box is checked by default.

Step 5 Check **Remove all XHTML formatting from messages** if you want to remove all Extensible Hypertext Markup Language (XHTML) from messages. The check box is unchecked by default.

Step 6 Check **Room owners can change XHTML formatting setting** if you want to allow room owners to change the XHTML formatting setting. The check box is unchecked by default.

Step 7 Click **Save**.

Configure Moderated Room Settings

Moderated rooms provide the ability for moderators to grant and revoke the voice privilege within a room (in the context of Group Chat, voice refers to the ability to send chat messages to the room). Visitors cannot send instant messages in moderated rooms.

Procedure

Step 1 Check **Rooms are moderated by default** if you want to enforce the role of moderator in a room. The check box is unchecked by default.

Step 2 Check **Room owners can change whether rooms are moderated by default** if you want to allow room owners the ability to change whether rooms are moderated. The check box is checked by default.

Step 3 Click **Save**.

Configure History Settings

Use History settings to set the default and maximum values of messages that are retrieved and displayed in the rooms, and to control the number of messages that can be retrieved through a history query. When a user joins a room, the user is sent the message history of the room. History settings determine the number of previous messages that the user receives.

Procedure

Step 1 To change the maximum number of messages that users can retrieve from the archive, enter a value in the field for **Maximum number of messages that can be retrieved from the archive**. The default value is set to 100. It serves as a limit for the next setting.

Step 2 To change the number of previous messages displayed when a user joins a chat room, enter a value in the field for **Number of messages in chat history displayed by default**. The default value is set to 15 and cannot be any higher than the value that is set in Step 1.

Step 3 Check **Room owners can change the number of messages displayed in chat history** if you want to allow room owners to change the number of previous messages displayed when a user joins a chat room. The check box is unchecked by default.

Step 4 Click **Save**.

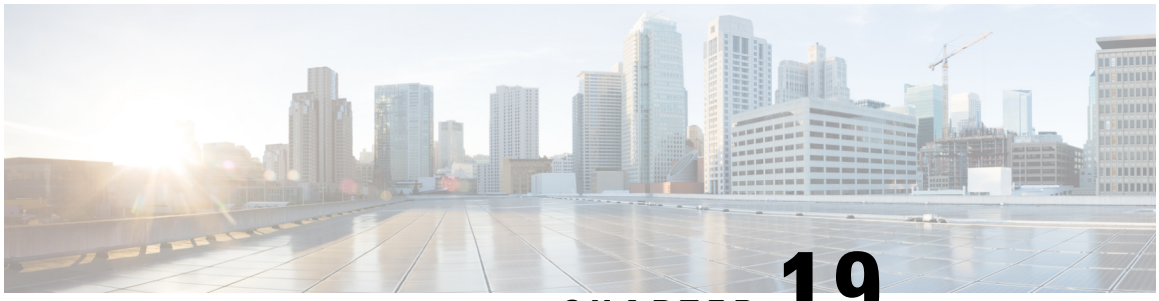
Group Chat and Persistent Chat Interactions and Restrictions

Table 27: Group Chat and Persistent Chat Interactions and Restrictions

Feature Interaction	Restriction
Archiving room joins	Archiving room joins and leaves is optional because it will increase traffic and consume space on the external database server.
Chat with anonymous rooms	If you are deploying chat via Cisco Jabber (either group chat or persistent chat), make sure that the **Rooms are anonymous by default** and **Room owners can change whether or not rooms are anonymous** options are not selected in the **Group Chat and Persistent Chat Settings** window. If either check box is checked, chat will fail
Database Connection Issues	If the connection with the external database fails after the Text Conference Manager service has started, the Text Conference Manager service will remain active and functional, however, messages will no longer be written to the database and new persistent rooms cannot be created until the connection recovers.
OVA Requirements	If you are deploying Persistent Chat or Intercluster Peering, the minimum OVA size that you can deploy for these features is the 5000 user OVA. It's recommended that you deploy at least the 15,000 user OVA. Centralized Deployments may require the 25,000 user OVA, depending on the size of the user base. For additional details on OVA options and user capacities, refer to the following site: **Note** It's strongly recommended to deploy at least the 15,000 user OVA on all IMP nodes. https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html
Persistent chat character limit with Microsoft SQL Server	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.

Feature Interaction	Restriction
Persistent Chat for Jabber Mobile where a peer cluster is running a non-supported release	Persistent chat for Jabber mobile is introduced with 11.5(1)SU5 and is not supported on earlier 11.5(1)SU releases. This feature is also not supported for 12.0(1) or 12.0(1)SU1. If you have Persistent Chat for Jabber mobile deployed in this release, and you also have intercluster peering set up with peer clusters that do not support persistent chat rooms for Jabber Mobile, the following conditions apply for Jabber mobile clients: If the persistent chat room is hosted on a non-supported release, such as 11.5(1): • A Jabber mobile client that is homed from the supported cluster can join persistent chat rooms hosted on the non-supported cluster, but will have no option to mute the room. They will see a Global Mute option, but it will not work. • A Jabber mobile client that is homed on the non-supported peer cluster will be unable to join any persistent chat rooms. If the persistent chat room is hosted on a supported release, such as 11.5(1)SU5: • A Jabber mobile client participant that is homed on the supported cluster will have all persistent chat on mobile functionality. • A Jabber mobile client from a non-supported peer cluster will be unable to join persistent chat rooms. **Note** The search feature for Persistent Chat does not work when the Jabber Configuration file *(jabber-config.xml)* is set to disable the IM History.
External Database connectivity and Cisco XCP Text Conferencing service	In a split-brain scenario, When the subscriber or publisher detects its peer Text Conferencing service or any node is down, then the subscriber or publisher attempts a transition from normal to backup. During this operation if loading of the peer's chat rooms fails to connect to external database, then the Cisco XCP Text Conferencing service will shutdown.

Feature Interaction	Restriction
Number of Persistent chat rooms supported if High Availability is configured	The maximum number of Persistent Chat Rooms supported on an IM&P deployment is 5000 per subcluster. If High Availability is enabled, it is recommended to create a maximum of 2500 rooms per node. (though the system allows to create upto maximum of 5000 rooms per node). If more than 2500 rooms are configured per node in a High Availability deployment, then during failover, there would be more than 5000 rooms hosted on the backup node. This might result in unexpected performance issues depending on the traffic load. The load of 5000 rooms on the system also depends on the number of participants in the room, the rate of message exchange in the rooms and the size of messages. Use Cisco Collaboration Sizing tool to ensure you have the right OVA setup for your Persistent Chat Deployment. For Information on Collaboration Sizing tool, Please refer: https://cucst.cloudapps.cisco.com/landing It is recommended to have your rooms balanced equally among both the nodes in a subcluster. And if you have more than one subcluster in a IM&P Cluster, it is recommended to also load balance the rooms across all the subclusters. Currently IM&P doesn't have a mechanism to automatically load balance the rooms. The responsibility of load balancing the room lies with the users creating the rooms. During room creation, users have to ensure that they use the jabber feature to automatically select a random node for a room creation.
Making ad hoc chat rooms private	Ad hoc chat rooms are public by default, but can be configured to be for members only with the following configuration: 1. From Cisco Unified CM IM and Presence Administration, choose **Messaging** > **Group Chat and Persistent Chat**. 2. Check the **Rooms are for members only by default** check box. 3. Uncheck the **Room owners can change whether or not rooms are for members onl**y check box. 4. Uncheck the **Only moderators can invite people to members-only rooms** check box. 5. Click **Save**. 6. Restart the Cisco XCP Text Conference service.



CHAPTER 19

End User Setup and Handling

End User Setup and Handling on IM and Presence Service

You can setup the authorization policy for IM and Presence Service end users, perform bulk user contact list imports and exports, as well as manage duplicate and invalid end user instances.

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

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

Authorization Policy Setup On IM and Presence Service

Automatic Authorization On IM and Presence Service

IM and Presence Service authorizes all presence subscription requests that it receives from SIP-based clients in the local enterprise. A local user running a SIP-based client automatically receives the availability status for contacts in the local enterprise, without being prompted to authorize these subscriptions on the client. IM and Presence Service only prompts the user to authorize the subscription of a contact in the local enterprise if the contact is on the blocked list for the user. This is the default authorization behavior for SIP-based clients on IM and Presence Service, and you cannot configure this behavior.

In the XMPP network, it is standard behavior for the node to send all presence subscriptions to the client, and the client prompts the user to authorize or reject the subscription. To allow enterprises to deploy IM and Presence Service with a mix of SIP-based and XMPP-based clients (to align the authorization policy for both client types), Cisco provides the following automatic authorization setting on IM and Presence Service:

- When you turn on automatic authorization, IM and Presence Service automatically authorizes all presence subscription requests it receives from both XMPP-based clients and SIP-based in the local enterprise. This is the default setting on IM and Presence Service.
- When you turn off automatic authorization, IM and Presence Service only supports XMPP-based clients. For XMPP-based clients, IM and Presence Service sends all presence subscriptions to the client, and the client prompts the user to authorize or reject the presence subscription. SIP-based clients will not operate correctly on IM and Presence when you turn off automatic authorization.

Caution If you turn off automatic authorization, SIP-based clients are not supported. Only XMPP-based clients are supported when you turn off automatic authorization.

User Policy and Automatic Authorization

In addition to reading the automatic authorization policy, IM and Presence Service reads the policy settings for the user to determine how to handle presence subscription requests. Users configure the policy settings from the Cisco Jabber client. A user policy contains the following configuration options:

- Blocked list - a list of local and external (federated) users that will always see the availability status of the user as unavailable regardless of the true status of the user. The user can also block a whole federated domain.
- Allowed list - a list of local and external users that the user has approved to see their availability. The user can also allow a whole external (federated) domain.
- Default policy - the default policy settings for the user. The user can set the policy to block all users, or allow all users.

Note that if you turn off automatic authorization, IM and Presence Service automatically authorizes subscription requests a user that is on the contact list of another user. This applies to users in the same domain, and users in different domains (federated users). For example:

- UserA wishes to subscribe the view the availability status of UserB. Automatic authorization is off on IM and Presence Service, and UserB is not in the Allowed or Blocked list for the UserA.
- IM and Presence Service sends the presence subscription request to the client application of UserB, and the client application prompts userB to accept or reject the subscription.
- UserB accepts the presence subscription request, and UserB is added to the contact list of UserA.
- UserA is then automatically added to the contact list for UserB without being prompted to authorize the presence subscription.

IM and Presence Service will automatically add UserA to the contact list of UserB even if the policy for UserB (i) blocks the external domain, or (ii) the default policy for the user is block all, or (iii) “ask me” is chosen.

If you deploy interdomain federation between a local IM and Presence Service enterprise and a supported external enterprise, IM and Presence Service does not apply the automatic authorization setting to presence subscription requests received from external contacts, unless the user has applied a policy on that external contact or domain. On receipt of a presence subscription request from an external contact, IM and Presence Service will only send the subscription request to the client application if the user chooses “ask me” to be prompted to set their own Allow/Block policy for external contacts, and if the external contact or domain is not in either the Allowed or Blocked list for the user. The client application prompts the user to authorize or reject the subscription.

Note IM and Presence Service uses common user policies for both availability and instant messages.

Related Topics

http://www.cisco.com/en/US/products/ps6837/products_user_guide_list.html
IM and Presence Service Configuration Guides

Configure Authorization Policy on IM and Presence Service

You can turn on automatic authorization so that IM and Presence Service automatically authorizes all presence subscription requests it receives from both XMPP-based clients and SIP-based in the local enterprise. If you turn off automatic authorization, IM and Presence Service only supports XMPP-based clients and sends all presence subscriptions to the client where the user is prompted to authorize or reject the presence subscription.

Tip See the Online Help topic in the Cisco Unified CM IM and Presence Administration interface for a definition of all the parameters on this window.

Procedure

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

Step 2 Configure the authorization policy. Perform one of the following actions:

- To turn on automatic authorization, check **Allow users to view the availability of other users without being prompted for approval**.
- To turn off automatic authorization, uncheck **Allow users to view the availability of other users without being prompted for approval.**.

Step 3 Click **Save**.

Step 4 Restart the Cisco XCP Router service.

What to do next

Proceed to configure the SIP publish trunk on IM and Presence Service.

Related Topics

Restart Cisco XCP Router Service, on page 78

IM Setup On IM and Presence Service, on page 164

Bulk Rename User Contact IDs

The IM and Presence Service Bulk Assignment Tool allows you to rename the contact ID (JID) in user contact lists from one format to another. For example, you can rename a user's contact ID from firstname.lastname@domain.com to userid@domain.com and the Bulk Administration Tool will update each user's contact list with the new contact ID.

Caution Bulk rename of contact IDs is used in the migration of users from a Microsoft server (for example Lync) to IM and Presence Service Service. See the *Partitioned Intradomain Federation Guide* on Cisco.com for detailed instructions of how this tool should be used as part of the user migration process. Using this tool in any other circumstances is not supported.

Before you can run this job, you must upload a file containing a list of contact IDs and the corresponding new format of each of those contact IDs. The file must be a CSV file with the following format:

`<Contact ID>, <New Contact ID>`

where **`<Contact ID>`** is the existing contact ID and **`<New Contact ID>`** is the new format of the contact ID.

From Release 10.0 the **`<Contact ID>`** is the user's IM address as it appears on the **Presence Topology User Assignment window**.

The following is a sample CSV file with one entry:

```
Contact ID, New Contact ID
john.smith@example.com, jsmith@example.com
```

Complete the following procedure to upload the CSV file and rename the contact IDs for a list of users.

Procedure

Step 1 Upload the CSV file with the list of contact IDs that you want to rename in all contact lists. Do the following:

a) On the IM and Presence database publisher node, choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Upload/Download Files**.
b) Click **Add New**.
c) Click **Browse** to locate and choose the CSV file.
d) Choose **Contacts** as the Target.
e) Choose **Rename Contacts – Custom File** as the Transaction Type.
f) Click **Save** to upload the file.

Step 2 On the publisher node, choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Contact List** > **Rename Contacts**.

Step 3 In the **File Name** field, choose the file that you uploaded.

Step 4 Choose one of the following actions:

- Click **Run Immediately** to execute the Bulk Administration job immediately.

- Click **Run Later** to schedule a time to execute the Bulk Administration job. For more information about scheduling jobs in the Bulk Administration Tool, see the Online Help in Cisco Unified CM IM and Presence Administration.

Step 5 Click **Submit**. If you chose to run the job immediately, the job runs after you click Submit.

Bulk Export User Contact Lists

The IM and Presence Service Bulk Administration Tool (BAT) allows you to export the contact lists of users who belong to a particular node or presence redundancy group to a CSV data file. You can then use BAT to import the user contact lists to another node or presence redundancy group in a different cluster. The BAT user contact list export and import features facilitate the moving of users between clusters. See topics related to bulk imports of user contact lists for more information.

From IM and Presence Service Release 11.5(0), you can also export non-presence contact lists. For further information, see Bulk Export Non-Presence Contact Lists, on page 258

Note Users on contact lists who do not have an IM address, will not be exported.

BAT allows you to find and choose the users whose contact lists you want to export. The user contact lists are exported to a CSV file with the following format:

```
<User ID>,<User Domain>,<Contact ID>,<Contact Domain>,<Nickname>,<Group Name>
```

The following table describes the parameters in the export file.

Parameter	Description
User ID	The user ID of the IM and Presence Service user. **Note** This value is the user portion of the user's IM address.
User Domain	The Presence domain of the IM and Presence Service user. **Note** This value is the domain portion of the user's IM address. **Example 1:** bjones@example.com—bjones is the user ID and example.com is the user domain. **Example 2:** bjones@usa@example.com—bjones@usa is the user ID and example.com is the user domain.
Contact ID	The user ID of the contact list entry.
Contact Domain	The Presence domain of the contact list entry.
Nickname	The nickname of the contact list entry. If the user has not specified a nickname for a contact, the Nickname parameter will be blank.

Parameter	Description
Group Name	The name of the group to which the contact list entry is to be added. If a user's contacts are not sorted into groups, the default group name will be specified in the Group Name field.

The following is a sample CSV file entry:

```
userA,example.com,userB,example.com,buddyB,General
```

Complete the following procedure to export user contact lists with BAT and download the export file.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Contact List** > **Export**.

Step 2 Use the selection criteria to find the users whose contact lists you want to export. See the Online Help topic in the Cisco Unified CM IM and Presence Administration interface for more information about finding and selecting users.

Step 3 Click **Next**.

Step 4 In the **File Name** field, enter a name for the CSV file.

Step 5 Choose one of the following:

- Click **Run Immediately** to execute the Bulk Administration job immediately.
- Click **Run Later** to schedule a time to execute the Bulk Administration job. For more information about scheduling jobs in BAT, see the Online Help in Cisco Unified CM IM and Presence Administration.

Step 6 Click **Submit**. If you chose to run the job immediately, the job runs after you click Submit.

Step 7 To download the export file after the job has run, choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Upload/Download Files**.

Step 8 Find and choose the export file that you want to download.

Step 9 Click **Download Selected**.

Bulk Export Non-Presence Contact Lists

With the BAT, you can also export all local cluster user's non-presence contact lists to a CSV data file. Non-presence contacts are contacts who do not have a IM address and can only be exported using this procedure.

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:

Parameter	Description
User JID	The User JID. This is the IM address of the user.

Parameter	Description
Contact JID	The User JID of the contact list entry, if available, otherwise it is the UUID.
Group Name	The name of the group to which the contact list entry is to be added.
Content Type	The text mime type and subtype used in the info field.
Version	The content type used in the info field.
Info	The contact information of the contact list entry in vCard format.

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
```

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Contact** > **Export Non-presence Contact List**.

Step 2 In the **File Name** field, enter a name for the CSV file.

Step 3 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 4 Click **Submit**. If you chose to run the job immediately, the job runs after you click Submit.

Step 5 To download the export file after the job has run, choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Upload/Download Files**.

Step 6 Find and choose the export file that you want to download.

Step 7 Click **Download Selected**.

Bulk Import Of User Contact Lists

You can use the IM and Presence Service Bulk Assignment Tool (BAT) to import user contact lists into IM and Presence Service. With this tool, you can prepopulate contact lists for new IM and Presence Service client users or add to existing contact lists. To import user contact lists, you must provide BAT with an input file that contains the user contact lists.

The input file must be a CSV file in the following format:

```
<User ID>,<User Domain>,<Contact ID>,<Contact Domain>,<Nickname>,<Group Name>
```

The following is a sample CSV file entry:

