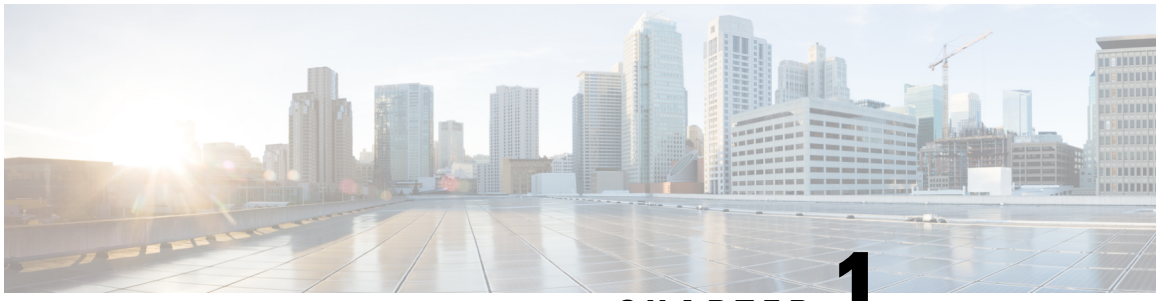
Configuration and Administration of the IM and Presence Service, Release 15

First Published: 2023-12-18

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 1

New and Changed Information

New and Changed Information

The following table provides an overview of the significant changes to the features in this guide up to this current release. The table does not provide an exhaustive list of all changes made to the guide or of the new features up to this release.

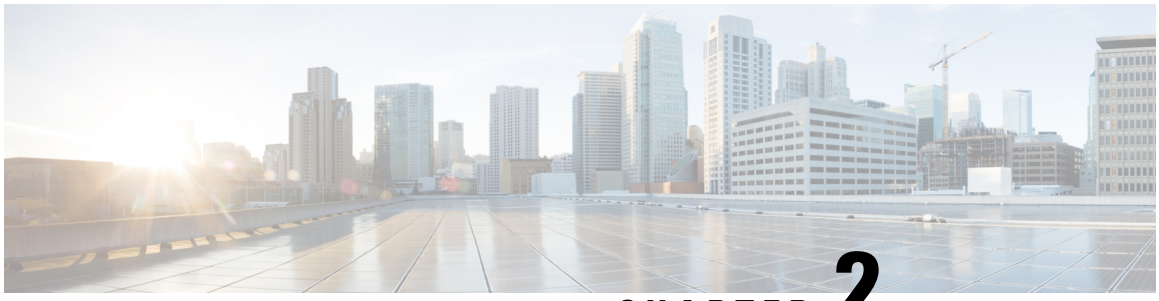
Table 1: New Features and Changed Behavior in IM and Presence Service

Date	Description	See
December 18, 2023	Removal of Microsoft Remote Call Control Feature.	-

New and Changed Information

PART I

Plan the System



CHAPTER 2

Plan the System

IM and Presence Service Overview

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

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

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

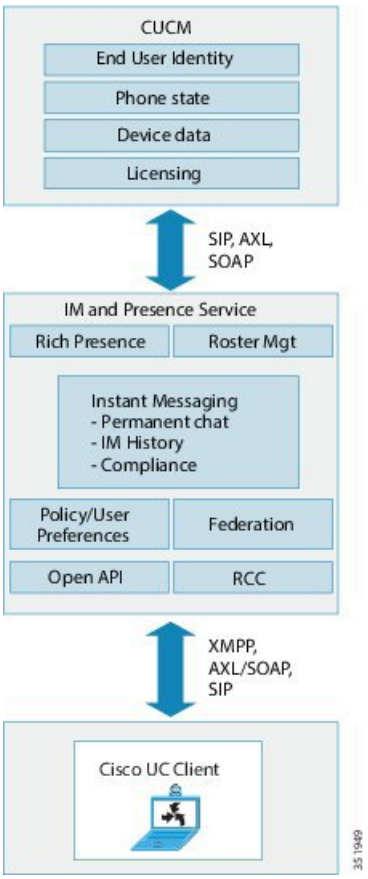
- Presence
- Instant messaging
- File Transfers
- Audio Calls
- Video
- Voicemail
- Conferencing

See Cisco Unified Communications Manager documentation for more.

IM and Presence Service Components

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

Figure 1: IM and Presence Service Basic Deployment



SIP Interface

You must configure the following to enable the SIP interface:

- In Cisco Unified Communications Manager, you must configure a SIP trunk that points to the IM and Presence Service for the presence information exchange.
- On the IM and Presence Service, configure Cisco Unified Communications Manager as a Presence Gateway so that IM and Presence Service can send SIP subscribe messages to Cisco Unified Communications Manager over the SIP trunk.

AXL/SOAP Interface

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

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

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

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

LDAP Interface

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

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

XMPP Interface

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

CTI Interface

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

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

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

Cisco IM and Presence Data Monitor Service

The Cisco IM and Presence Data Monitor monitors the IDS replication state on the IM and Presence Service. Other IM and Presence services are dependent on the Cisco IM and Presence Data Monitor so that they can delay startup until IDS replication is in a stable state.