```
userA,example.com,userB,example.com,buddyB,General
```

The following table describes the parameters in the input file.

Table 28: Description of Input File Parameters

Parameter	Description
User ID	This is a mandatory parameter. The user ID of the IM and Presence Service user. It can have a maximum 132 characters. **Note** This value is the user portion of the user's IM address.
User Domain	This is a mandatory parameter. The Presence domain of the IM and Presence Service user. It can have a maximum of 128 characters. **Note** This value is the domain portion of the user's IM address. **Example 1:** `bjones@example.com`—bjones is the user ID and example.com is the user domain. **Example 2:** `bjones@usa@example.com`—bjones@usa is the user ID and example.com is the user domain.
Contact ID	This is a mandatory parameter. The user ID of the contact list entry. It can have a maximum of 132 characters.
Contact Domain	This is a mandatory parameter. The Presence domain of the contact list entry. The following restrictions apply to the format of the domain name: • Length must be less than or equal to 128 characters • Contains only numbers, upper- and lowercase letters, and hyphens (-) • Must not start or end with hyphen (-) • Length of label must be less than or equal to 63 characters • Top-level domain must be characters only and have at least two characters

Parameter	Description
Nickname	The nickname of the contact list entry. It can have a maximum of 255 characters.
Group Name	This is a mandatory parameter. The name of the group to which the contact list entry is to be added. It can have a maximum of 255 characters.

Note If you are moving users to another node or presence redundancy group in a different cluster, you can use BAT to generate the CSV file for chosen users. See topics related to bulk exports of user contact lists for more information.

Complete the following steps to import user contact lists into IM and Presence Service:

- Check the maximum contact list size.
- Upload the input file using BAT.
- Create a new bulk administration job.
- Check the results of the bulk administration job.

Before You Begin

Before you import the user contact lists, you must complete the following:

1. Provision the users on Cisco Unified Communications Manager.
2. Ensure that the users are licensed on Cisco Unified Communications Manager for the IM and Presence Service.

Note The default contact list import rate is based on the virtual machine deployment hardware type. You can change the contact list import rate by choosing **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters** > **Cisco Bulk Provisioning Service**. However, if you increase the default import rate, this will result in higher CPU and memory usage on IM and Presence Service.

Check Maximum Contact List Size

Before you import contact lists to IM and Presence Service, check the Maximum Contact List Size and Maximum Watchers settings. The system default value is 200 for Maximum Contact List Size and 200 for Maximum Watchers.

Cisco recommends that you set the Maximum Contact List Size and Maximum Watchers settings to Unlimited while importing user contact lists to IM and Presence Service. This ensures that each migrated user contact list is fully imported. After all users have migrated, you can reset the Maximum Contact List Size and Maximum Watchers settings to the preferred values.

Note It is possible to exceed the maximum contact list size without losing data when importing contact lists using BAT; however, Cisco recommends temporarily increasing the Maximum Contact List Size setting or setting the value to Unlimited for the import. You can reset the maximum value after the import is complete.

You only need to check the maximum contact list size on those clusters that contain users for whom you wish to import contacts. When you change Presence settings, the changes are applied to all nodes in the cluster; therefore you only need to change these settings on the IM and Presence database publisher node within the cluster.

What To Do Next

Upload the input file using BAT.

Related Topics

Configure Maximum Contact List Size Per User, on page 162
Configure Maximum Number of Watchers Per User, on page 163

Upload Input File Using BAT

The following procedure describes how to upload the CSV file using BAT.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Upload/Download Files**.

Step 2 Click **Add New**.

Step 3 Click **Browse** to locate and choose the CSV file.

Step 4 Choose **Contact Lists** as the Target.

Step 5 Choose **Import Users' Contacts – Custom File** as the Transaction Type.

Step 6 Click **Save** to upload the file.

What to do next

Create a new bulk administration job.

Create New Bulk Administration Job

The following procedure describes how to create a new bulk administration job in Cisco Unified CM IM and Presence Administration.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Contact List** > **Update**.

Step 2 From the File Name drop-down list, choose the file to import.

Step 3 In the Job Description field, enter a description for this Bulk Administration job.

Step 4 Choose one of the following:

- Click **Run Immediately** to execute the Bulk Administration job immediately.
- Click **Run Later** to schedule a time to execute the Bulk Administration job. For more information about scheduling jobs in BAT, see the Online Help in Cisco Unified CM IM and Presence Administration.

Step 5 Click **Submit**. If you chose to run the job immediately, the job runs after you click Submit.

What to do next

Check the results of the bulk administration job.

Check Results of Bulk Administration Job

When the Bulk Administration job is complete, the IM and Presence Service BAT tool writes the results of the contact list import job to a log file. The log file contains the following information:

- The number of contacts that were successfully imported.
- The number of internal server errors that were encountered while trying to import the contacts.
- The number of contacts that were not imported (ignored). The log file lists a reason for each ignored contact at the end of the log file. The following are the reasons for not importing a contact:
  - Invalid format - invalid row format, for example, a required field is missing or empty
  - Invalid contact domain - the contact domain is in an invalid format. See topics related to bulk import of user contact lists for the valid format of the contact domain
  - Cannot add self as a contact - you cannot import a contact for a user if the contact is the user
  - User’s contact list is over limit - the user has reached the maximum contact list size and no more contacts can be imported for that user
  - User is not assigned to local node - the user is not assigned to the local node
- The number of contacts in the CSV file that were unprocessed due to an error that caused the BAT job to finish early. This error rarely occurs.

Complete the following procedure to access this log file.

Procedure

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Job Scheduler**.

Step 2 Click **Find** and choose the job ID of the contact list import job.

Step 3 Click the **Log File Name** link to open the log.

Bulk Import of User Non-Presence Contact Lists

You can use the IM and Presence Service Bulk Assignment Tool (BAT) to import user none-presence contact lists into IM and Presence Service. With this tool, you can prepopulate contact lists for new IM and Presence Service client users or add to existing non-presence contact lists. To import user non-presence contact lists, you must provide BAT with an input file that contains the user contact lists.

The input file must be a CSV file in the following format:

```
<User 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:test;user;;; 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 29: Description of Input File Parameters for Non-Presence Contact Lists

Parameter	Description
User JID	The User JID. This is the IM address of the user.
Contact JID	The User JID of the contact list entry, if available, otherwise it is the UUID.
Group Name	The name of the group to which the contact list entry is to be added.
Content Type	The text mime type and subtype used in the info field.
Version	The content type used in the info field.
Info	The contact information of the contact list entry in vCard format.

Note If you are moving users to another node or presence redundancy group in a different cluster, you can use BAT to generate the CSV file for chosen users. See topics related to bulk exports of user contact lists for more information.

Complete the following steps to import user contacts lists into IM and Presence Service:

- Upload the non-presence contacts list input file using BAT. See Upload Non-Presence Contacts Input File using BAT, on page 265
- Create a new bulk administration job for non-presence contact lists. See Create New Bulk Administration Job for Non-presence Contact Lists, on page 265
- Check the results of the bulk administration job. See Check Results of Bulk Administration Job, on page 263

Upload Non-Presence Contacts Input File using BAT

The following procedure describes how to upload the CSV file using BAT for Non-Presence Contacts.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Upload/Download Files**.

Step 2 Click **Add New**.

Step 3 Click **Browse** to locate and choose the CSV file.

Step 4 Choose **Non-presence Contact Lists** as the Target.

Step 5 Choose **Import Users' Non Presence Contacts** as the Transaction Type.

Step 6 Click **Save** to upload the file.

Create New Bulk Administration Job for Non-presence Contact Lists

The following procedure describes how to create a new bulk administration job in Cisco Unified CM IM and Presence Administration.

Procedure

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

Duplicate User ID and Directory URI Management

The Cisco IM and Presence Data Monitor service checks for duplicate user IDs and empty or duplicate directory URIs across all IM and Presence Service intercluster nodes. If any errors are detected, IM and Presence Service raises an alarm in the software. Cisco recommends that you take immediate action to remedy these errors to avoid communications disruptions for these users.

You can monitor the status of duplicate user IDs and directory URI checks from the System Troubleshooter using Cisco Unified CM IM and Presence Administration GUI. You can also set the time interval for user ID and directory URI checks using the GUI.

To gather specific information about which users caused these alarms, use the Command Line Interface. Use the Real-Time Monitoring Tool to monitor system alarms and alerts.

For more information about using the command line interface to validate user IDs or directory URIs, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*. For information about using the Real-Time Monitoring Tool, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

User ID and Directory URI Monitoring

The Cisco IM and Presence Data Monitor service checks the Active directory entries for duplicate user IDs and empty or duplicate directory URIs for all IM and Presence Service intercluster nodes. Duplicate user IDs or directory URIs are not possible within a cluster; however, it is possible to unintentionally assign the same user ID or directory URI value to users on different clusters in an intercluster deployment.

You can use the System Troubleshooter in Cisco Unified CM IM and Presence Administration GUI to monitor the status of duplicate user IDs and directory URI checks. The time interval for these user ID and directory URI checks are set using Cisco Unified CM IM and Presence Administration GUI. The valid range is from 5 minutes to 1440 minutes (12 hours). The default is 30 minutes.

If errors are detected, IM and Presence Service raises an alarm in the software.

DuplicateDirectoryURI
: This alert indicates that there are multiple users within the intercluster deployment that are assigned the same directory URI value when the Directory URI IM Address scheme is configured.

DuplicateDirectoryURIWarning
: This warning indicates that there are multiple users within the intercluster deployment that are assigned the same directory URI value when the *userID@Default_Domain* IM Address scheme is configured.

DuplicateUserid
: This alert indicates there are duplicate user IDs assigned to one or more users on different clusters within the intercluster deployment.

InvalidDirectoryURI
: This alert indicates that one or more users within the intercluster deployment are assigned an empty or invalid directory URI value when the Directory URI IM Address scheme is configured.

InvalidDirectoryURIWarning

This warning indicates that one or more users within the intercluster deployment are assigned an empty or invalid directory URI value when the *userID@Default_Domain* IM Address scheme is configured.

To gather specific information about which users have these alarm conditions, use the Command Line Interface for a complete listing. System alarms do not provide details about the affected users and the System Troubleshooter displays details for only up to 10 users. Use the Command Line Interface and validate users to gather information about which users caused an alarm. For more information, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Caution Take the appropriate action to fix duplicate user IDs and duplicate or invalid Directory URIs to avoid communications disruptions for the affected users. To modify user contact information, see the *Cisco Unified Communications Manager Administration Guide*.

User ID and Directory URI Error Conditions

The following table describes user ID and directory URI error conditions that can occur when a system check for duplicate user IDs and duplicate or invalid directory URIs is performed on an intercluster deployment. The alarms that are raised are listed, as well as suggested actions to take to correct the error.

Table 30: User ID and Directory URI Error Conditions

Error Condition	Description	Suggested Action
Duplicate user IDs	Duplicate user IDs are assigned to one or more users on different clusters within the intercluster deployment. The affected users may be homed on an intercluster peer. **Related alarms**: `DuplicateUserid`	If the `DuplicateUserid` alert is raised, take immediate action to correct the issue. Each user within the intercluster deployment must have a unique user ID.
Duplicate directory URIs	Multiple users within the intercluster deployment are assigned the same directory URI value. The affected users may be homed on an intercluster peer. **Related alarms**: • `DuplicateUserid` • `DuplicateDirectoryURIWarning`	If your system is configured to use the Directory URI IM address scheme and the `DuplicateDirectoryURI` alert is raised, take immediate action to correct the issue. Each user must be assigned a unique directory URI. If your system is configured to use the *userID@Default_Domain* IM address scheme and duplicate directory URIs are detected, the `DuplicateDirectoryURIWarning` warning is raised and no immediate action is required; however, Cisco recommends that you resolve the issue.

Error Condition	Description	Suggested Action
Invalid directory URIs	One or more users within the deployment are assigned an invalid or empty directory URI value. A URI that is not in the user@domain format is an invalid Directory URI. The affected users may be homed on an intercluster peer. **Related alarms**: • `InvalidDirectoryURI` • `InvalidDirectoryURIWarning`	If your system is configured to use the Directory URI IM address scheme and the following alert is raised, take immediate action to correct the issue:`InvalidDirectoryURI`. If your system is configured to use the *userID@Default_Domain* IM address scheme and invalid directory URIs are detected, the `InvalidDirectoryURIWarning` warning is raised and no immediate action is required; however, Cisco recommends that you resolve the issue.

User ID and Directory URI Validation and Modification

Cisco recommends that you perform a check for duplicate user information rather than wait for alarms to be raised in the system, especially after adding new users or when migrating contact lists.

You can use the System Troubleshooter in the Cisco Unified CM IM and Presence Administration GUI to view a summary of user ID and Directory URI errors. For a more detailed and comprehensive report, use the CLI command to validate IM and Presence Service users.

If any users are identified as having duplicate or invalid information, you can modify the user records in Cisco Unified Communications Manager using the **End User Configuration** window, (**User Management** > **EndUser**). Ensure that all users have a valid user ID or Directory URI value as necessary. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

User ID and Directory URI CLI Validation Examples

The CLI command to validate IM and Presence Service users to identify users that have duplicate user IDs and duplicate or invalid Directory URIs is **utils users validate { all | userid | uri }**.

The Directory URI must be unique for each user. You cannot use the same Directory URI for multiple users, irrespective of it being case-sensitive. For example, you cannot have two different Directory URI such as `aaa@bbb.ccc` and `AAA@BBB.CCC`, though they are case-sensitive.

For more information about using the CLI and command descriptions, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

CLI Example Output Showing User ID Errors

```
Users with Duplicate User IDs
---------------------------------------------
 User ID: user3
  Node Name
  cucm-imp-1
  cucm-imp-2
```

CLI Example Output Showing Directory URI Errors

```
Users with No Directory URI Configured
------------------------------------------------------
 Node Name: cucm-imp-2
 User ID
 user4

Users with Invalid Directory URI Configured
------------------------------------------------------
 Node Name: cucm-imp-2
 User ID   Directory URI
 user1     asdf@ASDF@asdf@ADSF@cisco

Users with Duplicate Directory URIs
------------------------------------------------------
Directory URI: user1@cisco.com
 Node Name   User ID
 cucm-imp-1  user4
 cucm-imp-2  user3
```

Set User Check Interval

Use Cisco Unified CM IM and Presence Administration to set the time interval for the Cisco IM and Presence Data Monitor service to check all nodes and clusters in your deployment for duplicate user IDs and directory URIs.

Enter the time interval in minutes using integers. The valid range is from 5 to 1440. The default is 30 minutes.

Procedure

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

Step 2 Choose **Cisco IM and Presence Data Monitor** in the **Service** field.

Step 3 Enter an integer from 5 through 1440 as the **User Check Interval** and click **Save**.

Validate User IDs and Directory URIs Using System Troubleshooter

Use the System Troubleshooter in the Cisco Unified CM IM and Presence Administration GUI to view the status of the system checks which identify duplicate user IDs and duplicate or invalid directory URIs across all nodes and clusters in the deployment.

For a more detailed and comprehensive report, use the CLI command to validate IM and Presence Service users. For more information about using the CLI and command details, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter**.

Step 2 Monitor the status of user IDs and Directory URIs in the **User Troubleshooter** area.

The **Problem** column is populated if the system check detects any issues.

- Verify all users have a unique User ID configured.
- Verify all users have a Directory URI configured.
- Verify all users have a unique Directory URI configured.
- Verify all users have a valid Directory URI configured.
- Verify all users have a unique Mail ID configured.

Note Duplicate mail IDs impact both Email Address for Federation and Exchange Calendar integration features.

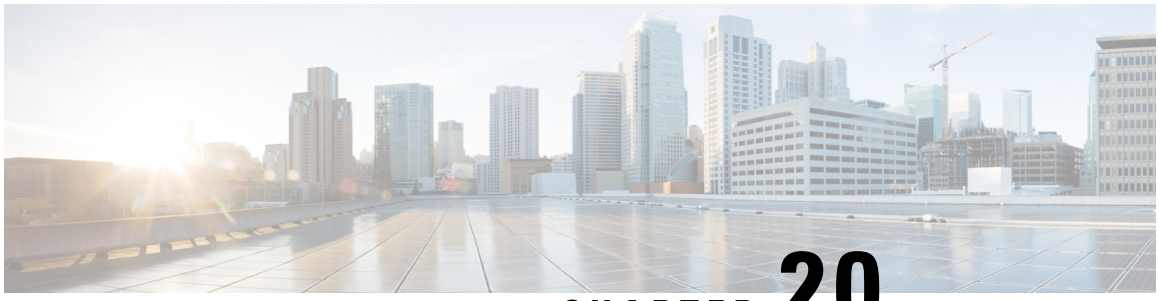
If duplicate or invalid user information is detected, perform the recommended solution. To troubleshoot UserID and directory URI errors, see topics related to troubleshooting.

Tip Clicking the **fix** link in the **Solution** column redirects you to the **End User Configuration** window in Cisco Unified Communications Manager Administration where you can locate and reconfigure user profiles. For detailed user validation information, use the CLI command to validate users.

Note The user ID and directory URI fields in the user profile may be mapped to the LDAP Directory. In that case, apply the fix in the LDAP Directory server.

Related Topics

Received Duplicate UserID Error, on page 317
Received Duplicate or Invalid Directory URI Error, on page 318



CHAPTER 20

User Migration

User Migration Between IM and Presence Service Clusters

This section describes how to migrate users between IM and Presence Service clusters. You must complete the following procedures in the order in which they are presented:

1. Before migrating users, remove all stale rosters, group entries and non-presence contract records..
2. Export the contact lists of the migrating users from their current home cluster.
3. Disable the migrating users for IM and Presence Service and Cisco Jabber on their current home cluster from Cisco Unified Communications Manager.
4. If LDAP Sync is enabled on Cisco Unified Communications Manager:
   - move the users to the new Organization Unit, from which their new cluster synchronizes its information
   - synchronize the users to the new home Cisco Unified Communications Manager.
5. If LDAP Sync is not enabled on Cisco Unified Communications Manager, manually provision the migrating users on Cisco Unified Communications Manager.
6. Enable users for IM and Presence Service and Cisco Jabber.
7. Import contact lists to the new home cluster to restore contact list data for migrated users.

Before You Begin

Complete the following tasks:

- Perform a full DRS of the current cluster and the new home cluster. See the *Disaster Recovery System Administration Guide* for more information.
- Ensure that the following services are running:
  - Cisco Intercluster Sync Agent
  - Cisco AXL Web Service
  - Cisco Sync Agent

- Run the Troubleshooter and ensure that there are no Intercluster Sync Agent issues reported. All Intercluster Sync Agent issues reported on the Troubleshooter must be resolved before proceeding with this procedure.
- Cisco recommends that the **Allow users to view the availability of other users without being prompted for approval** setting is enabled. To enable this setting, choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Settings**. Any change to this setting requires a restart of the Cisco XCP Router.
- Cisco recommends that the following settings are set to **No Limit**:
  - Maximum Contact List Size (per user)
  - Maximum Watchers (per user)

  To configure these settings, choose **Cisco Unified CM IM and Presence Administration** > **Presence** > **Settings**.
- Ensure that the users to be migrated are licensed for Cisco Unified Presence or Cisco Jabber on their current (pre-migration) home cluster only. If these users are licensed on any other cluster, they need to be fully unlicensed before proceeding with the following procedures.

Remove Stale Entries

Before migrating users, remove stale rosters, group entries and non-presence contact records. This is to be done on the publisher IM&P node from which the users had presence disabled.

Note Repeat these steps as necessary in batches of 2000. If it is too time consuming to remove a large amount of stale entries via CLI, open a TAC case to leverage the stale roster script at the end of this section that requires root access.

Procedure

Step 1 Start the CLI session. For details on how to start a CLI session, refer to the "Start CLI session" section of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

Step 2 Check and remove stale roster entries. To do this, run the following queries:

a) Check for stale roster entries:

```
run sql select count(*) from rosters where user_id in (select xcp_user_id from enduser
where primarynodeid is NULL)
```

b) Remove stale roster entries:

```
run sql delete from rosters where pkid in (select * from (select first 2000 pkid from
rosters where user_id in (select xcp_user_id from enduser where primarynodeid is NULL)))
```

Step 3 Check and remove stale group records. To do this, run the following queries:

a) Check for stale group records:

```
run sql select count(*) from groups where user_id in (select xcp_user_id from enduser
where primarynodeid is NULL)
```

b) Remove stale group records:

```
run sql delete from groups where pkid in (select * from (select first 2000 pkid from
groups where user_id in (select xcp_user_id from enduser where primarynodeid is NULL)))
```

Step 4 Check and remove stale non-contact records (in order). To do this, run the following queries:

a) Check for stale non-contact records (in order):

```
run sql select count(*) from nonpresencecontacts where fkenduser in (select pkid from
enduser where primarynodeid is null)
```

b) Remove stale non-contact records (in order):

```
run sql delete from nonpresencecontacts where pkid in (select * from (select first 2000
 pkid from nonpresencecontacts where fkenduser in (select pkid from enduser where
primarynodeid is null)))
```

c) Use this query if you have root access:

```
run sql delete from epascontactaddinfo where pkid in (select * from (select first 2000
pkid from epascontactaddinfo where pkid not in (select fkepascontactaddinfo from
nonpresencecontacts)))
```

Export User Contact Lists

Complete this procedure to export the contact lists of the migrating from their current cluster.

Procedure

Step 1 Export the contact lists of the migrating users from the current home cluster.

a) Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Contact List** > **Export**.
b) Choose **All unassigned users in the cluster** and click **Find.**
c) Review the results and use the **AND/OR** filter to filter the search results as required.
d) When the list is complete, click **Next.**
e) Choose a filename for the exported contact list data.
f) Optionally update the Job Description.
g) Click **Run Now** or schedule the job to run later.

Step 2 Monitor the status of the contact list export job.

a) Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Job Scheduler**.
b) Click **Find** to list all BAT jobs.
c) Find your contact list export job and when it is reported as completed, choose the job.
d) Choose the CSV File Name link to view the contents of the contact list export file. Note that a timestamp is appended to the filename.
e) From the **Job Results** section, choose the log file to see a summary of what was uploaded. The job begin and end time is listed and a result summary for the job is presented.

Step 3 Download the contact list export file and store it for use later when the user migration is complete.

a) Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Upload/Download Files**.

b) Click **Find.**
c) Choose the contact list export file and click **Download Selected**.
d) Save the CSV file locally for upload later in the procedure.

What to do next

Proceed to unlicense the users.

Disable Users for IM and Presence Service

The following procedure describes how to disable a migrating user for IM and Presence Service and Cisco Jabber on their current home cluster.

For information about how to update users in bulk, see the *Cisco Unified Communications Manager Bulk Administration Guide*.

Procedure

Step 1 Choose **Cisco Unified CM Administration** > **User Management** > **End User**.
Step 2 Use the filters to find the user that you want to disable for IM and Presence Service.
Step 3 In the **End User Configuration** screen, uncheck **Enable User for Unified CM IM and Presence**.
Step 4 Click **Save**.

Move Users to New Cluster

The procedure to move the users to the new cluster differs depending on whether LDAP Sync is enabled on Cisco Unified Communications Manager.

LDAP Sync Enabled on Cisco Unified Communications Manager

If LDAP Sync is enabled on Cisco Unified Communications Manager, you must move users to the new Organizational Unit and synchronize the users to the new home cluster.

Move Users To New Organizational Unit

If LDAP Sync is enabled on Cisco Unified Communications Manager, you must move the users to the new Organizational Unit (OU) from which their new cluster synchronizes if the deployment uses a separate LDAP structure (OU divided) for each cluster, where users are only synchronized from LDAP to their home cluster.

Note You do not need to move the users if the deployment uses a flat LDAP structure, that is, all users are synchronized to all Cisco Unified Communications Manager and IM and Presence Service clusters where users are licensed to only one cluster.

For more information about how to move the migrating users to the relevant OU of the new home cluster, see the LDAP Administration documentation.

After you move the users, you must delete the LDAP entries from the old LDAP cluster.

What to do next

Proceed to synchronize the users to the new home cluster.

Synchronize Users To New Home Cluster

If LDAP is enabled on Cisco Unified Communications Manager, you must synchronize the users to the new home Cisco Unified Communications Manager cluster. You can do this manually on Cisco Unified Communications Manager or you can wait for a scheduled synchronization on Cisco Unified Communications Manager.

To manually force the synchronization on Cisco Unified Communications Manager, complete the following procedure.

Procedure

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

Step 2 Click **Perform Full Sync Now**.

What to do next

Proceed to enable users for IM and Presence Service and license users on the new cluster.

Related Topics

Enable Users For IM and Presence Service On New Cluster, on page 275

LDAP Sync Not Enabled On Cisco Unified Communications Manager

If LDAP Sync is not enabled on Cisco Unified Communications Manager, you must manually provision the users on the new Cisco Unified Communications Manager cluster. See the *Cisco Unified Communications Manager Administration Guide* for more information.

Enable Users For IM and Presence Service On New Cluster

When the users have been synchronized, or manually provisioned, on the new home cluster, you must enable the users for IM and Presence Service and Cisco Jabber.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End User**.

Step 2 Use the filters to find the user that you want to enable for IM and Presence Service.

Step 3 In the **End User Configuration** screen, check **Enable User for Unified CM IM and Presence**.

Step 4 Click **Save**.

Step 5 Provision the users on Cisco Unified Communications Manager for Phone and CSF. See the *Cisco Unified Communications Manager Administration Guide* for more information.

For information about how to update users in bulk, see the *Cisco Unified Communications Manager Bulk Administration Guide*.

What to do next

Proceed to import contact lists on the new home cluster.

Import Contact Lists On Home Cluster

You must import the contact lists to restore contact data for the migrated users.

Procedure

Step 1 Upload the previously exported contact list CSV file.

a) Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Upload/Download Files**.
b) Click **Add New**.
c) Click **Browse** to locate and choose the contact list CSV file.
d) Choose **Contact Lists** as the Target.
e) Choose **Import Users' Contacts - Custom File** as the Transaction Type,
f) Optionally check **Overwrite File if it exists**.
g) Click **Save** to upload the file.

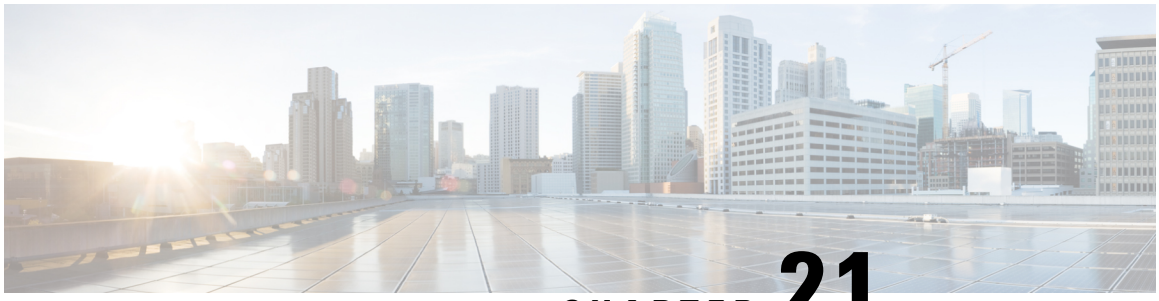
Step 2 Run the import contact list job.

a) Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Contact List** > **Update**.
b) Choose the CSV file you uploaded in Step 1.
c) Optionally update the Job Description.
d) To run the job now, click **Run Immediately**. Click **Run Later** to schedule the update for a later time.
e) Click **Submit.**

Step 3 Monitor the contact list import status.

a) Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Job Scheduler**.
b) Click **Find** to list all BAT jobs.
c) Choose the job ID of the contact list import job when its status is reported as complete.
d) To view the contents of the contact list file, choose the file listed at **CSV File Name**.
e) Click the **Log File Name** link to open the log.

The begin and end time of the job is listed and a result summary is also displayed.



CHAPTER 21

Migrate Users to Centralized Deployment

Centralized Deployment User Migration Overview

This chapter contains procedures for migrating existing IM and Presence Service users from a standard decentralized IM and Presence deployment (IM and Presence Service on Cisco Unified Communications Manager) to a centralized deployment. With the centralized deployment, the IM and Presence deployment and the telephony deployment are in separate clusters.

Prerequisite Tasks for Central Cluster Migration

If you are setting up a new IM and Presence central cluster whereby all the users are migrating from existing decentralized clusters, complete the following prerequisite steps to set up the cluster for migration.

Note If you are adding new users whom are not a part of the migration, you can follow the instructions in Configure Centralized Deployment, on page 57 to set up the central cluster with your new users. Migrate existing users to the central cluster only after you are confident that your configuration works.

Table 31: Pre-Migration Tasks

	Pre-Migration Tasks
Step 1	Connect your new central cluster to the migrating cluster. **1.** Log in to database publisher node on the IM and Presence Service centralized cluster. **2.** From Cisco Unified CM IM and Presence Administration, choose **System** > **Centralized Deployment**. **3.** Click **Find** and do either of the following: • Select an existing cluster and click **Edit Selected**. • Click **Add New** to add the migrating cluster. **4.** Complete the following fields for each migrating cluster: • **Peer Address**—The FQDN, hostname, IPv4 address, or IPv6 address of the publisher node on the remote telephony • **AXL Username**—The login username for the AXL account on the remote telephony cluster. • **AXL Password**—The password for the AXL account on the remote cluster. **5.** Click **Save**.
Step 2	If the new central cluster will be part of an IM and Presence intercluster network, configure intercluster peering between the central cluster and any IM and Presence peer clusters that are not a part of the migration. The following guidelines apply: • You do not need to configure intercluster peering between the central cluster and the migrating clusters. However, if a migrating cluster has an intercluster peer connection configured with any number of non-migrating clusters at the time of the migration, it's mandatory that those intercluster peer connections are configured in the central cluster prior to the migration or the migration will not work. • After configuring intercluster peering, make sure to verify the intercluster peering status to ensure that the configuration works properly For details, see Configure Intercluster Peers, on page 153.

Migration to Central Cluster Task Flow

Complete these tasks to migrate existing users from a decentralized cluster (IM and Presence Service on Cisco Unified Communications Manager) to a centralized IM and Presence cluster. In this task flow:

- **IM and Presence Central Cluster** refers to the cluster to which you are migating users. Following the migration, this cluster handles IM and Presence only.
- **Migrating Cluster** refers to the cluster from which IM and Presence users are being migrated. Following the migration, this cluster handles telephony only.

Before You Begin

If your IM and Presence central cluster is a newly installed cluster, and does not yet have users, complete the Prerequisite Tasks for Central Cluster Migration, on page 277 before you migrate users.

Table 32: Migration to Central Cluster Task Flow

	IM and Presence Central Cluster	Migrating Cluster	Purpose
Step 1		Export Contact Lists from Migrating Cluster, on page 280	Export user contact lists in the migrating cluster to a csv file.
Step 2		Disable High Availability in Migrating Cluster, on page 281	Disable High Availability for all Presence Redundancy Groups (subclusters) in the migrating cluster.
Step 3		Configure UC Service for IM and Presence, on page 282	In the migrating cluster, configure IM and Presence UC services that point to the IM and Presence central cluster.
Step 4		Create Service Profile for IM and Presence, on page 282	In the migrating cluster, create a service profile that uses the IM and Presence UC services that you set up.
Step 5		Disable Presence Users in Telephony Cluster, on page 283	Use Bulk Administration in the migrating cluster to disable IM and Presence for users.
Step 6		Enable OAuth Authentication for Central Cluster, on page 284	Optional. In the migrating cluster, enable OAuth Refresh Logins. This will enable the feature for the central cluster as well.
Step 7	Disable High Availability in Central Cluster, on page 284		Disable High Availability in all Presence Redundancy Groups (subcluster) of the IM and Presence central cluster.
Step 8	Delete Peer Relationship for Central and Migrating Clusters, on page 285		If intercluster peering exists between the central cluster and migrating cluster, delete the peer connection on both clusters.
Step 9	Stop the Cisco Intercluster Sync Agent, on page 285		Stop the Cisco Intercluster Sync Agent in the IM and Presence central cluster.

	IM and Presence Central Cluster	Migrating Cluster	Purpose
Step 10	Enable IM and Presence via Feature Group Template, on page 286		In the cenral cluster, configure a Feature Group Template that enables the IM and Presence Service.
Step 11	Complete LDAP Sync on Central Cluster, on page 286		Add the feature group template to an LDAP directory sync. Use the sync to add users from the migrating cluster.
Step 12	Import Contact Lists into Central Cluster, on page 288		Use Bulk Administration and the csv export file that you created earlier to import contact lists into the central cluster.
Step 13	Start Cisco Intercluster Sync Agent, on page 289		Start the Cisco Intercluster Sync Agent in the central cluster.
Step 14	Enable High Availability in Central Cluster, on page 289		In the central cluster, enable High Availability in all Presence Redundancy Groups.
Step 15		Delete Remaining Peers for Migrating Cluster, on page 290	Delete remaining intercluster peer connections between migrating cluster (now a telephony cluster) and other peer clusters.

Export Contact Lists from Migrating Cluster

Use this procedure only if you are migrating from a Decentralized IM and Presence Deployment to a Centralized Deployment. In the migrating cluster, export your users' contact lists to a csv file that you will later be able to import into the central cluster. You can export two types of contact lists:

- Contact Lists—This list consists of IM and Presence contacts. Contacts whom do not have an IM address will not be exported with this list (you must export a non-presence contact list).
- Non-presence Contact Lists—This list consists of contacts whom do not have an IM address.

Procedure

Step 1 Log in to Cisco Unified CM IM and Presence Administration in the old clsuter (the telephony cluster).

Step 2 Choose one of the following options, depending on which type of contact list you want to export:

- For Contact List exports, choose **Bulk Administration** > **Contact List** > **Export Contact List**
- for Non-presence Contact List exports, choose **Bulk Administration** > **Non-presence Contact List** > **Export Non-presence Contact List** and skip the next step.

Step 3 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 option is **All users in the cluster**.

b) Click **Find** to bring up the list of users and then click **Next**.

Step 4 Enter a **File Name**.

Step 5 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 to run.

Step 6 Click **Submit**.

Note If you chose **Run Immediately**, your export file gets generated right away. If you chose **Run Later**, you must use the Job Scheduler at (**Bulk Administration** > **Job Scheduler**) to schedule a time for this job to run.

Step 7 After the export file is generated, download the csv file:

a) Choose **Bulk Administration** > **Upload/Download Files**.

b) Click **Find**.

c) Select the export file that you want to download and click **Download Selected**.

d) Save the file to a safe location.

Step 8 Repeat this procedure if you want to create another csv export file. For example, if you create an export file for Contact Lists, you may want to create another file for Non-presence Contact Lists.

What to do next

Disable High Availability in Migrating Cluster, on page 281

Disable High Availability in Migrating Cluster

For migrations to a Centralized Deployment, disable High Availability in each Presence Redundancy Group (subcluster) on the migrating telephony cluster.

Procedure

Step 1 Log in to the Cisco Unified Communications Manager publisher node on the old cluster.

Step 2 From Cisco Unified CM Administration, choose **System** > **Presence Redundancy Groups**.

Step 3 Click **Find** and select a subcluster.

Step 4 Uncheck the **Enable High Availability** check box.

Step 5 Click **Save**.

Step 6 Repeat this procedure for each subcluster.

Note After completing this procedure for all subclusters, wait at least 2 minutes before completing any additional configurations on this cluster.

What to do next

Configure UC Service for IM and Presence, on page 282

Configure UC Service for IM and Presence

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

What to do next

Create Service Profile for IM and Presence, on page 282

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. Users in the telephony cluster will use this service profile to get IM and Presence services from the central cluster.

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

Disable Presence Users in Telephony Cluster, on page 283

Disable 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.

- **Enable User for Unified CM IM and Presence**—Leave the right check box unchecked. This setting disables the telephony cluster as the provider of IM and Presence.
- **UC Service Profile**—From the drop-down, select the service profile that you configured in the previous task. This setting points users to the IM and Presence central cluster, which will be the provider of the IM and Presence Service.

Note For Expressway MRA configuration, see *Mobile and Remote Access via Cisco Expressway Deployment Guide* at https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html.

Step 5 Complete any remaining fields that you want. For help with the fields and their settings, see the online help.

Step 6 Under **Job Information**, select **Run Immediately**.

Step 7 Click **Submit**.

What to do next

Enable OAuth Authentication for Central Cluster, on page 284

Enable OAuth Authentication for Central Cluster

Use this procedure to enable OAuth authentication in the telephony cluster. This also enables OAuth authentication in the IM and Presence central cluster.

Procedure

Step 1 Log in to Cisco Unified CM Administration on the telephony cluster.

Step 2 Choose **System** > **Enterprise Parameters**

Step 3 Under **SSO And OAuth Configuration**, set the **OAuth with Refresh Login Flow** enterprise parameter to **Enabled**.

Step 4 If you edited the parameter setting, click **Save**.

Disable High Availability in Central Cluster

Make sure that High Availability is disabled in each Presence Redundancy Group (subcluster) of the IM and Presence central cluster. You must do this before you begin applying configurations or migrating users.

Procedure

Step 1 Log in to Cisco Unified CM Administration instance for the central cluster.

Step 2 Choose **System** > **Presence Redundancy Groups**.

Step 3 Click **Find** and select an existing subcluster.

Step 4 Uncheck the **Enable High Availability** check box.

Step 5 Click **Save**.

Step 6 Repeat this step for each subcluster.

What to do next

Stop the Cisco Intercluster Sync Agent, on page 285

Delete Peer Relationship for Central and Migrating Clusters

If intercluster peering exists between the IM and Presence central cluster and the migrating cluster, delete that peer relationship.

Procedure

Step 1 Log in to the IM and Presence Service central cluster's database publisher node.

Step 2 From Cisco Unified CM IM and Presence Administration, choose **Presence** > **Inter-Clustering**.

Step 3 Click **Find** and select the migrating cluster.

Step 4 Click **Delete**.

Step 5 Restart the **Cisco XCP Router**:

a) Log in to Unified IM and Presence Serviceability and choose **Tools** > **Control Center - Network Services**.
b) From the **Server** list, choose the database publisher node and click **Go**.
c) Under **IM and Presence Services**, select **Cisco XCP Router** and click **Restart**.

Step 6 Repeat these steps on the migrating cluster.

Stop the Cisco Intercluster Sync Agent

Before you configure the IM and Presence central cluster, make sure that the **Cisco Intercluster Sync Agent** service is stopped on the central cluster.

Procedure

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

Step 2 From the **Server** drop-down, select the central cluster database publisher node, and click **Go**.

Step 3 Confirm the status of the **Cisco Intercluster Sync Agent** service. If the service is running or activated, select the adjacent radio button and click **Stop**.

What to do next

Enable IM and Presence via Feature Group Template, on page 286

Enable IM and Presence via Feature Group Template

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 65.

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 add the Feature Group Template to an LDAP directory configuration where the initial sync has not yet occurred, and then complete the initial sync.

Complete LDAP Sync on Central Cluster, on page 286

Complete LDAP Sync on Central Cluster

Use this procedure on your remote Cisco Unified Communications Manager telephony clusters to use an LDAP sync to deploy your centralized IM and Presence settings to your Cisco Unified Communications Manager deployment.

Note For more details on how to set up an LDAP Directory sync, 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 the **System** > **LDAP** > **LDAP Directory**.

Step 2 Do either of the following:

- Click **Find** and select an existing LDAP Directory sync.
- Click **Add New** to create a new LDAP Directory sync.

Step 3 From the **Feature Group Template** drop-down list box, select the feature group template that you created in the previous task. IM and Presence must be disabled on this template.

Step 4 Complete the remaining fields in the **LDAP Directory** window. For help with the fields and their settings, refer to the online help.

Step 5 Click **Save**.

Step 6 Click **Perform Full Sync**.
Cisco Unified Communications Manager synchronizes its database with the LDAP directory and assigns the updated IM and Presence settings.

What to do next

Import Contact Lists into Central Cluster, on page 288

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.

Note 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 the 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**.

Import Contact Lists into Central Cluster

If you have migrated users to the IM and Presence Central Cluster, you can use this procedure to import your users' contact lists into the IM and Presence central cluster. You can import either of the following types of contact lists:

- Contact lists—This list contains IM and Presence contacts.
- Non-presence contact lists—This list contains contacts whom do not have an IM address.

Before you begin

You require the contact list csv file(s) that you exported from the old cluster (the telephony cluster).

Procedure

Step 1 Log in to Cisco Unified CM IM and Presence Administration on the IM and Presence central cluster.

Step 2 Upload the csv file that you exported from the telephony cluster:

a) Choose **Bulk Administration** > **Upload/Download Files**.
b) Click **Add New**.
c) Click **Choose File** and select the csv file that you want to import.
d) From the **Select the Target** drop-down select either of the following: **Contact Lists** or **Non-presence Contact Lists** depending on which type of contact list you are importing.
e) From the **Select Transaction Type**, select the import job.
f) Click **Save**.

Step 3 Import the csv information into the central cluster:

a) From Cisco Unified CM IM and Presence Administration, do either of the following:

- For Contact List imports, choose **Bulk Administration** > **Contact Lists** > **Update Contact Lists**.
- For Non-presence Contact List imports, choose **Bulk Administration** > **Non-presence Contact Lists** > **Import Non-presence Contact Lists**.

b) From the **File Name** drop-down, select the csv file that you uploaded.
c) Under **Job Information**, select either **Run Immediately** or **Run Later** depending on when you want the job to run.
d) Click **Submit**. If you chose **Run Immediately**, the contact lists get imported right away

Note . If you chose **Run Later**, you must go to **Bulk Administration** > **Job Scheduler** where you can select the job and schedule a time for it to run.

Step 4 Repeat this procedure if you have a second csv file to import.

What to do next

Start Cisco Intercluster Sync Agent, on page 289

Start Cisco Intercluster Sync Agent

After your configuration or migration is complete, start the **Cisco Intercluster Sync Agent** in the IM and Presence central cluster. This service is required if you are using intercluster peering.

Procedure

Step 1 From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**.
Step 2 From the **Server** drop-down, select the IM and Presence database publisher node and click **Go**.
Step 3 Under **IM and Presence Services**, select the **Cisco Intercluster Sync Agent** and click **Start**.

What to do next

Enable High Availability in Central Cluster, on page 289

Enable High Availability in Central Cluster

After your configuration or user migration is complete, enable High Availability in the Presence Redundancy Groups (subclusters) for the IM and Presence central cluster.

Procedure

Step 1 Log in to the Cisco Unified CM Administration instance on the IM and Presence central cluster.
Step 2 Choose **System** > **Presence Redundancy Groups**.
Step 3 Click **Find** and select an existing subcluster.

Step 4 Check the **Enable High Availability** check box.

Step 5 Click **Save**.

Step 6 Repeat this procedure for each subcluster in the IM and Presence central cluster.

Delete Remaining Peers for Migrating Cluster

Delete intercluster peer relationships between the migrating cluster (now a telephony cluster) and any remaining IM and Presence Service peer clusters.

Note Removing intercluster connections can be postponed to a later date depending on the Cisco XCP Router restart availability across the entire mesh. As long as there are existing intercluster connections between telephony cluster and any number of peer clusters, currently running Cisco XCP Router services should be kept in **Running** state on the telephony cluster.

Procedure

Step 1 Log in to the migrating cluster's IM and Presence database publisher node.

Step 2 From Cisco Unified CM IM and Presence Administration, choose **Presence** > **Inter-Clustering**.

Step 3 Click **Find** and select the peer cluster.

Step 4 Click **Delete**.

Step 5 Restart the **Cisco XCP Router**:

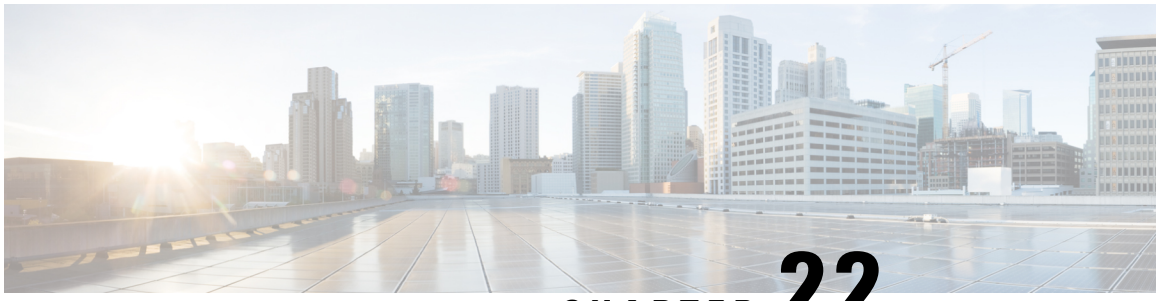
a) Log in to Unified IM and Presence Serviceability and choose **Tools** > **Control Center - Network Services**.

b) From the **Server** list, choose the database publisher node and click **Go**.

c) Under **IM and Presence Services**, select **Cisco XCP Router** and click **Restart**.

Step 6 Repeat these steps on the IM and Presence Service peer cluster.

Note If the migrating cluster has intercluster peer connections to multiple clusters, you must repeat this procedure for each peer cluster that remains in the intercluster network. This means that, on the migrating cluster, there will be as many cycles of **Cisco XCP Router** restarts as there are peer cluster connections that are being broken.