The Cisco IM and Presence Data Monitor also checks the status of the Cisco Sync Agent sync from Cisco Unified Communications Manager. Dependent services are only allowed to start after IDS replication has set up and the Sync Agent on the IM and Presence database publisher node has completed its sync from Cisco

Unified Communications Manager. After the timeout has been reached, the Cisco IM and Presence Data Monitor on the Publisher node will allow dependent services to start even if IDS replication and the Sync Agent have not completed.

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

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

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

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

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

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

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

Planning Overview

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

For detailed information on how to design a Cisco Collaboration system that includes an IM and Presence Service deployment that meets your needs, refer to 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.

Plan Your Deployment

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

Procedure

	Command or Action	Purpose
Step 1	Size your Collaboration deployment	For information, refer to the "Collaboration Solution Sizing Guidance" chapter of 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.
Step 2	Determine which features you want to deploy.	For details, see Feature Deployment Options, on page 10.
Step 3	Determine if you will install the standard deployment or an IM and Presence central cluster deployment	Decide whether you want to deploy the IM and Presence Service on the same cluster as your telephony, or whether you want to deploy a centralized cluster for IM and Presence. For details, see Standard Deployment vs Centralized Cluster.
Step 4	Plan how many cluster nodes you want to deploy.	The IM and Presence multinode scalability features allow you to size your deployment to meet your needs. For details, see Multinode Scalability Requirements, on page 12.
Step 5	Plan how you are going to add redundancy.	Scalability Options for Deployment, on page 13
Step 6	Plan your geographic sites	You can install at a single site in order to maintain your hardware from a single location. However, you can also deploy your clusters over the WAN to add geographic redundancy with deploying multiple sites. For details, see: • Intracluster Deployments Over WAN, on page 15 • Intercluster Deployments Over WAN, on page 16
Step 7	Plan the schema for Jabber identifiers (JIDs) for IM and Presence users.	For the allowed characters in the Jabber identifier (JID), please refer RFC 3920 (3. Addressing Scheme) and XEP-0106. Cisco Jabber and other 3rd party XMPP clients may impose further restrictions for which the client-side documentation should be referred.
Step 8	Decide if you want to configure SAML Single-Sign On.	For details, see SAML Single Sign-On Deployments, on page 16.
Step 9	Determine if you want to integrate with a third-party application.	This includes Microsoft Outlook calendar integration as well as federation with a

	Command or Action	Purpose
		third-party system. For details, see Third Party Integrations, on page 16.

IM and Presence Service Deployment Sizing

For information on how to size your Collaboration deployment, refer to the "Collaboration Solution Sizing Guidance" chapter of 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.

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.

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

Table 2: Feature Deployment Options for the IM and Presence Service

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 Intercluster peering Enterprise federation: • IM and Presence Service integration • Cisco WebEx Messenger integration • Microsoft Lync/Skype for Business/Office365 server integration • IBM SameTime integration • Cisco Jabber XCP Public federation: • Google Talk, AOL integration • XMMP services or BOTs • Third-party Exchange Service integration IM Compliance SAML Single Sign On Custom login banner	Cisco telephony availability Microsoft Outlook calendar integration (on-premise Exchange or hosted Office 365 deployments)	Remote Cisco IP Phone control Remote Softphone Control

Standard Deployment vs Centralized Cluster

Before you even install your system, you must decide whether you want to deploy a standard deployment of the IM and Presence Service or whether you want an IM and Presence Service central cluster as this will affect your topology and installation:

- IM and Presence Service on Cisco Unified Communications Manager (Standard deployment)—In standard deployments, the IM and Presence Service cluster is installed on the same servers as the Cisco Unified Communications Manager telephonynodes. The IM and Presence cluster shares a platform and many of the same services as the telephony cluster. This option requires a 1x1 mapping of telephony clusters to IM and Presence clusters.
- Centralized IM and Presence cluster—In this deployment, the IM and Presence Service cluster is installed separately from your telephony cluster. Depending on how you plan your topology, the IM and Presence central cluster may be located on completely different hardware servers from your telephony cluster. This deployment option removes the 1x1 mapping requirement of telephony clusters and IM and Presence clusters, which allows you to better scale each deployment type to its own needs.

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

The procedures in this document can be used for both standard deployments and central cluster deployments. However, for central cluster deployments, you must also complete the tasks in the Configure Centralized Deployment, on page 101, chapter to properly align your telephony cluster and IM and Presence cluster.

Multinode Scalability Feature

Multinode Scalability Requirements

IM and Presence Service supports multinode scalability:

- Six nodes per cluster
- 75,000 users per cluster with a maximum of 25,000 users per node in a full Unified Communication (UC) mode deployment
- 25,000 users in a presence redundancy group, and 75,000 users per cluster in a deployment with High Availability.
- Administrable customer-defined limit on the maximum contacts per user (default unlimited)
- The IM and Presence Service continues to support intercluster deployments with the multinode feature.