CHAPTER 22

Multilingual Support Configuration For IM and Presence Service

Locale Installation

You can configure Cisco Unified Communications Manager and IM and Presence Service to support multiple languages. There is no limit to the number of supported languages you can install.

Cisco provides locale-specific versions of the Cisco Unified Communications Manager Locale Installer and the IM and Presence Service Locale Installer on www.cisco.com. Installed by the system administrator, the locale installer allows the user to view/receive the chosen translated text or tones, if applicable, when a user works with supported interfaces.

After you upgrade Cisco Unified Communications Manager or the IM & Presence Service, you must reinstall all the locales. Install the latest version of the locales that match the major.minor version number of your Cisco Unified Communications Manager node or IM and Presence Service node.

Install locales after you have installed Cisco Unified Communications Manager on every node in the cluster and have set up the database. If you want to install specific locales on IM and Presence Service nodes, you must first install the Cisco Unified Communications Manager locale file for the same country on the Cisco Unified Communications Manager cluster.

Use the information in the following sections to install locales on Cisco Unified Communications Manager nodes and on IM and Presence Service nodes after you complete the software upgrade.

User Locales

User locale files contain language information for a specific language and country. They provide translated text and voice prompts, if available, for phone displays, user applications, and user web pages in the locale that the user chooses. These files use the following naming convention:.

- cm-locale-language-country-version.cop (Cisco Unified Communications Manager)
- ps-locale-language_country-version.cop (IM and Presence Service)

If your system requires user locales only, install them after you have installed the CUCM locale.

Network Locales

Network locale files provide country-specific files for various network items, including phone tones, annunciators, and gateway tones. The combined network locale file uses the following naming convention:

- cm-locale-combinednetworklocale-version.cop (Cisco Unified Communications Manager)

Cisco may combine multiple network locales in a single locale installer.

Note Virtualized deployments of Cisco Unified Communications Manager on Cisco-approved, customer-provided servers can support multiple locales. Installing multiple locale installers ensures that the user can choose from a multitude of locales.

You can install locale files from either a local or a remote source by using the same process for installing software upgrades. You can install more than one locale file on each node in the cluster. Changes do not take effect until you reboot every node in the cluster. Cisco strongly recommends that you do not reboot the nodes until you have installed all locales on all nodes in the cluster. Minimize call-processing interruptions by rebooting the nodes after regular business hours.

Locale Installation Considerations

Install locales after you have installed Cisco Unified Communications Manager on every node in the cluster and have set up the database. If you want to install specific locales on IM and Presence Service nodes, you must first install the Cisco Unified Communications Manager locale file for the same country on the Cisco Unified Communications Manager cluster.

You can install more than one locale file on each node in the cluster. To activate the new locale, you must restart each node in the cluster after installation.

You can install locale files from either a local or a remote source by using the same process for installing software upgrades. See the *Upgrade Guide for Cisco Unified Communications Manager* for more information about upgrading from a local or a remote source.

Locale Files

Install locales after you have installed Cisco Unified Communications Manager on every node in the cluster and have set up the database. If you want to install specific locales on IM and Presence Service nodes, you must first install the Cisco Unified Communications Manager locale file for the same country on the Cisco Unified Communications Manager cluster.

You can install more than one locale file on each node in the cluster. To activate the new locale, you must restart each node in the cluster after installation.

When you install locales on a node, install the following files:

- User Locale files - These files contain language information for a specific language and country and use the following convention:

  `cm-locale-language-country-version.cop` (Cisco Unified Communications Manager)

ps-locale-language_country-version.cop (IM and Presence Service)

- Combined Network Locale file - Contains country-specific files for all countries for various network items, including phone tones, annunciators, and gateway tones. The combined network locale file uses the following naming convention:

  `cm-locale-combinednetworklocale-version.cop` (Cisco Unified Communications Manager)

Install Locale Installer on IM and Presence Service

Before you begin

- Install the Locale Installer on Cisco Unified Communications Manager. If you want to use a locale other than English, you must install the appropriate language installers on both Cisco Unified Communications Manager and on IM and Presence Service.
- If your IM and Presence Service cluster has more than one node, make sure that the locale installer is installed on every node in the cluster (install on the IM and Presence database publisher node before the subscriber nodes).
- User locales should not be set until all appropriate locale installers are loaded on both systems. Users may experience problems if they inadvertently set their user locale after the locale installer is loaded on Cisco Unified Communications Manager but before the locale installer is loaded on IM and Presence Service. If issues are reported, we recommend that you notify each user to sign into the Cisco Unified Communications Self Care Portal and change their locale from the current setting to English and then back again to the appropriate language. You can also use the BAT tool to synchronize user locales to the appropriate language.
- You must restart the server for the changes to take effect. After you complete all locale installation procedures, restart each server in the cluster. Updates do not occur in the system until you restart all servers in the cluster; services restart after the server reboots.

Procedure

Step 1 Navigate to `cisco.com` and choose the locale installer for your version of IM and Presence Service.

http://software.cisco.com/download/navigator.html?mdfid=285971059

Step 2 Click the version of the IM and Presence Locale Installer that is appropriate for your working environment.

Step 3 After downloading the file, save the file to the hard drive and note the location of the saved file.

Step 4 Copy this file to a server that supports SFTP.

Step 5 Sign into Cisco Unified IM and Presence Operating System Administration using the administrator account and password.

Step 6 Choose **Software Upgrades** > **Install/Upgrade**.

Step 7 Choose Remote File System as the software location source.

Step 8 Enter the file location, for example `/tmp`, in the Directory field.

Step 9 Enter the IM and Presence Service server name in the Server field.

Step 10 Enter your username and password credentials in the User Name and User Password fields.

Step 11 Choose SFTP for the Transfer Protocol.

Step 12 Click **Next**.

Step 13 Choose the IM and Presence Service locale installer from the list of search results.

Step 14 Click **Next** to load the installer file and validate it.

Step 15 After you complete the locale installation, restart each server in the cluster.

Step 16 The default setting for installed locales is "English, United States". While your IM and Presence Service node is restarting, change the language of your browser, if necessary, to match the locale of the installer that you have downloaded.

Step 17 Verify that your users can choose the locales for supported products.

Tip Make sure that you install the same components on every server in the cluster.

Error Messages

See the following table for a description of the messages that can occur during Locale Installer activation. If an error occurs, you can view the messages in the installation log.

Table 33: Locale Installer Messages and Descriptions

Message	Description
[LOCALE] File not found: <language>_<country>_user_locale.csv, the user locale has not been added to the database.	This error occurs when the system cannot locate the CSV file, which contains user locale information to add to the database, which indicates an error with the build process.
[LOCALE] File not found: <country>_network_locale.csv, the network locale has not been added to the database.	This error occurs when the system cannot locate the CSV file, which contains network locale information to add to the database This indicates an error with the build process.
[LOCALE] CSV file installer installdb is not present or not executable	You must ensure that an application called *installdb* is present. It reads information that a CSV file contains and applies it correctly to the target database. If this application is not found, it did not get installed with the Cisco Unified Communications application (very unlikely), has been deleted (more likely), or the node does not have a Cisco Unified Communications application, such as Cisco Unified Communications Manager or IM and Presence Service, installed (most likely). Installation of the locale will terminate because locales will not work without the correct records in the database.

Message	Description
[LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maDialogs_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maMessages_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maGlobalUI_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt.Checksum.	These errors could occur when the system fails to create a checksum file, which an absent Java executable, `/usr/local/thirdparty/java/j2sdk/jre/bin/java`, `an absent or damaged Java archive file, /usr/local/cm/jar/cmutil.jar`, or an absent or damaged Java class, `com.cisco.ccm.util.Zipper`, causes. Even if these errors occur, the locale will continue to work correctly, with the exception of Cisco Unified Communications Manager Assistant, which can not detect a change in localized Cisco Unified Communications Manager Assistant files.
[LOCALE] Could not find /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt in order to update Unified CM Assistant locale information.	This error occurs when the system does not find the file in the correct location, which is most likely due to an error in the build process.
[LOCALE] Addition of <locale-installer-file-name> to the database has failed!	This error occurs because the collective result of any failure that occurs when a locale is being installed causes it; it indicates a terminal condition.
[LOCALE] Could not locate <locale-installer-file-name>	The system will not migrate this locale during an upgrade. The downloaded locale installer file no longer resides in the download location. The platform may have moved or deleted it. This is noncritical error indicates that after the Cisco Unified Communications application has been upgraded, you need to either reapply the locale installer or download and apply a new locale installer.
[LOCALE] Could not copy <locale-installer-file-name> to migratory path. This locale will not be migrated during an upgrade!	You cannot copy the downloaded locale installer file to the migration path. This noncritical error indicates that after the Cisco Unified Communications application has been upgraded, you need to either reapply the locale installer or download and apply a new locale installer.
[LOCALE] DRS unregistration failed	The locale installer could not deregister from the Disaster Recovery System. A backup or restore record will not include the locale installer. Record the installation log and contact Cisco TAC.

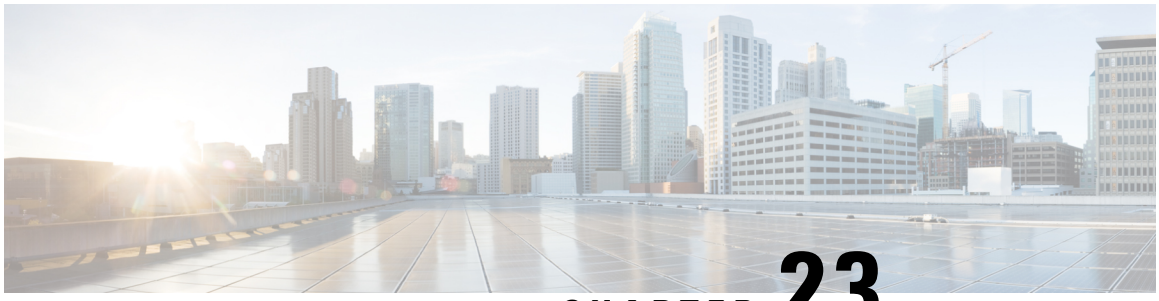
Message	Description
[LOCALE] Backup failed!	The Disaster Recovery System could not create a tarball from the downloaded locale installer files. Re-apply the local installer before attempting to back up. **Note** Manually reinstalling locales after a system restore achieves the same goal.
[LOCALE] No COP files found in restored tarball!	Corruption of backup files may prevent successful extraction of locale installer files. **Note** Manual reapplication of the locale installer will restore the locale fully.
[LOCALE] Failed to successfully reinstall COP files!	Corruption of backup files may damage locale installer files. **Note** Manual reapplication of the locale installer will restore the locale fully.
[LOCALE] Failed to build script to reinstall COP files!	The platform could not dynamically create the script used to reinstall locales. **Note** Manual reapplication of the locale installer will restore the locale fully. Record the installation log and contact TAC.

Localized Applications

IM and Presence Service applications support a variety of different languages. See the following table for a list of localized applications and the available languages.

Table 34: List of Localized Applications and Supported Languages

Interface	Supported Languages
Administrative Applications	
Cisco Unified CM IM and Presence Administration	Chinese (China), English, Japanese (Japan), Korean (Korean Republic)
Cisco Unified IM and Presence Operating System	Chinese (China), English, Japanese (Japan), Korean (Korean Republic)



CHAPTER 23

Branding Customizations

Branding Overview

The Branding feature lets you apply customized branding for the IM and Presence Service. The branding customizations display in the Cisco Unified CM IM and Presence Administration login and configuration windows. Among the items that you can add or modify include:

- Company logos
- Background colors
- Border colors
- Font colors

Branding Prerequisites

You must create a branding zip file with the prescribed folder structure and files. For details, see Branding File Requirements, on page 298.

Enable Branding

Use this procedure to enable branding customizations for the IM and Presence Service cluster. Branding updates display even if you have SAML SSO enabled.

Before you begin

Save the `branding.zip` file with your IM and Presence customizations in a location that the IM and Presence Service can access.

Procedure

Step 1 Log in to Cisco Unified IM and Presence OS Administration.
Step 2 Choose **Software Upgrades** > **Branding**.
Step 3 **Browse** to your remote server and select the `branding.zip` file.
Step 4 Click **Upload File**.
Step 5 Click **Enable Branding**.

Note You can also enable branding by running the **utils branding enable** CLI command.

Step 6 Refresh your browser to see the changes.
Step 7 Repeat this procedure on all IM and Presence Service cluster nodes.

Disable Branding

Use this procedure to disable branding in the IM and Presence Service cluster.

Note To disable branding, you must use the master administrator account with privilege level 4 access. This is the main administrator account that is created during installation.

Procedure

Step 1 Log in to Cisco Unified IM and Presence OS Administration.
Step 2 Choose **Software Upgrades** > **Branding**.
Step 3 Click **Disable Branding**.

Note You can also disable branding by running the **utils branding disable** CLI command.

Step 4 Refresh your browser to see the changes.
Step 5 Repeat this procedure on all IM and Presence Service cluster nodes.

Branding File Requirements

Before you apply customized branding to your system, create your `branding.zip` file according to the specifications. On a remote server, create a `Branding` folder and fill the folder with the specified contents. Once you have added all the image files and subfolders, zip the entire folder and save the file as `branding.zip`.

There are two options for the folder structure, depending on whether you want to use a single image for the header, or a combination of six images in order to create a graded effect for the header.

Table 35: Folder Structure Options

Branding Option	Folder Structure

Single Header Option	If you want a single image for the header background (callout item 3), your branding folder must contain the following subfolders and image files:
	
	`Branding (folder)`
	`  cup (folder)`
	`  BrandingProperties.properties (properties file)`
	`  brandingHeader.gif (652*1 pixel)`
	`  ciscoLogo12pxMargin.gif (44*44 pixel)`

Graded Header Option	If you want to create a graded image for the header background (callout item 3, 4, 5), you need six separate image files to create the graded effect. Your branding folder must contain these subfolders and files
	
	`Branding(folder)`
	`  cup (folder)`
	`  BrandingProperties.properties (file)`
	`  brandingHeaderBegLTR.gif (652*1 pixel image)`
	`  brandingHeaderBegRTR.gif (652*1 pixel image)`
	`  brandingHeaderEndLTR.gif (652*1 pixel image)`
	`  brandingHeaderEndRTR.gif (652*1 pixel image)`
	`  brandingHeaderMidLTR.gif (652*1 pixel image)`
	`  brandingHeaderMidRTR.gif (652*1 pixel image)`
	`  ciscoLogo12pxMargin.gif (44*44 pixel image)`

User Interface Branding Options

The following images display the branding options for the Cisco Unified CM IM and Presence Administration user interface.

Figure 17: Branding Options for the Administration Login Screen

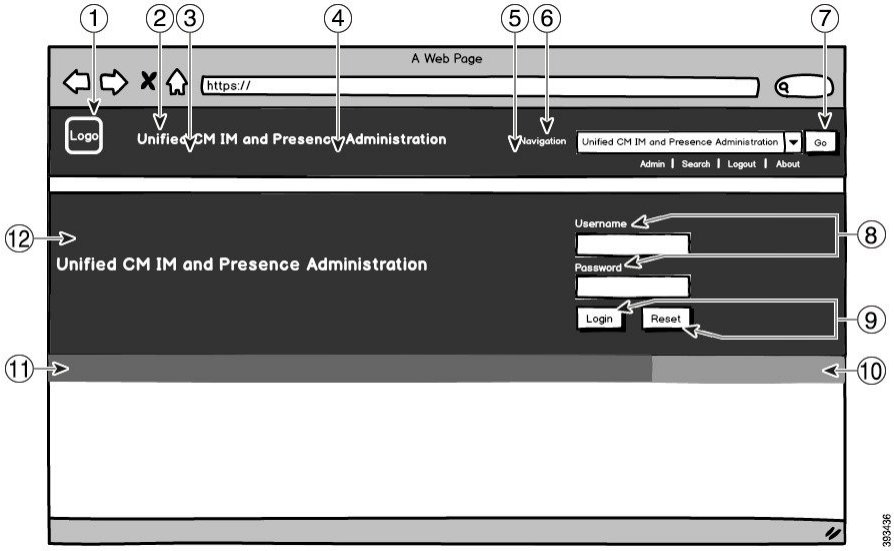
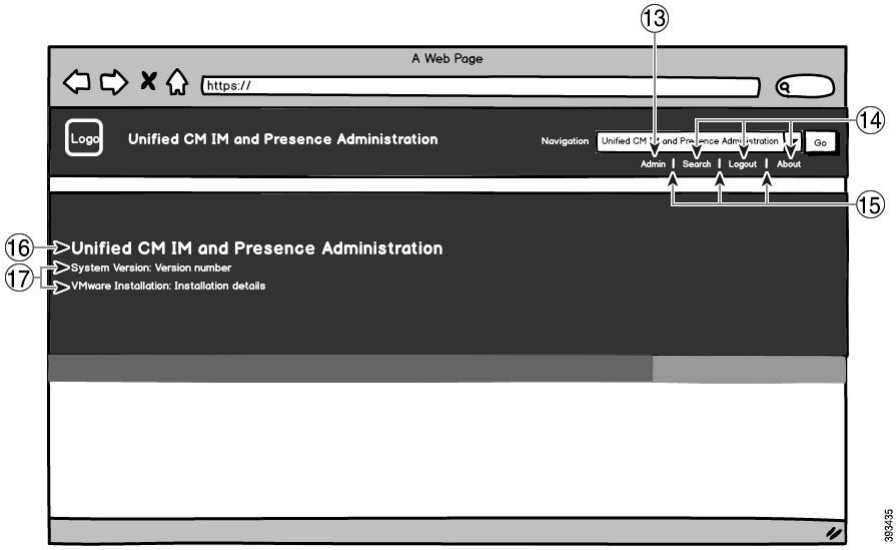


Figure 18: Branding Options for the Administration Logged In Screen



The following table describes how the callout items in the above screen captures can be customized.

Table 36: User Interface Branding Options

Item	Description	Branding Edits
Login Screen Image		
1	Company Logo	To add your logo to the IM and Presence Service interface, save your company logo as a 44x44 pixel image with the following filename: `ciscoLogo12pxMargin.gif` (44*44 pixels)
2	Unified CM IM and Presence Administration text in header	header.heading.color
3	Header Background (Graded option - left)	If you want to have a graded effect for the header image, use the following images for the left side. • `brandingHeaderBegLTR.gif` (652 x 1 pixel) • `brandingHeaderBegLTR.gif` (652 x 1 pixel)

Item	Description	Branding Edits
4	Header Background	If you want to use a single image for the header: • `brandingHeader.gif` (652 x 1 pixel) Otherwise, if you are creating a header with a graded effect, use the following images: • `brandingHeaderMidLTR.gif` (652 x 1 pixel) • `brandingHeaderMidRTR.gif` (652 x 1 pixel)
5	Header Background (Graded option - right)	If you want to use a graded effect for the header, use this image for the right header: • `brandingHeaderEndLTR` (652 x 1 pixel) • `brandingHeaderEndRTR` (652 x 1 pixel)
6	Navigation text	header.navigation.color
7	Go button	header.go.font.color header.go.background.color
8	Username and Password text	splash.loginfield.color
9	Login and Reset buttons	splash.button.text.color splash.button.color
10	Bottom background color – right	splash.hex.code.3
11	Bottom background color – left	splash.hex.code.2
12	Banner	splash.hex.code.1
Post Login Image		
13	Logged in user text (for example, the 'admin' user)	header.text.bold.color
14	Search, About, Logout links	header.link.color
15	Link divider	header.divider.color
16	Unified CM IM and Presence Administration text in banner (post-login)	splash.login.text.color
17	System version and VMware Installation text	splash.version.color

Branding Properties Editing Example

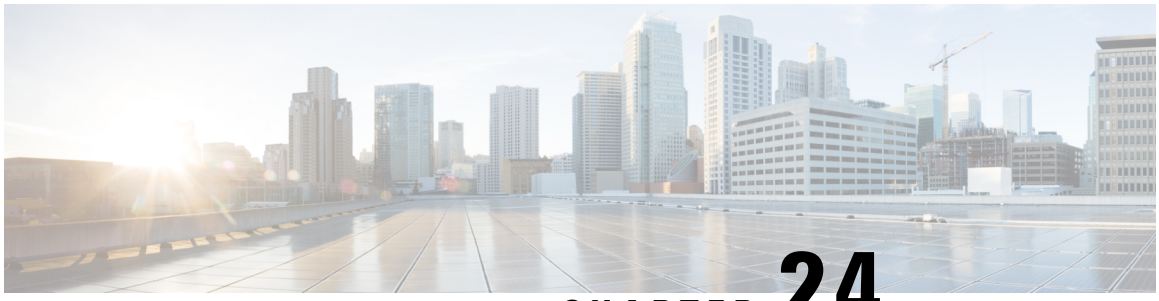
Branding properties can be edited by adding the hex code in the properties file (`BrandingProperties.properties`). The properties file uses HTML-based hex code. For example, if you want to change the color of the Navigation text item (callout item #6) to red, add the following code to your properties file:

```
header.navigation.color="#FF0000"
```

In this code, `header.navigation.color` is the branding property that you want to edit, and `"#FF0000"` is the new setting (red).

PART V

Troubleshooting IM and Presence Service



CHAPTER 24

Troubleshooting High Availability

Manual Failover, Fallback, and Recovery

Use Cisco Unified Communications Manager Administration to initiate a manual failover, fallback, and recovery for IM and Presence Service nodes in a presence redundancy group. You can also initiate these actions from Cisco Unified Communications Manager or IM and Presence Service using the CLI. See the *Command Line Interface Guide for Cisco Unified Communications Solutions* for details.

- Manual failover: When you initiate a manual failover, the Cisco Server Recovery Manager stops the critical services on the failed node. All users from the failed node are disconnected and must re-login to the backup node.

  Note After a manual failover occurs, critical services will not be started unless we invoke manual fallback.

- Manual fallback: When you initiate a manual fallback, the Cisco Server Recovery Manager restarts critical services on the primary node and disconnects all users that had been failed over. Those users must then re-login to their assigned node.
- Manual recovery: When both nodes in the presence redundancy group are in a failed state and you initiate a manual recovery, the IM and Presence Service restarts the Cisco Server Recovery Manager service on both nodes in the presence redundancy group.

Initiate Manual Failover

You can manually initiate a failover of IM and Presence Service nodes in a presence redundancy group using Cisco Unified Communications Manager Administration.

Procedure

Step 1 Select **System** > **Presence Redundancy Groups**.

The **Find and List Presence Redundancy Groups** window displays.

Step 2 Select the presence redundancy group search parameters, and then click **Find**.

Matching records appear.

Step 3 Select the presence redundancy group that is listed in the **Find and List Presence Redundancy Group** window.

The **Presence Redundancy Group Configuration** window appears.

Step 4 Click **Failover** in the ServerAction field.

Note This button appears only when the server and presence redundancy group are in the correct states.

Initiate Manual Fallback

Use Cisco Unified Communications Manager Administration to manually initiate the fallback of an IM and Presence Service node in a presence redundancy group that has failed over. For more information about presence redundancy group node status, see topics related to node state, state change causes, and recommended actions.

Procedure

Step 1 Select **System** > **Presence Redundancy Groups**.

The **Find and List Presence Redundancy Groups** window displays.

Step 2 Select the presence redundancy group search parameters, and then click **Find**.

Matching records appear.

Step 3 Select the presence redundancy group that is listed in the **Find and List Presence Redundancy Group** window.

The **Presence Redundancy Group Configuration** window appears.

Step 4 Click **Fallback** in the ServerAction field.

Note This button appears only when the server and presence redundancy group are in the correct states.

Initiate Manual Recovery

A manual recovery is necessary when both nodes in the presence redundancy group are in the failed state. Use Cisco Unified Communications Manager Administration to manually initiate the recovery of IM and Presence Service nodes in a presence redundancy group that is in the failed state.

For more information about presence redundancy group node status, see topics related to node state, state change causes, and recommended actions.

Before you begin

A manual recovery is necessary when both nodes in the presence redundancy group are in the failed state. Use Cisco Unified Communications Manager Administration to manually initiate the recovery of IM and Presence Service nodes in a presence redundancy group that is in the failed state.

Procedure

Step 1 Select **System** > **Presence Redundancy Groups**.

The **Find and List Presence Redundancy Groups** window displays.

Step 2 Select the presence redundancy group search parameters, and then click **Find**.

Matching records appear.

Step 3 Select the presence redundancy group that is listed in the **Find and List Presence Redundancy Group** window.

The **Presence Redundancy Group Configuration** window appears.

Step 4 Click **Recover**.

Note This button appears only when the server and presence redundancy group are in the correct states.

View Presence Redundancy Group Node Status

Use the **Cisco Unified CM Administration** user interface to view the status of IM and Presence Service nodes that are members of a presence redundancy group.

Procedure

Step 1 Choose **System** > **Presence Redundancy Groups**.

The **Find and List Presence Redundancy Groups** window displays.

Step 2 Choose the presence redundancy group search parameters, and then click **Find**.

Matching records appear.

Step 3 Choose a presence redundancy group that is listed in the search results.

The **Presence Redundancy Group Configuration** window appears. If two nodes are configured in that group and high availability is enabled, then the status of the nodes within that group are displayed in the High Availability area.

Node State Definitions

Table 37: Presence Redundancy Group Node State Definitions

State	Description
Initializing	This is the initial (transition) state when the Cisco Server Recovery Manager service starts; it is a temporary state.
Idle	IM and Presence Service is in Idle state when failover occurs and services are stopped. In Idle state, the IM and Presence Service node does not provide any availability or Instant Messaging services. In Idle state, you can manually initiate a fallback to this node using the **Cisco Unified CM Administration** user interface.
Normal	This is a stable state. The IM and Presence Service node is operating normally. In this state, you can manually initiate a failover to this node using the **Cisco Unified CM Administration** user interface.
Running in Backup Mode	This is a stable state. The IM and Presence Service node is acting as the backup for its peer node. Users have moved to this (backup) node.
Taking Over	This is a transition state. The IM and Presence Service node is taking over for its peer node.
Failing Over	This is a transition state. The IM and Presence Service node is being taken over by its peer node.
Failed Over	This is a steady state. The IM and Presence Service node has failed over, but no critical services are down. In this state, you can manually initiate a fallback to this node using the **Cisco Unified CM Administration** user interface.
Failed Over with Critical Services Not Running	This is a steady state. Some of the critical services on the IM and Presence Service node have either stopped or failed.
Falling Back	This is a transition state. The system is falling back to this IM and Presence Service node from the node that is running in backup mode.
Taking Back	This is a transition state. The failed IM and Presence Service node is taking back over from its peer.
Running in Failed Mode	An error occurs during the transition states or Running in Backup Mode state.
Unknown	Node state is unknown. 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 38: Presence Redundancy Group Node High-Availability States, Causes, and Recommended Actions

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Normal	Normal	Normal	Normal	Normal
Failing Over	On Admin Request	Taking Over	On Admin Request	The administrator initiated a manual failover from node 1 to node 2. The manual failover is in progress.
Idle	On Admin Request	Running in Backup Mode	On Admin Request	The manual failover from node 1 to node 2 that the administrator initiated is complete.
Taking Back	On Admin Request	Falling Back	On Admin Request	The administrator initiated a manual fallback from node 2 to node 1. The manual fallback is in progress.
Idle	Initialization	Running in Backup Mode	On Admin Request	The administrator restarts the SRM service on node 1 while node 1 is in “Idle” state.
Idle	Initialization	Running in Backup Mode	Initialization	The administrator either restarts both nodes in the presence redundancy group, or restarts the SRM service on both nodes while the presence redundancy group was in manual failover mode.
Idle	On Admin Request	Running in Backup Mode	Initialization	The administrator restarts the SRM service on node 2 while node 2 is running in backup mode, but before the heartbeat on node 1 times out.
Failing Over	On Admin Request	Taking Over	Initialization	The administrator restarts the SRM service on node 2 while node 2 is taking over, but before the heartbeat on node1 times out.
Taking Back	Initialization	Falling Back	On Admin Request	The administrator restarts the SRM service on node 1 while taking back, but before the heartbeat on node 2 times out. After the taking back process is complete, both nodes are in Normal state.
Taking Back	Automatic Fallback	Falling Back	Automatic Fallback	Automatic Fallback has been initiated from node 2 to node 1 and is currently in progress.

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Failed Over	Initialization or Critical Services Down	Running in Backup Mode	Critical Service Down	Node 1 transitions to Failed Over state when either of the following conditions occur: • 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.

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Running in Failed Mode	Start of Critical Services Failed	Running in Failed Mode	Start of Critical Services Failed	Critical services fail to start while a node in the presence redundancy group is taking back from the other node. **Recommended 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.

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Node 1 is down due to loss of network connectivity or the SRM service is not running.		Running in Backup Mode	Peer Down	Node 2 has lost the heartbeat from node 1. IM and Presence Service performs an automatic failover to node 2. **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.
Node 1 is down (due to possible power down, hardware failure, shutdown, reboot)		Running in Backup Mode	Peer Reboot	IM and Presence Service performs an automatic failover to node 2 due to the following possible conditions on node 1: • hardware failure • power down • restart • shutdown **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 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Failed Over with Critical Services not Running OR Failed Over	Initialization	Backup Mode	Peer Down During Initialization	Node 2 does not see node 1 during startup. **Recommended Action:** When node1 is up and all critical services are running, perform a manual fallback to restore the nodes in the presence redundancy group to the Normal state.
Running in Failed Mode	Cisco Server Recovery Manager Take Over Users Failed	Running in Failed Mode	Cisco Server Recovery Manager Take Over Users Failed	User move fails during the taking over process. **Recommended Action:** Possible database error. Click **Recovery** in the **Presence Redundancy Group Configuration** window. If the problem persists, then reboot the nodes.
Running in Failed Mode	Cisco Server Recovery Manager Take Back Users Failed	Running in Failed Mode	Cisco Server Recovery Manager Take Back Users Failed	User move fails during falling back process. **Recommended Action:** Possible database error. Click **Recovery** in the **Presence Redundancy Group Configuration** window. If the problem persists, then reboot the nodes.
Running in Failed Mode	Unknown	Running in Failed Mode	Unknown	The SRM on a node restarts while the SRM on the other node is in a failed state, or an internal system error occurs. **Recommended Action:** Click **Recovery** in the **Presence Redundancy Group Configuration** window. If the problem persists, then reboot the nodes.
Backup Activated	Auto Recover Database Failure	Failover Affected Services	Auto Recovery Database Failure.	The database goes down on the backup node. The peer node is in failover mode and can take over for all users in the presence redundancy group. Auto-recovery operation automatically occurs and all users are moved over to the primary node.
Backup Activated	Auto Recover Database Failure	Failover Affected Services	Auto Recover Critical Service Down	A critical service goes down on the backup node. The peer node is in failover mode and can take over for all users in the presence redundancy group. Auto-recovery operation automatically occurs and all users are moved over to the peer node.

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Unknown		Unknown		Node state is unknown. A possible cause is that high availability was not enabled properly on the IM and Presence Service node. **Recommended Action:** Restart the Server Recovery Manager service on both nodes in the presence redundancy group.

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

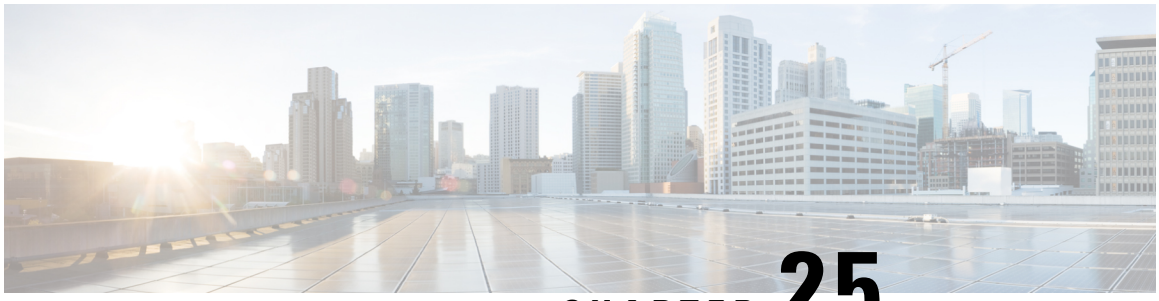
Step 4 After the restart, monitor the number of active sessions on all nodes.

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.



CHAPTER 25

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 User ID assigned to them, then rename the UserID value for one of the users to ensure there is no longer any duplication.
4. If the user information is invalid or empty, proceed to correct the user ID information for that user using the Cisco Unified Communications Manager Administration GUI.
5. You can modify the user records in Cisco Unified Communications Manager using the **End User Configuration** window, (**User Management** > **EndUser**) to ensure that all users have a valid user ID or Directory URI value as necessary. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

Note The user ID and directory URI fields in the user profile may be mapped to the LDAP Directory. In that case, apply the fix in the LDAP Directory server.

6. Run the CLI command to validate users again to ensure that there are no more duplicate user ID errors.

Received Duplicate or Invalid Directory URI Error

Problem I received an alarm indicating that there are duplicate or invalid user Directory URIs and I have to modify the contact information for those users.

Solution Perform the following steps.

1. Use the **utils users validate { all | userid | uri }** CLI command to generate a list of all users. For more information about using the CLI, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

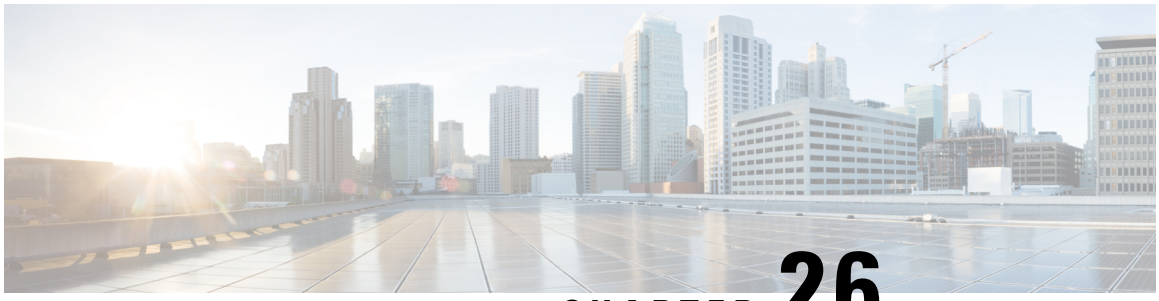
   The Directory URI value is entered in the result set and is followed by the list of servers where the duplicate or invalid Directory URIs are homed. The following sample CLI output shows Directory URI errors detected during a validation check:

```
Users with No Directory URI Configured
--------------------------------------------------
 Node Name: cucm-imp-2
 User ID
 user4

Users with Invalid Directory URI Configured
--------------------------------------------------
 Node Name: cucm-imp-2
 User ID   Directory URI
 user1     asdf@ASDF@asdf@ADSF@cisco

Users with Duplicate Directory URIs
--------------------------------------------------
Directory URI: user1@cisco.com
 Node Name   User ID
 cucm-imp-1  user4
 cucm-imp-2  user3
```

2. If the same user is assigned to two different clusters, then unassign the user from one of the clusters.
3. If different users on different clusters have the same Directory URI value assigned to them, then rename the Directory URI value for one of the users to ensure there is no longer any duplication.
4. If the user information is invalid or empty, proceed to correct the user's Directory URI information.
5. You can modify the user records in Cisco Unified Communications Manager using the **End User Configuration** window, (**User Management** > **EndUser**) to ensure that all users have a valid user ID or Directory URI value as necessary. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

Note The user ID and directory URI fields in the user profile may be mapped to the LDAP Directory. In that case, apply the fix in the LDAP Directory server.

6. Run the CLI command to validate users again to ensure that there are no more duplicate or invalid Directory URI errors.



CHAPTER 26

Traces Used To Troubleshoot 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 susequent 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 39: Common IM and Presence Issue Troubleshooting

Issues with...	View Traces for These Services	Additional Instructions
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 324 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 324 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 324 for CLI commands to build logs and output locations.
Contact Lists	Cisco XCP Connection Manager Cisco XCP Router Cisco Presence Engine	See Common Traces via CLI, on page 324 for CLI commands to build logs and output locations.
Chat Rooms	Cisco XCP Connection Manager Cisco XCP Router Cisco XCP Text Conferencing Manager	See Common Traces via CLI, on page 324 for CLI commands to build logs and output locations.
Partitioned Intradomain Federation	Cisco XCP Router Cisco XCP SIP Federation Connection Manager Cisco SIP Proxy Cisco Presence Engine	See Common Traces via CLI, on page 324 for CLI commands to build logs and output locations. **Note** Cisco SIP Proxy debug logging is required to see the SIP message exchange
Availability and IMs for XMPP Based Interdomain Federation Contact	Cisco XCP Connection Manager Cisco XCP Router Cisco Presence Engine Cisco XCP XMPP Federation Connection Manager	See Common Traces via CLI, on page 324 for CLI commands to build logs and output locations. Perform trace on each IM and Presence node on which XMPP Federation is enabled

Issues with...	View Traces for These Services	Additional Instructions
Availability and IMs for SIP Interdomain Federation Contact	Cisco XCP Connection Manager Cisco XCP Router Cisco Presence Engine Cisco SIP Proxy Cisco XCP SIP Federation Connection Manager	See Common Traces via CLI, on page 324 for CLI commands to build logs and output locations.
Calendaring Traces	Cisco Presence Engine	See Common Traces via CLI, on page 324 for CLI commands to build logs and output locations.
Intercluster Synchronization Traces and Intercluster Troubleshooter	Cisco Intercluster Sync Agent Cisco AXL Web Service Cisco Tomcat Security Log Cisco Syslog Agent	Run the system troubleshooter at **Diagnostics** > **System Troubleshooter** to check for interclustering errors.
SIP Federation Traces	Cisco SIP Proxy Cisco XCP Router Cisco XCP SIP Federation Connection Manager	See Common Traces via CLI, on page 324 for CLI commands to build logs and file output locations.
XMPP Federation Traces	Cisco XCP Router Cisco XCP XMPP Federation Connection Manager	See Common Traces via CLI, on page 324 for CLI commands to build logs and file output locations.

Issues with...	View Traces for These Services	Additional Instructions
High CPU and Low VM Alert Troubleshooting	Cisco XCP Router Cisco XCP SIP Federation Connection Manager Cisco SIP Proxy Cisco Presence Engine Cisco Tomcat Security Log Cisco Syslog Agent	For additional troubleshooting, run the following CLI commands: • `show process using-most cpu` • `show process using-most memory` • `utils dbreplication runtimestate` • `utils service list` Run the following CLI to get RIS (Real-Time Information Service) data: • `file get activelog cm/log/ris/csv` 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.

Common Traces via CLI

Use the Command Line Interface to build trace log files to troubleshoot your system. With the CLI, you can choose the component for which you want to run a trace and specify the <duration>, which is the number of days looking backwards from today that you want to include in your log file.

The following two tables contain the CLI commands that you can use to build trace log files and the log output locations for:

- IM and Presence Services
- IM and Presence Features

Note 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 328.

Table 40: Common Traces for IM and Presence Services using CLI

Service	CLI to Build Log	CLI Output File
Cisco Audit Logs	file build log cisco_audit_logs <duration>	/epas/trace/log_cisco_audit_logs_*.tar.gz
Cisco Client Profile Agent	file build log cisco_client_profile_agent <duration>	/epas/trace/log_cisco_client_profile_agent_*.tar.gz
Cisco Cluster Manager	file build log cisco_config_agent <duration>	/epas/trace/log_cisco_cluster_manager_*.tar.gz
Cisco Config Agent	file build log cisco_config_agent<duration>	/epas/trace/log_cisco_config_agent_*.tar.gz
Cisco Database Layer Monitor	file build log cisco_database_layer_monitor <duration>	/epas/trace/log_cisco_database_layer_monitor_*.tar.gz
Cisco Intercluster Sync Agent	file build log cisco_inter_cluster_sync_agent <duration>	/epas/trace/log_cisco_inter_cluster_sync_agent_*.tar.gz
Cisco OAM Agent	file build log cisco_oam_agent <duration>	/epas/trace/log_cisco_oam_agent_*.gz
Cisco Presence Engine	file build log cisco_presence_engine <duration>	/epas/trace/log_cisco_presence_engine_*.tar.gz
Cisco RIS (Real-time Information Service) Data Collector	file build log cisco_ris_data_collector <duration>	/epas/trace/log_cisco_ris_data_collector_*.tar.gz
Cisco Service Management	file build log cisco_service_management <duration>	/epas/trace/log_cisco_service_management_*.tar.gz
Cisco SIP Proxy	file build log cisco_sip_proxy <duration>	/epas/trace/log_cisco_sip_proxy_*.tar.gz
Cisco Sync Agent	file build log cisco_sync_agent <duration>	/epas/trace/log_cisco_sync_agent_*.tar.gz
Cisco XCP Config Manager	file build log cisco_xcp_config_mgr <duration>	/epas/trace/log_cisco_xcp_config_mgr_*.tar.gz
Cisco XCP Router	file build log cisco_xcp_router <duration>	/epas/trace/log_cisco_xcp_router_*.tar.gz

Table 41: Common Traces for IM and Presence Features using CLI

Feature Name	CLI to Build Log	CLI Output File
Administration GUI	file build log admin_ui <duration>	/epas/trace/log_admin_ui_*.tar.gz
Bulk Administration	file build log bat <duration>	/epas/trace/log_bat_*.tar.gz
Bidirectional Streams over Synchronous HTTP	file build log bosh <duration>	/epas/trace/log_bosh_*.tar.gz
Certificates	file build log certificates <duration>	/epas/trace/log_certificates_*.tar.gz
Config Agent Core	file build log cfg_agent_core <duration>	/epas/trace/log_cfg_agent_core_*.tar.gz
Customer Voice Portal	file build log cvp <duration>	/epas/trace/log_cvp_*.tar.gz
Directory Groups	file build log directory_groups <duration>	/epas/trace/log_directory_groups_*.tar.gz
Disaster Recovery	file build log disaster_recovery <duration>	/epas/trace/log_disaster_recovery_*.tar.gz
Flexible IM address	file build log flexable_im_address <duration>	/epas/trace/log_flexible_im_address_*.tar.gz
General core	file build log general_core <duration>	/epas/trace/log_general_core_*.tar.gz
High Availability	file build log ha <duration>	/epas/trace/log_ha_*.tar.gz
High CPU	file build log high_cpu <duration>	/epas/trace/log_high_cpu_*.tar.gz
High Memory	file build log high_memory <duration>	/epas/trace/log_high_memory_*.tar.gz
Instant Messaging Database Core	file build log imdb <duration>	/epas/trace/log_imdb_core_*.tar.gz
Intercluster Peering	file build log inter_cluster <duration>	/epas/trace/log_inter_cluster_*.tar.gz
Managed File Transfer	file build log managed_file_transfer <duration>	/epas/trace/log_managed_file_transfer_*.tar.gz
Microsoft Exchange	file build log msft_exchange <duration>	/epas/trace/log_msft_exchange_*.tar.gz
Message Archiver	file build log msg_archiver <duration>	/epas/trace/log_msg_archiver_*.tar.gz

Feature Name	CLI to Build Log	CLI Output File
Presence Engine Core	file build log pe_core <duration>	/epas/trace/log_pe_core_*.tar.gz
Presence and IM Message Exchange	file build log presence_im_exchange <duration>	/epas/trace/log_presence_im_exchange_*.tar.gz
SIP Login Issues	file build log pws <duration>	/epas/trace/log_pws_*.tar.gz
Remote Call Control	file build log remote_call_control <duration>	/epas/trace/log_remote_call_control_*.tar.gz
Security Vulnerabilities	file build log sec_vulnerability <duration>	/epas/trace/log_sec_vulnerability_*.tar.gz
Serviceability GUI	file build log serviceability_ui <duration>	/epas/trace/log_serviceability_ui_*.tar.gz
SIP Interdomain Federation	file build log sip_inter_federation <duration>	/epas/trace/log_sip_inter_federation_*.tar.gz
SIP Partitioned Intradomain Federation	file build log sip_partitioned_federation <duration>	/epas/trace/log_sip_partitioned_federation_*.tar.gz
SIP Proxy Core	file build log sipd_core <duration>	/epas/trace/log_sipd_core_*.tar.gz
Persistent Chat High Availability	file build log tc_ha <duration>	/epas/trace/log_tc_ha_*.tar.gz
Persistent Chat	file build log text_conference <duration>	/epas/trace/log_text_conference_*.tar.gz
Upgrade Issues	file build log upgrade_issues <duration>	/epas/trace/log_upgrade_issues_*.tar.gz
User Connectivity	file build log user_connectivity <duration>	/epas/trace/log_user_connectivity_*.tar.gz
Rosters	file build log user_rosters <duration>	/epas/trace/log_user_rosters_*.tar.gz
XCP Router Core	file build log xcp_core <duration>	/epas/trace/log_xcp_core_*.tar.gz
XMPP Interdomain Federation	file build log xmpp_inter_federation <duration>	/epas/trace/log_xmpp_inter_federation_*.tar.gz
Deployment Info	file build log deployment_info <duration>	/epas/trace/log_deployment_info_*.tar.gz

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 324 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`.

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).

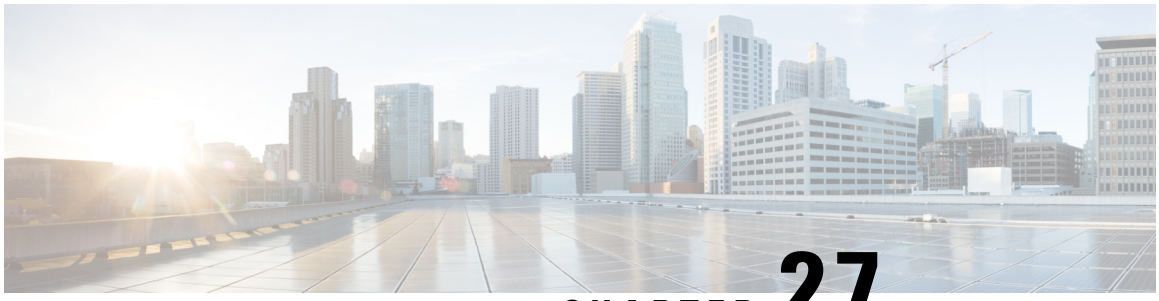
Note The CLI can be used to pull a subset of the same individual traces files that you can view with RTMT, but groups and stores them in a single compressed zip file. For CLI traces, see Common Traces via CLI, on page 324.

Table 42: Common Traces and Log Files for IM and Presence Nodes

Service	Trace Log Filename
Cisco AXL Web Services	/tomcat/logs/axl/log4j/axl*.log
Cisco Intercluster Sync Agent	/epas/trace/cupicsa/log4j/icSyncAgent*.log
Cisco Presence Engine	/epas/trace/epe/sdi/epe*.txt.gz
Cisco SIP Proxy	/epas/trace/esp/sdi/esp*.txt.gz
Cisco Syslog Agent	/cm/trace/syslogmib/sdi/syslogmib*.txt
Cisco Tomcat Security Log	/tomcat/logs/security/log4/security*.log
Cisco XCP Authentication Service	/epas/trace/xcp/log/auth-svc-1*.log.gz
Cisco XCP Config Manager	/epas/trace/xcpconfigmgr/log4j/xcpconfigmgr*.log
Cisco XCP Connection Manager	/epas/trace/xcp/log/client-cm-1*.log.gz
Cisco XCP Router	/epas/trace/xcp/log/rtr-jsm-1*.log.gz
Cisco XCP SIP Federation Connection Manager	/epas/trace/xcp/log/sip-cm-3*.log
Cisco XCP Text Conferencing Manager	/epas/trace/xcp/log/txt-conf-1*.log.gz
Cisco XCP XMPP Federation Connection Manager	/epas/trace/xcp/log/xmpp-cm-4*.log
Cluster Manager	/platform/log/clustermgr*.log
Cisco Client Profile Agent (CPA)	/tomcat/logs/epassoap/log4j/EPASSoap*.log
dbmon	/cm/trace/dbl/sdi/dbmon*.txt

PART VI

Reference Information



CHAPTER 27

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

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.

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.

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.

Note 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.

Note The ephemeral port range for the system is 32768 to 61000, and the ports needs to be open to keep the phones registered. 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.

Note 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

Table 43: Intracluster Ports Between Cisco Unified Communications Manager Servers

From (Sender)	To (Listener)	Destination Port	Purpose
Endpoint	Unified Communications Manager	514 / UDP	System logging service
Unified Communications Manager	RTMT	1090, 1099 / TCP	Cisco AMC Service for RTMT performance monitors, data collection, logging, and alerting
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1500, 1501 / TCP	Database connection (1501 / TCP is the secondary connection)
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1510 / TCP	CAR IDS DB. CAR IDS engine listens on waiting for connection requests from the clients.
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1511 / TCP	CAR IDS DB. An alternate port used to bring up a second instance of CAR IDS during upgrade.
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1515 / TCP	Database replication between nodes during installation
Cisco Extended Functions (QRT)	Unified Communications Manager (DB)	2552 / TCP	Allows subscribers to receive Cisco Unified Communications Manager database change notification
Unified Communications Manager	Unified Communications Manager	2551 / TCP	Intracluster communication between Cisco Extended Services for Active/Backup determination
Unified Communications Manager (RIS)	Unified Communications Manager (RIS)	2555 / TCP	Real-time Information Services (RIS) database server

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager (RTMT/AMC/SOAP)	Unified Communications Manager (RIS)	2556 / TCP	Real-time Information Services (RIS) database client for Cisco RIS
Unified Communications Manager (DRS)	Unified Communications Manager (DRS)	4040 / TCP	DRS Primary Agent
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5001/TCP	This port is used by SOAP monitor for Real Time Monitoring Service.
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5002/TCP	This port is used by SOAP monitor for Performance Monitor Service.
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5003/TCP	This port is used by SOAP monitor for Control Center Service.
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5004/TCP	This port is used by SOAP monitor for Log Collection Service.
Standard CCM Admin Users / Admin	Unified Communications Manager	5005 / TCP	This port is used by SOAP CDROnDemand2 services
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5007 / TCP	SOAP monitor
Unified Communications Manager (RTMT)	Unified Communications Manager (TCTS)	Ephemeral / TCP	Cisco Trace Collection Tool Service (TCTS) -- the back end service for RTMT Trace and Log Central (TLC)
Unified Communications Manager (Tomcat)	Unified Communications Manager (TCTS)	7000, 7001, 7002 / TCP	This port is used for communication between Cisco Trace Collection Tool Service and Cisco Trace Collection servlet.
Unified Communications Manager (DB)	Unified Communications Manager (CDLM)	8001 / TCP	Client database change notification
Unified Communications Manager (SDL)	Unified Communications Manager (SDL)	8002 / TCP	Intracluster communication service
Unified Communications Manager (SDL)	Unified Communications Manager (SDL)	8003 / TCP	Intracluster communication service (to CTI)

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager	CMI Manager	8004 / TCP	Intracluster communication between Cisco Unified Communications Manager and CMI Manager
Unified Communications Manager (Tomcat)	Unified Communications Manager (Tomcat)	8005 / TCP	Internal listening port used by Tomcat shutdown scripts
Unified Communications Manager (Tomcat)	Unified Communications Manager (Tomcat)	8080 / TCP	Communication between servers used for diagnostic tests
Gateway	Unified Communications Manager	8090	HTTP Port for communication between CuCM and GW (Cayuga interfae) for Gateway Recording feature.
Unified Communications Manager	Gateway		
Unified Communications Manager (IPSec)	Unified Communications Manager (IPSec)	8500 / TCP and UDP	Intracluster replication of system data by IPSec Cluster Manager
Unified Communications Manager (RIS)	Unified Communications Manager (RIS)	8888 - 8889 / TCP	RIS Service Manager status request and reply
Location Bandwidth Manager (LBM)	Location Bandwidth Manager (LBM)	9004 / TCP	Intracluster communication between LBMs
Unified Communications Manager Publisher	Unified Communications Manager Subscriber	22 / TCP	Cisco SFTP service. You must open this port when installing a new subscriber.
Unified Communications Manager	Unified Communications Manager	8443 / TCP	Allows access to Control Center - Feature and Network service between nodes.

Common Service Ports

Table 44: Common Service Ports

From (Sender)	To (Listener)	Destination Port	Purpose
Endpoint	Unified Communications Manager	7	Internet Control Message Protocol (ICMP) This protocol number carries echo-related traffic. It does not constitute a port as indicated in the column heading.
Unified Communications Manager	Endpoint		
Unified Communications Manager (DRS, CDR)	SFTP server	22 / TCP	Send the backup data to SFTP server. (DRS Local Agent) Send the CDR data to SFTP server.
Endpoint	Unified Communications Manager (DHCP Server)	67 / UDP	Cisco Unified Communications Manager acting as a DHCP server **Note** Cisco does not recommend running DHCP server on Cisco Unified Communications Manager.
Unified Communications Manager	DHCP Server	68 / UDP	Cisco Unified Communications Manager acting as a DHCP client **Note** Cisco does not recommend running DHCP client on Cisco Unified Communications Manager. Configure Cisco Unified Communications Manager with static IP addresses instead.)

From (Sender)	To (Listener)	Destination Port	Purpose
Endpoint or Gateway	Unified Communications Manager	69, 6969, then Ephemeral / UDP	Trivial File Transfer Protocol (TFTP) service to phones and gateways
Endpoint or Gateway	Unified Communications Manager	6970 / TCP	Trivial File Transfer Protocol (TFTP) between primary and proxy servers. HTTP service from the TFTP server to phones and gateways.
Unified Communications Manager	NTP Server	123 / UDP	Network Time Protocol (NTP)
SNMP Server	Unified Communications Manager	161 / UDP	SNMP service response (requests from management applications)
CUCM Server SNMP Primary Agent application	SNMP trap destination	162 / UDP	SNMP traps
SNMP Server	Unified Communications Manager	199 / TCP	Native SNMP agent listening port for SMUX support
Unified Communications Manager	DHCP Server	546 / UDP	DHCPv6. DHCP port for IPv6.
Unified Communications Manager Serviceability	Location Bandwidth Manager (LBM)	5546 / TCP	Enhanced Location CAC Serviceability
Unified Communications Manager	Location Bandwidth Manager (LBM)	5547 / TCP	Call Admission requests and bandwidth deductions
Unified Communications Manager	Unified Communications Manager	6161 / UDP	Used for communication between Primary Agent and Native Agent to process Native agent MIB requests
Unified Communications Manager	Unified Communications Manager	6162 / UDP	Used for communication between Primary Agent and Native Agent to forward notifications generated from Native Agent
Centralized TFTP	Alternate TFTP	6970 / TCP	Centralized TFTP File Locator Service

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager	Unified Communications Manager	7161 / TCP	Used for communication between SNMP Primary Agent and subagents
SNMP Server	Unified Communications Manager	7999 / TCP	Cisco Discovery Protocol (CDP) agent communicates with CDP executable
Endpoint	Unified Communications Manager	443, 8443 / TCP	Used for Cisco User Data Services (UDS) requests
Unified Communications Manager	Unified Communications Manager	9050 / TCP	Service CRS requests through the TAPS residing on Cisco Unified Communications Manager
Unified Communications Manager	Unified Communications Manager	61441 / UDP	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.
Unified Communications Manager	Unified Communications Manager	5060, 5061 / TCP	Provide trunk-based SIP services
Unified Communications Manager	Unified Communications Manager	7501	Used by Intercluster Lookup Service (ILS) for certificate based authentication.
Unified Communications Manager	Unified Communications Manager	7502	Used by ILS for password based authentication.
--	--	8000-48200	ASR and ISR G3 platforms default port range.
		16384-32766	ISR G2 platform default port range.

Ports Between Cisco Unified Communications Manager and LDAP Directory

Table 45: Ports Between Cisco Unified Communications Manager and LDAP Directory

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager	External Directory	389, 636, 3268, 3269 / TCP	Lightweight Directory Access Protocol (LDAP) query to external directory (Active Directory, Netscape Directory)
External Directory	Unified Communications Manager	Ephemeral	

Web Requests From CCMAdmin or CCMUser to Cisco Unified Communications Manager

Table 46: Web Requests From CCMAdmin or CCMUser to Cisco Unified Communications Manager

From (Sender)	To (Listener)	Destination Port	Purpose
Browser	Unified Communications Manager	80, 8080 / TCP	Hypertext Transport Protocol (HTTP)
Browser	Unified Communications Manager	443, 8443 / TCP	Hypertext Transport Protocol over SSL (HTTPS)

Web Requests From Cisco Unified Communications Manager to Phone

Table 47: Web Requests From Cisco Unified Communications Manager to Phone

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager • QRT • RTMT • Find and List Phones page • Phone Configuration page	Phone	80 / TCP	Hypertext Transport Protocol (HTTP)

Signaling, Media, and Other Communication Between Phones and Cisco Unified Communications Manager

Table 48: Signaling, Media, and Other Communication Between Phones and Cisco Unified Communications Manager

From (Sender)	To (Listener)	Destination Port	Purpose
Phone	Unified Communications Manager	53/ TCP	Session Initiation Protocol (SIP) phones resolve the Fully Qualified Domain Name (FQDN) using a Domain Name System (DNS) **Note** By default, some wireless access points block TCP 53 port, which prevents wireless SIP phones from registering when CUCM is configured using FQDN.
Phone	Unified Communications Manager (TFTP)	69, then Ephemeral / UDP	Trivial File Transfer Protocol (TFTP) used to download firmware and configuration files
Phone	Unified Communications Manager	2000 / TCP	Skinny Client Control Protocol (SCCP)
Phone	Unified Communications Manager	2443 / TCP	Secure Skinny Client Control Protocol (SCCPS)
Phone	Unified Communications Manager	2445 / TCP	Provide trust verification service to endpoints.
Phone	Unified Communications Manager (CAPF)	3804 / TCP	Certificate Authority Proxy Function (CAPF) listening port for issuing Locally Significant Certificates (LSCs) to IP phones

From (Sender)	To (Listener)	Destination Port	Purpose
Phone	Unified Communications Manager	5060 / TCP and UDP	Session Initiation Protocol (SIP) phone
Unified Communications Manager	Phone		
Phone	Unified Communications Manager	5061 TCP	Secure Session Initiation Protocol (SIPS) phone
Unified Communications Manager	Phone		
Phone	Unified Communications Manager (TFTP)	6970 TCP	HTTP-based download of firmware and configuration files
Phone	Unified Communications Manager (TFTP)	6971, 6972 / TCP	HTTPS interface to TFTP. Phones use this port to download a secure configuration file from TFTP.
Phone	Unified Communications Manager	8080 / TCP	Phone URLs for XML applications, authentication, directories, services, etc. You can configure these ports on a per-service basis.
Phone	Unified Communications Manager	9443 / TCP	Phone use this port for authenticated contact search.
Phone	Unified Communications Manager	9444	
IP VMS	Phone	16384 - 32767 / UDP	Real-Time Protocol (RTP), Secure Real-Time Protocol (SRTP) **Note** Cisco Unified Communications Manager only uses 24576-32767 although other devices use the full range.
Phone	IP VMS		

Signaling, Media, and Other Communication Between Gateways and Cisco Unified Communications Manager

Table 49: Signaling, Media, and Other Communication Between Gateways and Cisco Unified Communications Manager

From (Sender)	To (Listener)	Destination Port	Purpose
Gateway	Unified Communications Manager	47, 50, 51	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.
Unified Communications Manager	Gateway		
Gateway	Unified Communications Manager	500 / UDP	Internet Key Exchange (IKE) for IP Security protocol (IPSec) establishment
Unified Communications Manager	Gateway		
Gateway	Unified Communications Manager (TFTP)	69, then Ephemeral / UDP	Trivial File Transfer Protocol (TFTP)
Unified Communications Manager with Cisco Intercompany Media Engine (CIME) trunk	CIME ASA	1024-65535 / TCP	Port mapping service. Only used in the CIME off-path deployment model.
Gatekeeper	Unified Communications Manager	1719 / UDP	Gatekeeper (H.225) RAS
Gateway	Unified Communications Manager	1720 / TCP	H.225 signaling services for H.323 gateways and Intercluster Trunk (ICT)
Unified Communications Manager	Gateway		
Gateway	Unified Communications Manager	Ephemeral / TCP	H.225 signaling services on gatekeeper-controlled trunk
Unified Communications Manager	Gateway		

From (Sender)	To (Listener)	Destination Port	Purpose
Gateway	Unified Communications Manager	Ephemeral / TCP	H.245 signaling services for establishing voice, video, and data **Note** The H.245 port used by the remote system depends on the type of gateway. For IOS gateways, the H.245 port range is from 11000 to 65535.
Unified Communications Manager	Gateway		
Gateway	Unified Communications Manager	2000 / TCP	Skinny Client Control Protocol (SCCP)
Gateway	Unified Communications Manager	2001 / TCP	Upgrade port for 6608 gateways with Cisco Unified Communications Manager deployments
Gateway	Unified Communications Manager	2002 / TCP	Upgrade port for 6624 gateways with Cisco Unified Communications Manager deployments
Gateway	Unified Communications Manager	2427 / UDP	Media Gateway Control Protocol (MGCP) gateway control
Gateway	Unified Communications Manager	2428 / TCP	Media Gateway Control Protocol (MGCP) backhaul
--	--	4000 - 4005 / TCP	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.

From (Sender)	To (Listener)	Destination Port	Purpose
Gateway	Unified Communications Manager	5060 / TCP and UDP	Session Initiation Protocol (SIP) gateway and Intercluster Trunk (ICT)
Unified Communications Manager	Gateway		
Gateway	Unified Communications Manager	5061 / TCP	Secure Session Initiation Protocol (SIPS) gateway and Intercluster Trunk (ICT)
Unified Communications Manager	Gateway		
Gateway	Unified Communications Manager	16384 - 32767 / UDP	Real-Time Protocol (RTP), Secure Real-Time Protocol (SRTP) **Note** Cisco Unified Communications Manager only uses 24576-32767 although other devices use the full range.
Unified Communications Manager	Gateway		

Communication Between Applications and Cisco Unified Communications Manager

Table 50: Communication Between Applications and Cisco Unified Communications Manager

From (Sender)	To (Listener)	Destination Port	Purpose
CTL Client	Unified Communications Manager CTL Provider	2444 / TCP	Certificate Trust List (CTL) provider listening service in Cisco Unified Communications Manager
Cisco Unified Communications App	Unified Communications Manager	2748 / TCP	CTI application server
Cisco Unified Communications App	Unified Communications Manager	2749 / TCP	TLS connection between CTI applications (JTAPI/TSP) and CTIManager
Cisco Unified Communications App	Unified Communications Manager	2789 / TCP	JTAPI application server

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager Assistant Console	Unified Communications Manager	2912 / TCP	Cisco Unified Communications Manager Assistant server (formerly IPMA)
Unified Communications Manager Attendant Console	Unified Communications Manager	1103 -1129 / TCP	Cisco Unified Communications Manager Attendant Console (AC) JAVA RMI Registry server
Unified Communications Manager Attendant Console	Unified Communications Manager	1101 / TCP	RMI server sends RMI callback messages to clients on these ports.
Unified Communications Manager Attendant Console	Unified Communications Manager	1102 / TCP	Attendant Console (AC) RMI server bind port -- RMI server sends RMI messages on these ports.
Unified Communications Manager Attendant Console	Unified Communications Manager	3223 / UDP	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.
Unified Communications Manager Attendant Console	Unified Communications Manager	3224 / UDP	Cisco Unified Communications Manager Attendant Console (AC) clients register with the AC server for line and device state information.
Unified Communications ManagerAttendant Console	Unified Communications Manager	4321 / UDP	Cisco Unified Communications Manager Attendant Console (AC) clients register to the AC server for call control.
Unified Communications Manager with SAF/CCD	IOS Router running SAF image	5050 / TCP	Multi-Service IOS Router running EIGRP/SAF Protocol.

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager	Cisco Intercompany Media Engine (IME) Server	5620 / TCP Cisco recommends a value of 5620 for this port, but you can change the value by executing the add ime vapserver or set ime vapserver port CLI command on the Cisco IME server.	VAP protocol used to communicate to the Cisco Intercompany Media Engine server.
Cisco Unified Communications App	Unified Communications Manager	8443 / TCP	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.

Communication Between CTL Client and Firewalls

Table 51: Communication Between CTL Client and Firewalls

From (Sender)	To (Listener)	Destination Port	Purpose
CTL Client	TLS Proxy Server	2444 / TCP	Certificate Trust List (CTL) provider listening service in an ASA firewall

Special Ports on HP Servers

Table 52: Special Ports on HP Servers

From (Sender)	To (Listener)	Destination Port	Purpose
Endpoint	HP SIM	2301 / TCP	HTTP port to HP agent
Endpoint	HP SIM	2381 / TCP	HTTPS port to HP agent
Endpoint	Compaq Management Agent	25375, 25376, 25393 / UDP	COMPAQ Management Agent extension (cmaX)
Endpoint	HP SIM	50000 - 50004 / TCP	HTTPS port to HP SIM

Port References

Firewall Application Inspection Guides

ASA Series reference information

http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html

PIX Application Inspection Configuration Guides

http://www.cisco.com/c/en/us/support/security/pix-firewall-software/products-installation-and-configuration-guides-list.html

FWSM 3.1 Application Inspection Configuration Guide

http://www-author.cisco.com/c/en/us/td/docs/security/fwsm/fwsm31/configuration/guide/fwsm_cfg/inspct_f.html

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

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Port Utilization Guide for Cisco ICM/IPCC Enterprise and Hosted Editions

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html

Cisco Unified Communications Manager Express Security Guide to Best Practices

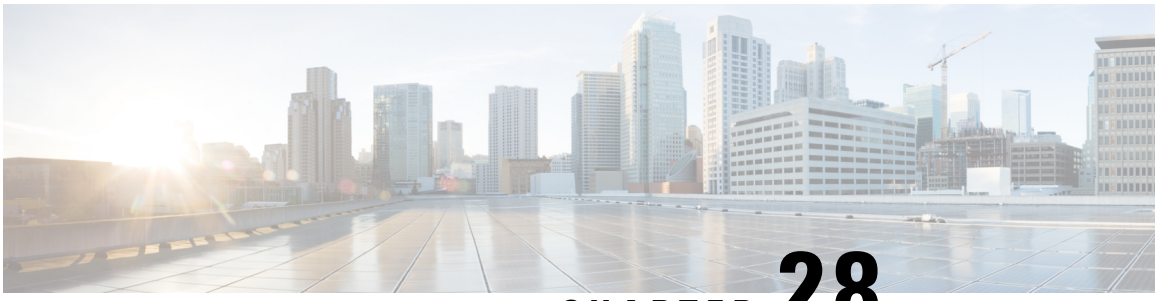
http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e30.html

Cisco Unity Express Security Guide to Best Practices

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e31.html#wp41149

VMware Port Assignment List

TCP and UDP Ports for vCenter Server, ESX hosts, and Other Network Components Management Access



CHAPTER 28

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 53: Definition of Table Information

Table Heading	Description
From	The client sending requests to this port
To	The client receiving requests on this port
Role	A client or server application or process
Protocol	Either a Session-layer protocol used for establishing and ending communications, or an Application-layer protocol used for request and response transactions
Transport Protocol	A Transport-layer protocol that is connection-oriented (TCP) or connectionless (UDP)
Destination / Listener	The port used for receiving requests
Source / Sender	The port used for sending requests

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 54: IM and Presence Service Ports - SIP Proxy Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
SIP Gateway --- IM and Presence	IM and Presence --- SIP Gateway	SIP	TCP/UDP	5060	Ephemeral	Default SIP Proxy UDP and TCP Listener
SIP Gateway	IM and Presence	SIP	TLS	5061	Ephemeral	TLS Server Authentication listener port
IM and Presence	IM and Presence	SIP	TLS	5062	Ephemeral	TLS Mutual Authentication listener port
IM and Presence	IM and Presence	SIP	UDP / TCP	5049	Ephemeral	Internal port. Localhost traffic only.
IM and Presence	IM and Presence	HTTP	TCP	8081	Ephemeral	Used for HTTP requests from the Config Agent to indicate a change in configuration.

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
Third-party Client	IM and Presence	HTTP	TCP	8082	Ephemeral	Default IM and Presence HTTP Listener. Used for Third-Party Clients to connect
Third-party Client	IM and Presence	HTTPS	TLS / TCP	8083	Ephemeral	Default IM and Presence HTTPS Listener. Used for Third-Party Clients to connect

Table 55: IM and Presence Service Ports - Presence Engine Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	IM and Presence (Presence Engine)	SIP	UDP / TCP	5080	Ephemeral	Default SIP UDP/TCP Listener port
IM and Presence (Presence Engine)	IM and Presence (Presence Engine)	Livebus	UDP	50000	Ephemeral	Internal port. Localhost traffic only. LiveBus messaging port. The IM and Presence Service uses this port for cluster communication.

Table 56: IM and Presence Service Ports - Cisco Tomcat WebRequests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
Browser	IM and Presence	HTTPS	TCP	8080	Ephemeral	Used for web access
Browser	IM and Presence	AXL / HTTPS	TLS / TCP	8443	Ephemeral	Provides database and serviceability access via SOAP
Browser	IM and Presence	HTTPS	TLS / TCP	8443	Ephemeral	Provides access to Web administration
Browser	IM and Presence	HTTPS	TLS / TCP	8443	Ephemeral	Provides access to User option pages

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
Browser	IM and Presence	SOAP	TLS / TCP	8443	Ephemeral	Provides access to Cisco Unified Personal Communicator, Cisco Unified Mobility Advantage, and third-party API clients via SOAP

Table 57: IM and Presence Service Ports - External Corporate Directory Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence --- External Corporate Directory	External Corporate Directory --- IM and Presence	LDAP	TCP	389 / 3268	Ephemeral	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&P and the LDAP server for authentication.
IM and Presence	External Corporate Directory	LDAPS	TCP	636	Ephemeral	Allows the Directory protocol to integrate with the external Corporate Directory. LDAP port depends on the Corporate Directory (636 is the default).

Table 58: IM and Presence Service Ports - Configuration Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence (Config Agent)	IM and Presence (Config Agent)	TCP	TCP	8600	Ephemeral	Config Agent heartbeat port

Table 59: IM and Presence Service Ports - Certificate Manager Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	Certificate Manager	TCP	TCP	7070	Ephemeral	Internal port - Localhost traffic only

Table 60: IM and Presence Service Ports - IDS Database Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence (Database)	IM and Presence (Database)	TCP	TCP	1500	Ephemeral	Internal IDS port for Database clients. Localhost traffic only.
IM and Presence (Database)	IM and Presence (Database)	TCP	TCP	1501	Ephemeral	Internal port - this is an alternate port to bring up a second instance of IDS during upgrade. Localhost traffic only.
IM and Presence (Database)	IM and Presence (Database)	XML	TCP	1515	Ephemeral	Internal port. Localhost traffic only. DB replication port

Table 61: IM and Presence Service Ports - IPSec Manager Request

From Sender	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence (IPSec)	IM and Presence (IPSec)	Proprietary	UDP/TCP	8500	8500	Internal port - cluster manager port used by the ipsec_mgr daemon for cluster replication of platform data (hosts) certs

Table 62: IM and Presence Service Ports - DRF Master Agent Server Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence (DRF)	IM and Presence (DRF)	TCP	TCP	4040	Ephemeral	DRF Master Agent server port, which accepts connections from Local Agent, GUI, and CLI

Table 63: IM and Presence Service Ports - RISDC Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence (RIS)	IM and Presence (RIS)	TCP	TCP	2555	Ephemeral	Real-time Information Services (RIS) database server. Connects to other RISDC services in the cluster to provide clusterwide real-time information
IM and Presence (RTMT/AMC/ SOAP)	IM and Presence (RIS)	TCP	TCP	2556	Ephemeral	Real-time Information Services (RIS) database client for Cisco RIS. Allows RIS client connection to retrieve real-time information
IM and Presence (RIS)	IM and Presence (RIS)	TCP	TCP	8889	8888	Internal port. Localhost traffic only. Used by RISDC (System Access) to link to servM via TCP for service status request and reply

Table 64: IM and Presence Service Ports - SNMP Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
SNMP Server	IM and Presence	SNMP	UDP	161, 8161	Ephemeral	Provides services for SNMP-based management applications
IM and Presence	IM and Presence	SNMP	UDP	6162	Ephemeral	Native SNMP agent that listens for requests forwarded by SNMP master agents
IM and Presence	IM and Presence	SNMP	UDP	6161	Ephemeral	SNMP Master agent that listens for traps from the native SNMP agent, and forwards to management applications
SNMP Server	IM and Presence	TCP	TCP	7999	Ephemeral	Used as a socket for the cdp agent to communicate with the cdp binary

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	IM and Presence	TCP	TCP	7161	Ephemeral	Used for communication between the SNMP Master agent and subagents
IM and Presence	SNMP Trap Monitor	SNMP	UDP	162	Ephemeral	Sends SNMP traps to management applications
IM and Presence	IM and Presence	SNMP	UDP	Configurable	61441	Internal SNMP trap receiver

Table 65: IM and Presence Service Ports - Racoon Server Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
Gateway --- IM and Presence	IM and Presence --- Gateway	Ipsec	UDP	500	Ephemeral	Enables Internet Security Association and the Key Management Protocol

Table 66: IM and Presence Service Ports - System Service Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence (RIS)	IM and Presence (RIS)	XML	TCP	8888 and 8889	Ephemeral	Internal port. Localhost traffic only. Used to listen to clients communicating with the RIS Service Manager (servM).

Table 67: IM and Presence Service Ports - DNS Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	DNS Server	DNS	UDP	53	Ephemeral	The port that DNS server listen on for IM and Presence DNS queries. To: DNS Server | From: IM and Presence

Table 68: IM and Presence Service Ports - SSH/SFTP Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	Endpoint	SSH / SFTP	TCP	22	Ephemeral	Used by many applications to get command line access to the server. Also used between nodes for certificate and other file exchanges (sftp)

Table 69: IM and Presence Service Ports - ICMP Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence --- Cisco Unified Communications Manager	Cisco Unified Communications Manager --- IM and Presence	ICMP	IP	Not Applicable	Ephemeral	Internet Control Message Protocol (ICMP). Used to communicate with the Cisco Unified Communications Manager server

Table 70: IM and Presence Service Ports - NTP Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	NTP Server	NTP	UDP	123	Ephemeral	Cisco Unified Communications Manager is the acting NTP server. Used by subscriber nodes to synchronize time with the publisher node.

Table 71: IM and Presence Service Ports - Microsoft Exchange Notify Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
Microsoft Exchange	IM and Presence	HTTP (HTTPu)	) WebDAV - HTTP /UDP/IP notifications 2) EWS - HTTP/TCP /IP SOAP notifications	IM and Presence server port (default 50020)	Ephemeral	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.

Table 72: IM and Presence Service Ports - SOAP Services Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence (Tomcat)	IM and Presence (SOAP)	TCP	TCP	5007	Ephemeral	SOAP monitor port

Table 73: IM and Presence Service Ports - AMC RMI Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	RTMT	TCP	TCP	1090	Ephemeral	AMC RMI Object port. Cisco AMC Service for RTMT performance monitors, data collection, logging, and alerting.
IM and Presence	RTMT	TCP	TCP	1099	Ephemeral	AMC RMI Registry port. Cisco AMC Service for RTMT performance monitors, data collection, logging, and alerting.

Table 74: IM and Presence Service Ports - XCP Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
XMPP Client	IM and Presence	TCP	TCP	5222	Ephemeral	Client access port
IM and Presence	IM and Presence	TCP	TCP	5269	Ephemeral	Server to Server connection (S2S) port
Third-party BOSH client	IM and Presence	TCP	TCP	7335	Ephemeral	HTTP listening port used by the XCP Web Connection Manager for BOSH third-party API connections
IM and Presence (XCP Services)	IM and Presence (XCP Router	TCP	TCP	7400	Ephemeral	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.
IM and Presence (XCP Router	IM and Presence (XCP Router	UDP	UDP	5353	Ephemeral	MDNS port. XCP routers in a cluster use this port to discover each other.
IM and Presence (XCP Router	IM and Presence (XCP Router	TCP	TCP	7336	HTTPS	MFT File transfer (On-Premises only).

Table 75: IM and Presence Service Ports - External Database (PostgreSQL) Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	PostgreSQL database	TCP	TCP	5432[2]	Ephemeral	PostgreSQL database listening port

[2] This is the default port, however you can configure the PostgreSQL database to listen on any port.

Table 76: IM and Presence Service Ports - High Availability Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence (Server Recovery Manager)	IM and Presence (Server Recovery Manager)	TCP	TCP	20075	Ephemeral	The port that Cisco Server Recovery Manager uses to provide admin rpc requests.
IM and Presence (Server Recovery Manager)	IM and Presence (Server Recovery Manager)	UDP	UDP	21999	Ephemeral	The port that Cisco Server Recovery Manager uses to communicate with its peer.

Table 77: IM and Presence Service Ports - In Memory Database Replication Messages

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	IM and Presence	Proprietary	TCP	6603*	Ephemeral	Cisco Presence Datastore
IM and Presence	IM and Presence	Proprietary	TCP	6604*	Ephemeral	Cisco Login Datastore
IM and Presence	IM and Presence	Proprietary	TCP	6605*	Ephemeral	Cisco SIP Registration Datastore
IM and Presence	IM and Presence	Proprietary	TCP	9003	Ephemeral	Cisco Presence Datastore dual node presence redundancy group replication.
IM and Presence	IM and Presence	Proprietary	TCP	9004	Ephemeral	Cisco Login Datastore dual node presence redundancy group replication.
IM and Presence	IM and Presence	Proprietary	TCP	9005	Ephemeral	Cisco SIP Registration Datastore dual node presence redundancy group replication.

* 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 78: IM and Presence Service Ports - In Memory Database SQL Messages

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	IM and Presence	Proprietary	TCP	6603	Ephemeral	Cisco Presence Datastore SQL Queries.
IM and Presence	IM and Presence	Proprietary	TCP	6604	Ephemeral	Cisco Login Datastore SQL Queries.
IM and Presence	IM and Presence	Proprietary	TCP	6605	Ephemeral	Cisco SIP Registration Datastore SQL Queries.
IM and Presence	IM and Presence	Proprietary	TCP	6606	Ephemeral	Cisco Route Datastore SQL Queries.

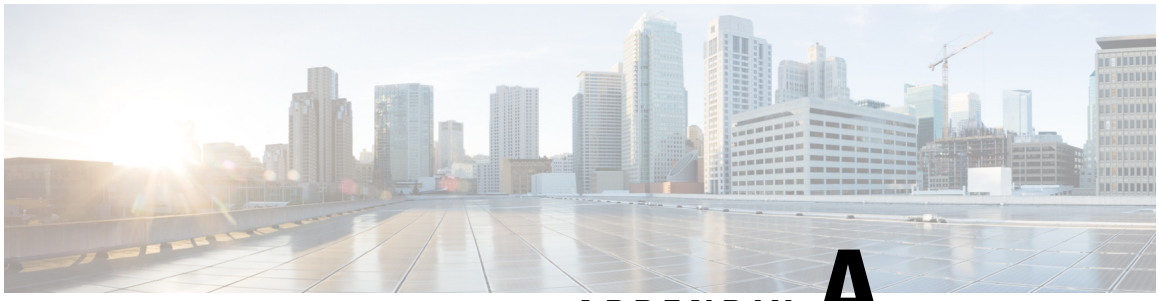
Table 79: IM and Presence Service Ports - In Memory Database Notification Messages

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	IM and Presence	Proprietary	TCP	6607	Ephemeral	Cisco Presence Datastore XML-based change notification.
IM and Presence	IM and Presence	Proprietary	TCP	6608	Ephemeral	Cisco Login Datastore XML-based change notification.
IM and Presence	IM and Presence	Proprietary	TCP	6609	Ephemeral	Cisco SIP Registration Datastore XML-based change notification.
IM and Presence	IM and Presence	Proprietary	TCP	6610	Ephemeral	Cisco Route Datastore XML-based change notification.

Table 80: IM and Presence Service Ports - Force Manual Sync/X.509 Certificate Update Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence (Intercluster Sync Agent)	IM and Presence (Intercluster Sync Agent)	TCP	TCP	37239	Ephemeral	Cisco Intercluster Sync Agent service uses this port to establish a socket connection for handling commands.

See the *Cisco Unified Serviceability Administration Guide* for information about SNMP.



APPENDIX A

High Availability Client Login Profiles

High Availability Login Profiles

Important Notes About High Availability Login Profiles

- You can use the High Availability login profile tables in this section to configure the upper and lower client re-login values for your presence redundancy group. You configure the upper and lower client login values by choosing **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters**, and choosing **Cisco Server Recovery Manager** from the Service menu.
- High Availability client login profiles apply only to single cluster deployments. High Availability client login profiles cannot configure the upper and lower client re-login values for the redundancy group if multiple clusters are present. You must perform more tests to discover High Availability client login profiles in multiple cluster deployments.
- If Debug Logging is enabled for the Cisco XCP Router service, then you should expect increased CPU usage and a decrease in the currently supported logging levels for IM and Presence Service.
- By configuring the upper and lower client re-login limits on your presence redundancy group based on the tables we provide here, you can avoid performance issues and high CPU spikes in your deployment.
- We provide a High Availability login profile for each IM and Presence Service node memory size, and for each High Availability deployment type, active/active or active/standby.
- The High Availability login profile tables are calculated based on the following inputs:
    - The lower client re-login limit is based on the Server Recovery Manager service parameter "Critical Service Down Delay", for which the default is 90 seconds. If the Critical Service Down Delay is changed then the lower limit must also change.
    - The total number of users in the presence redundancy group for Active/Standby deployments, or the node with highest number of users for Active/Active deployments.
- You must configure the upper and lower client re-login limit values on both nodes in a presence redundancy group. You must manually configure all these values on both nodes in the presence redundancy group.

- The upper and lower client re-login limit values must be the same on each node in the presence redundancy group.
- If you **rebalance** your users, you must reconfigure the upper and lower client re-login limit values based on the High Availability login profile tables.

Use High Availability Login Profile Tables

Use the High Availability login profile tables to retrieve the following values:

- **Client Re-Login Lower Limit** service parameter value
- **Client Re-Login Upper Limit** service parameter value.

Procedure

Step 1 Choose a profile table based on your virtual hardware configuration, and your High Availability deployment type.

Step 2 In the profile table, choose the number of users in your deployment (round up to the nearest value). If you have an active/standby deployment, use the node with the highest number of users.

Step 3 Based on the Number of Users value for your presence redundancy group, retrieve the corresponding lower and upper retry limits in the profile table.

Step 4 Configure the lower and upper retry limits on IM and Presence Service by choosing **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters**, and choosing **Cisco Server Recovery Manager** from the Service menu.

Step 5 Check the Critical Service Down Delay value by choosing **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters** and choosing **Cisco Server Recovery Manager** from the **Service** Menu. The default value is 90 seconds. The lower retry limit should be set to this value.

Example High Availability Login Configurations

Example 1: 15000 Users Full UC Profile - active/active deployment

You have 3000 users in your presence redundancy group, with 2000 users on one node, and 1000 users on the second node. For an unbalanced active/active deployment, Cisco recommends you use the node with the highest number of users, in this case the node with 2000 users. Using the 15000 users full US (4 vCPU 8GB) active/active profile, you retrieve these lower and upper retry values:

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
2000	120	253

Note The upper retry limit is the approximate time (seconds) it takes for all clients to login to their backup node after a failover occurs.

Note The lower limit of 120 assumes the **Critical Service Down Delay** service parameter is set to 120.

Example 2: 5000 Users Full UC Profile - active/active deployment

You have 4700 users on each node in your presence redundancy group . Cisco recommends that you round up to the nearest value, so using the 5000 users full US (4 vCPU 8GB) active/active profile you retrieve the lower and upper retry value based on a number of users value of 5000:

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
5000	120	953

Single Cluster Configuration

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

Table 81: User Login Retry Limits for Standard Deployment (500 Users Full UC Active/Active)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	187
250	120	287

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

Table 82: User Login Retry Limits for Standard Deployment (500 Users Full UC Active/Standby)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	187
250	120	287
500	120	453

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

Table 83: User Login Retry Limits for Standard Deployment (1000 Users Full UC Active/Active)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	153
250	120	203
500	120	287

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

Table 84: User Login Retry Limits for Standard Deployment (1000 Users Full UC Active/Standby)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	153
250	120	203
500	120	287
750	120	370
1000	120	453

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

Table 85: User Login Retry Limits for Standard Deployment (2000 Users Full UC Active/Active)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	153
500	120	287
1000	120	453

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

Table 86: User Login Retry Limits for Standard Deployment (2000 Users Full UC Active/Standby)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	153
250	120	203
500	120	287
750	120	370
1000	120	453
1250	120	537
1500	120	620
1750	120	703
2000	120	787

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

Table 87: User Login Retry Limits for Standard Deployment (5000 Users Full UC Active/Active)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	137
500	120	203
1000	120	287
1500	120	370
2000	120	453
2500	120	537

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

Table 88: User Login Retry Limits for Standard Deployment (5000 Users Full UC Active/Standby)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	137
500	120	203
1000	120	287
1500	120	370
2000	120	453
2500	120	537
3000	120	620
3500	120	703
4000	120	787
4500	120	870
5000	120	953

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

Attention To achieve maximum client login throughput on a 15000 user system, Cisco recommends a minimum of 2.5GHz CPU clock speed.

Table 89: User Login Retry Limits for Standard Deployment (15000 Users Full UC Active/Active)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	127
500	120	153
1000	120	187
1500	120	220
2000	120	253
2500	120	287
3000	120	320

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
3500	120	353
4000	120	387
4500	120	420
5000	120	453
6000	120	520
7000	120	587
7500	120	620

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

Attention To achieve maximum client login throughput on a 15000 user system, Cisco recommends a minimum of 2.5GHz CPU clock speed.

Table 90: User Login Retry Limits for Standard Deployment (15000 Users Full UC Active/Standby)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	127
500	120	153
1000	120	187
1500	120	220
2000	120	253
2500	120	287
3000	120	320
3500	120	353
4000	120	387
4500	120	420
5000	120	453
6000	120	520
7000	120	587
8000	120	653

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
9000	120	720
10000	120	787
11000	120	853
12000	120	920
13000	120	987
14000	120	1053
15000	120	1120

25000 Users Full UC (6 vCPU 16GB) Active/Active Profile

Attention To achieve maximum client login throughput on a 25000 user system, Cisco recommends a minimum of 2.8GHz CPU clock speed.

Table 91: Login rates for active /active profiles: 9 uses 45% CPU

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
100	120	131
500	120	176
1000	120	231
1500	120	287
2000	120	342
2500	120	398
3000	120	453
3500	120	509
4000	120	564
4500	120	620
5000	120	676
6000	120	787
7000	120	898
7500	120	953

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
8000	120	1009
9000	120	1120
10000	120	1231
11000	120	1342
12000	120	1453
12500	120	1509

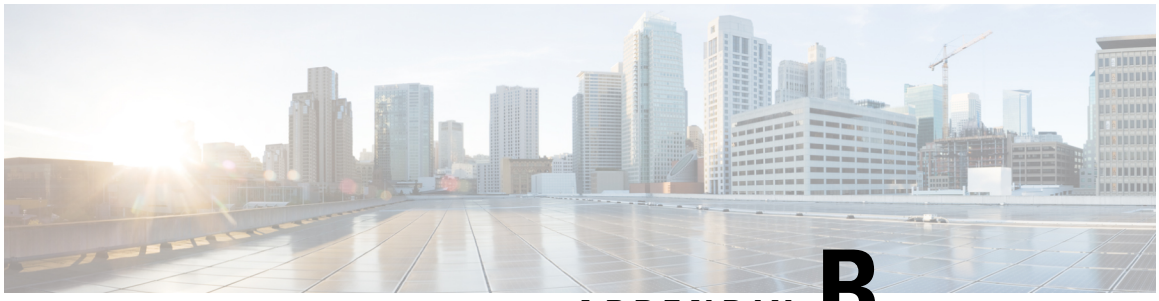
25000 Users Full UC (6 vCPU 16GB) Active/Standby Profile

Attention To achieve maximum client login throughput on a 25000 user system, Cisco recommends a minimum of 2.8GHz CPU clock speed.

Table 92: Login rates for active /standby profiles: 16 users 80% CPU

Expected number of Active Users	Lower Retry Limit	Upper Retry Limit
100	120	126
500	120	151
1000	120	183
1500	120	214
2000	120	245
2500	120	276
3000	120	308
3500	120	339
4000	120	370
4500	120	401
5000	120	433
6000	120	495
7000	120	558
8000	120	620
9000	120	683

Expected number of Active Users	Lower Retry Limit	Upper Retry Limit
10000	120	745
11000	120	808
12000	120	870
13000	120	933
14000	120	995
15000	120	1058
16000	120	1120
17000	120	1183
18000	120	1245
19000	120	1308
20000	120	1370
21000	120	1433
22000	120	1495
23000	120	1558
24000	120	1620
25000	120	1683



APPENDIX B

Additional Requirements

High Availability Login Profiles

Important Notes About High Availability Login Profiles

- You can use the High Availability login profile tables in this section to configure the upper and lower client re-login values for your presence redundancy group. You configure the upper and lower client login values by choosing **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters**, and choosing **Cisco Server Recovery Manager** from the Service menu.
- High Availability client login profiles apply only to single cluster deployments. High Availability client login profiles cannot configure the upper and lower client re-login values for the redundancy group if multiple clusters are present. You must perform more tests to discover High Availability client login profiles in multiple cluster deployments.
- If Debug Logging is enabled for the Cisco XCP Router service, then you should expect increased CPU usage and a decrease in the currently supported logging levels for IM and Presence Service.
- By configuring the upper and lower client re-login limits on your presence redundancy group based on the tables we provide here, you can avoid performance issues and high CPU spikes in your deployment.
- We provide a High Availability login profile for each IM and Presence Service node memory size, and for each High Availability deployment type, active/active or active/standby.
- The High Availability login profile tables are calculated based on the following inputs:
  - The lower client re-login limit is based on the Server Recovery Manager service parameter "Critical Service Down Delay", for which the default is 90 seconds. If the Critical Service Down Delay is changed then the lower limit must also change.
  - The total number of users in the presence redundancy group for Active/Standby deployments, or the node with highest number of users for Active/Active deployments.

- You must configure the upper and lower client re-login limit values on both nodes in a presence redundancy group. You must manually configure all these values on both nodes in the presence redundancy group.
- The upper and lower client re-login limit values must be the same on each node in the presence redundancy group.
- If you **rebalance** your users, you must reconfigure the upper and lower client re-login limit values based on the High Availability login profile tables.

Use High Availability Login Profile Tables

Use the High Availability login profile tables to retrieve the following values:

- **Client Re-Login Lower Limit** service parameter value
- **Client Re-Login Upper Limit** service parameter value.

Procedure

Step 1 Choose a profile table based on your virtual hardware configuration, and your High Availability deployment type.

Step 2 In the profile table, choose the number of users in your deployment (round up to the nearest value). If you have an active/standby deployment, use the node with the highest number of users.

Step 3 Based on the Number of Users value for your presence redundancy group, retrieve the corresponding lower and upper retry limits in the profile table.

Step 4 Configure the lower and upper retry limits on IM and Presence Service by choosing **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters**, and choosing **Cisco Server Recovery Manager** from the Service menu.

Step 5 Check the Critical Service Down Delay value by choosing **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters** and choosing **Cisco Server Recovery Manager** from the **Service** Menu. The default value is 90 seconds. The lower retry limit should be set to this value.

Example High Availability Login Configurations

Example 1: 15000 Users Full UC Profile - active/active deployment

You have 3000 users in your presence redundancy group, with 2000 users on one node, and 1000 users on the second node. For an unbalanced active/active deployment, Cisco recommends you use the node with the highest number of users, in this case the node with 2000 users. Using the 15000 users full US (4 vCPU 8GB) active/active profile, you retrieve these lower and upper retry values:

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
2000	120	253

Note The upper retry limit is the approximate time (seconds) it takes for all clients to login to their backup node after a failover occurs.

Note The lower limit of 120 assumes the **Critical Service Down Delay** service parameter is set to 120.

Example 2: 5000 Users Full UC Profile - active/active deployment

You have 4700 users on each node in your presence redundancy group . Cisco recommends that you round up to the nearest value, so using the 5000 users full US (4 vCPU 8GB) active/active profile you retrieve the lower and upper retry value based on a number of users value of 5000:

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
5000	120	953

Single Cluster Configuration

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

Table 93: User Login Retry Limits for Standard Deployment (500 Users Full UC Active/Active)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	187
250	120	287

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

Table 94: User Login Retry Limits for Standard Deployment (500 Users Full UC Active/Standby)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	187
250	120	287
500	120	453

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

Table 95: User Login Retry Limits for Standard Deployment (1000 Users Full UC Active/Active)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	153
250	120	203
500	120	287

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

Table 96: User Login Retry Limits for Standard Deployment (1000 Users Full UC Active/Standby)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	153
250	120	203
500	120	287
750	120	370
1000	120	453

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

Table 97: User Login Retry Limits for Standard Deployment (2000 Users Full UC Active/Active)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	153
500	120	287
1000	120	453

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

Table 98: User Login Retry Limits for Standard Deployment (2000 Users Full UC Active/Standby)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	153
250	120	203
500	120	287
750	120	370
1000	120	453
1250	120	537
1500	120	620
1750	120	703
2000	120	787

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

Table 99: User Login Retry Limits for Standard Deployment (5000 Users Full UC Active/Active)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	137
500	120	203
1000	120	287
1500	120	370
2000	120	453
2500	120	537

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

Table 100: User Login Retry Limits for Standard Deployment (5000 Users Full UC Active/Standby)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	137
500	120	203
1000	120	287
1500	120	370
2000	120	453
2500	120	537
3000	120	620
3500	120	703
4000	120	787
4500	120	870
5000	120	953

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

Attention To achieve maximum client login throughput on a 15000 user system, Cisco recommends a minimum of 2.5GHz CPU clock speed.

Table 101: User Login Retry Limits for Standard Deployment (15000 Users Full UC Active/Active)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	127
500	120	153
1000	120	187
1500	120	220
2000	120	253
2500	120	287
3000	120	320

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
3500	120	353
4000	120	387
4500	120	420
5000	120	453
6000	120	520
7000	120	587
7500	120	620

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

Attention To achieve maximum client login throughput on a 15000 user system, Cisco recommends a minimum of 2.5GHz CPU clock speed.

Table 102: User Login Retry Limits for Standard Deployment (15000 Users Full UC Active/Standby)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	127
500	120	153
1000	120	187
1500	120	220
2000	120	253
2500	120	287
3000	120	320
3500	120	353
4000	120	387
4500	120	420
5000	120	453
6000	120	520
7000	120	587
8000	120	653

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
9000	120	720
10000	120	787
11000	120	853
12000	120	920
13000	120	987
14000	120	1053
15000	120	1120

25000 Users Full UC (6 vCPU 16GB) Active/Active Profile

Attention To achieve maximum client login throughput on a 25000 user system, Cisco recommends a minimum of 2.8GHz CPU clock speed.

Table 103: Login rates for active /active profiles: 9 uses 45% CPU

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
100	120	131
500	120	176
1000	120	231
1500	120	287
2000	120	342
2500	120	398
3000	120	453
3500	120	509
4000	120	564
4500	120	620
5000	120	676
6000	120	787
7000	120	898
7500	120	953

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
8000	120	1009
9000	120	1120
10000	120	1231
11000	120	1342
12000	120	1453
12500	120	1509

25000 Users Full UC (6 vCPU 16GB) Active/Standby Profile

Attention To achieve maximum client login throughput on a 25000 user system, Cisco recommends a minimum of 2.8GHz CPU clock speed.

Table 104: Login rates for active /standby profiles: 16 users 80% CPU

Expected number of Active Users	Lower Retry Limit	Upper Retry Limit
100	120	126
500	120	151
1000	120	183
1500	120	214
2000	120	245
2500	120	276
3000	120	308
3500	120	339
4000	120	370
4500	120	401
5000	120	433
6000	120	495
7000	120	558
8000	120	620
9000	120	683

Expected number of Active Users	Lower Retry Limit	Upper Retry Limit
10000	120	745
11000	120	808
12000	120	870
13000	120	933
14000	120	995
15000	120	1058
16000	120	1120
17000	120	1183
18000	120	1245
19000	120	1308
20000	120	1370
21000	120	1433
22000	120	1495
23000	120	1558
24000	120	1620
25000	120	1683

XMPP Standards Compliance

The IM and Presence Service is compliant with the following XMPP standards:

- RFC 3920 Extensible Messaging and Presence Protocol (XMPP): Core RFC 3921 Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence
  - XEP-0004 Data Forms
  - XEP-0012 Last Activity
  - XEP-0013 Flexible Offline Message Retrieval
  - XEP-0016 Privacy Lists
  - XEP-0030 Service Discovery
  - XEP-0045 Multi-User Chat
  - XEP-0054 Vcard-temp
  - XEP-0055 Jabber Search

- XEP-0060 Publish-Subscribe
- XEP-0065 SOCKS5 Bystreams
- XEP-0066 Out of Band Data Archive OOB requests
- XEP-0068 Field Standardization for Data Forms
- XEP-0071 XHTML-IM
- XEP-0082 XMPP Date and Time Profiles
- XEP-0092 Software Version
- XEP-0106 JID Escaping
- XEP-0114 Jabber Component Protocol
- XEP-0115 Entity Capabilities
- XEP-0124 Bidirectional Streams over Synchronous HTTP (BOSH)
- XEP-0126 Invisibility
- XEP-0128 Service Discovery Extensions
- XEP-0160 Best Practices for Handling Offline Messages
- XEP-0163 Personal Eventing Via PubSub
- XEP-0170 Recommended Order of Stream Feature Negotiation
- XEP-0178 Best Practices for Use of SASL EXTERNAL
- XEP-0220 Server Dialback
- XEP-0273 SIFT (Stanza Interception and Filtering Technology)

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.

Configurations that Require a Restart	Restart this Service
Application Listener Configuration (System > Application Listeners) Editing Application Listeners	Cisco SIP Proxy
Compliance Profile Configuration (Messaging > Compliance > Compliance Settings) (Messaging > Compliance > Compliance Profiles If you edit settings for events that are assigned to a 3rd party compliance server	Cisco XCP Router
Group Chat System Administrators (Messaging >Group Chat System Administrators) If you enable or disable this setting	Cisco XCP Router
External File Server Configuration (Messaging > External Server Setup > External File Servers) If you edit the **Host/IP Address Setting** If you regenerate the **External File Server Public Key**	Cisco XCP Router
Group Chat and Persistent Chat Configuration (Messaging > Group Chat and Persistent Chat) If a chat node cannot reach its external DB at startup, the Cisco XCP Text Conference Mgr Service is not running	Cisco XCP Router
Group Chat Server Alias Mapping (Messaging > Group Chat Server Alias Mapping) Adding a chat alias	Cisco XCP Router
ACL Configuration (System > Security > Incoming ACL) (System > Security > Outgoing ACL) Edit Incoming or Outgoing ACL Configuration	Cisco SIP Proxy
Compliance Settings Message Archiver - edit the settings	Cisco XCP Router
LDAP Server (Application > Third-Party Clients > Third-party LDAP Settings) LDAP Search - editing LDAP Search Editing the Build vCards from LDAP Editing the LDAP attribute to use for vCard FN	Cisco XCP Router

Configurations that Require a Restart	Restart this Service
Message Settings Configuration (Messaging > Settings) Editing the Enable instant message Suppress offline instant messaging	Cisco XCP Router
Microsoft RCC Configuration (Application > Microsoft RCC > Settings) Editing any of the settings on this page	Cisco SIP Proxy
Presence Gateway (Presence > Gateways) Add, edit, delete a presence gateway After you upload MS Exchange certificates	Cisco Presence engine
Presence Settings Configuration (Presence > Settings > Standard Configuration) Editing the Enable Availability Sharing setting Allow users to view the availability of other users without being prompted for approval Maximum Contact List Size (per user) Maximum Watchers	Cisco Presence Engine Cisco XCP Router
Presence Settings Configuration (Presence > Settings > Standard Configuration) Editing the **Enable user of Email address for Interdomain Federation** field	Cisco XCP Router
Partitioned Intradomain Federation Configuration Presence > Settings > Standard Configuration (check box) Presence > Intradomain Federation Setup (wizard) Enable Partitioned Intradomain Federation with LCS/OCS/Lync via the check box or via the wizard Partitioned intradomain Routing Mode - configured via the Standard Configuration window or via the wizard	Editing these settings causes automatic restart of Cisco SIP Proxy In addition, you must restart XCP Router
Proxy Configuration (Presence > Routing > Settings) Any edit to the Proxy Configuration	Cisco SIP Proxy

Configurations that Require a Restart	Restart this Service
Security Settings (System > Security > Settings) Editing any SIP security settings such as SIP Intracluster Proxy to Proxy Transport Protocol Editing any XMPP security setting	Cisco SIP Proxy (for SIP security edits) Cisco XCP Router (for XMPP security edits)
SIP Federated Domain (Presence > Interdomain Federation > SIP Federation) Add, edit, delete this configuration	Cisco XCP Router
Third-Party Compliance Service (Application > Third-Party Clients > Third-Party LDAP Servers) Edit the Hostname/IP Address, Port, Password/Confirm Password fields	Cisco XCP Router
TLS Peer Subject Configuration (System > Security > TLS Peer Subjects) Any edits on this page	Cisco SIP Proxy
TLS Context (System > Security > TLS Context Configuration) Any edits on this page	You may need to restart the associated chat server
XMPP Federation (Presence > Interdomain Federation > XMPP Federation > Settings) (Presence > Interdomain Federation > XMPP Federation > Policy) Any edits to XMPP Federation	Cisco XCP Router
Intercluster Peering (Presence Inter-clustering) Editing the intercluster peer configuration	You may be asked to restart the Cisco XCP Router (a notification appears in the top right window) in some cases
Ethernet settings (From Cisco Unified IM and Presence OS Administration, Settings > IP > Ethernet/Ethernet IPv6) Editing any ethernet settings	Causes immediate system restart
IPv6 Configuration (System > Enterprise Parameters) Editing the Enable IPv6 enterprise parameter	Cisco XCP Router Cisco SIP Proxy Cisco Presence Engine

Configurations that Require a Restart	Restart this Service
Troubleshooting If an IM and Presence publisher changes while subscriber is offline Edit the Settings > IP > Publisher setting from the subscriber	Restart subscriber node
Upgrading IM and Presence and you need to switch to previous version	Restart the system
Regenerating the cup certificate	Cisco SIP Proxy Cisco Presence Engine
Regenerate cup-xmpp	Cisco XCP Router
Regenerate cup-xmpp-s2s certificate	Cisco XCP Router
Upload new certificate	Restart relevant service for that certificate. For Cup-trust certificates, restart the Cisco SIP Proxy
Remote Audit Log Transfer Protocol if you run any of the utils remotesyslog set protocol * CLI commands	Restart the node
If you get any of the following alerts: • PEIDSQueryError • PEIDStoIMDBDatabaseSyncError • PEIDSSubscribeError • PEWebDAVInitializationFailure	It's recommended to restart Cisco Presence Engine
If you get any of the following alerts: • • XCPConfigMgrJabberRestartRequired • XCPConfigMgrR2RPasswordEncryptionFailed • XCPConfigMgrR2RRequestTimedOut • XCPConfigMgrHostNameResolutionFailed	It's recommended to restart Cisco XCP Router
PWSSCBInitFailed	It's recommended to restart Cisco SIP Proxy

Configurations that Require a Restart	Restart this Service
Editing any of the Exchange Service Parameters • Microsoft Exchange Notification Port • Calendar Spread • Exchange Timeout (seconds) • Exchange Queue • Exchange Threads • EWS Status Frequency	Cisco Presence Engine
Upload Exchange Certificates	Cisco SIP Proxy Cisco Presence Engine
Installing locales	Restart the IM and Presence Service
Create new MSSQL external database	Cisco XCP Router
Editing external database configuration	Cisco XCP Router
Merging external database	Cisco XCP Router
Configuring TLS Peer Subjects	Cisco SIP Proxy
Configuring Peer Authentication TLS Context	Cisco SIP Proxy
Editing the following Cisco SIP Proxy Service Parameters: • CUCM Domain • Server Name (supplemental) • HTTP Port • Stateful Server (transaction Stateful) • Persist TCP Connections • Shared memory size (bytes) • Federation Routing IM/P FQDN • Microsoft Federation User-Agent Headers (comma-delimited)	Cisco SIP Proxy
Edit the **Routing Communication Type** service parameter	Cisco XCP Router
Editing the IM address scheme	Cisco XCP Router
Assign a default domain	Cisco XCP Router
Deleting or removing a node from the cluster	Cisco XCP Router

Configurations that Require a Restart	Restart this Service
Any edit to a parameter that affects the Cisco XCP router requires you to restart the Cisco XCP router	Cisco XCP Router
Routing Communication Type service parameters	Cisco XCP Router
Editing either of the Cisco XCP File Transfer Manager service parameters: • **External File Server Available Space Lower Threshold** • **External File Server Available Space Upper Threshold**	Cisco XCP Router
Edit the **Enable Mulitple Device Messaging** service parameter	Cisco XCP Router
Editing the **Maximum number of logon sessions per user** service parameter	Cisco XCP Router
Updating the `install_dir /data/pg_hba.conf` or `install_dir /data/postgresql.conf` config files on the external database	Cisco XCP Router
Migration utilities: • Editing the **Allow users to view the availability of other users without being prompted for approval** setting in the Presence Settings window. • Editing the **Maximum Contact Lists Size (per user)** and **Maximum Watchers (per user**) setting in the Presence Settings configuration window.	Cisco XCP Router
Deleting or removing a node from a cluster	Cisco XCP Router

Additional Requirements