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:

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.

WAN Deployments

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

Intracluster Deployments Over WAN

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

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

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

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

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

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

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

Multinode Configuration for Deployment Over WAN

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

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

Intercluster Deployments Over WAN

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

- Intercluster Peers—You can configure peer relationships that interconnect standalone IM and Presence Service clusters, known as intercluster peers. This intercluster peer functionality allows users in one IM and Presence Service cluster to communicate and subscribe to the availability information of users in a remote IM and Presence Service cluster within the same domain. For details on how to set up intercluster peers, see Configure Intercluster Peers, on page 160.
- Node Names—The node name that you define for any IM and Presence Service node must be resolvable by every other IM and Presence Service node on every cluster. Therefore, each IM and Presence Service node name must be the FQDN of the node. If DNS is not deployed in your network, each node name must be an IP address.
- IM Address Scheme—For intercluster deployments, all nodes in each of the clusters must use the same IM address scheme. If any node in a cluster is running a version of IM and Presence Service that is earlier than Release 10, all nodes must be set to use the UserID@Default_Domain IM address scheme for backward compatibility.
- Router-to-Router Communications—By default, IM and Presence Service assigns all nodes in a cluster as intercluster router-to-router connectors. When IM and Presence Service establishes an intercluster peer connection between the clusters over the AXL interface, it synchronizes the information from all intercluster router-to-router connector nodes in the home and remote clusters.

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

SAML Single Sign-On Deployments

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

- A single login is required to access a number of Cisco Collaboration applications after a single sign-in.
- Only one password is required–there's no longer any need to remember different passwords for each application.
- Administrators can manage all passwords and authentication from a single Identity Provider (IdP).

For details on how to setup and configure SAML Single Sign-On, see the *SAML SSO Deployment Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Third Party Integrations

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

Guide Title	This Guide Contains ...
Microsoft Outlook Calendar Integration for the IM and Presence Service	Configure the IM and Presence Service to connect with an on-premise Microsoft Exchange server or a hosted Office 365 server in order to use calendar information from Microsoft Outlook in an IM and Presence user's Presence status.
Interdomain Federation for the IM and Presence Service	Configure the IM and Presence Service for interdomain federation with the following systems. This allows IM and Presence users to exchange IM and Presence with users on the other system. • Microsoft Lync • Microsoft Skype for Business • Microsoft Office 365 • GoogleTalk • AOL • IBM SameTime • Cisco WebEx Messenger • another IM and Presence Service enterprise
Partitioned Intradomain Federation for the IM and Presence Service	Configuring the IM and Presence Service for Partitioned Intradomain Federation with Microsoft Lync or Skype for Business. You can use this integration to maintain communications within your network while you are in the process of migrating users to the IM and Presence Service.

Third Party Client Integration

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

Supported Third-Party XMPP Clients

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

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

http://developer.cisco.com/

License Requirements

You must assign IM and Presence Service capabilities for each user of an XMPP client application. IM and Presence capabilities are included within both User Connect Licensing (UCL) and Cisco Unified Workspace Licensing (CUWL).

For additional information on licensing, see the "Smart Software Licensing" chapter of the *System Configuration Guide for Cisco Unified Communications Manager* athttp://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

XMPP Client Integration on Cisco Unified Communications Manager

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

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

LDAP Integration for XMPP Contact Search

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

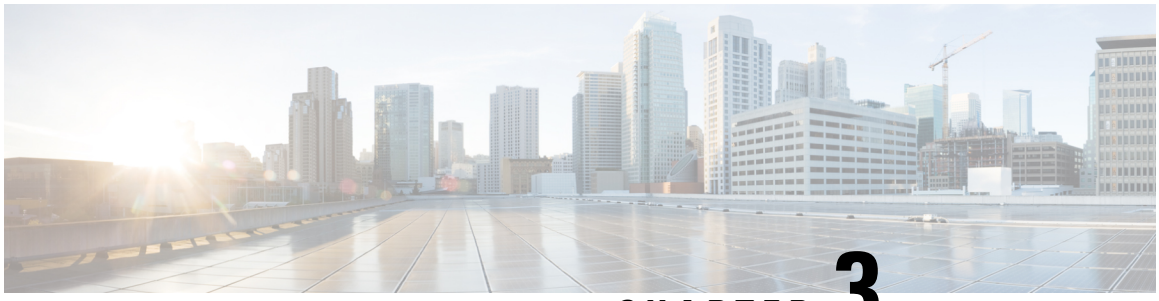
DNS Configuration for XMPP Clients

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

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

PART II

Configure the System



CHAPTER 3

Configure the Domain

Configure the Domain Overview

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

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

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

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

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

Domain Configuration Examples

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

- Multiple Cluster with Different DNS Domains and Subdomains
- Single Cluster with Different DNS Domains or Subdomains

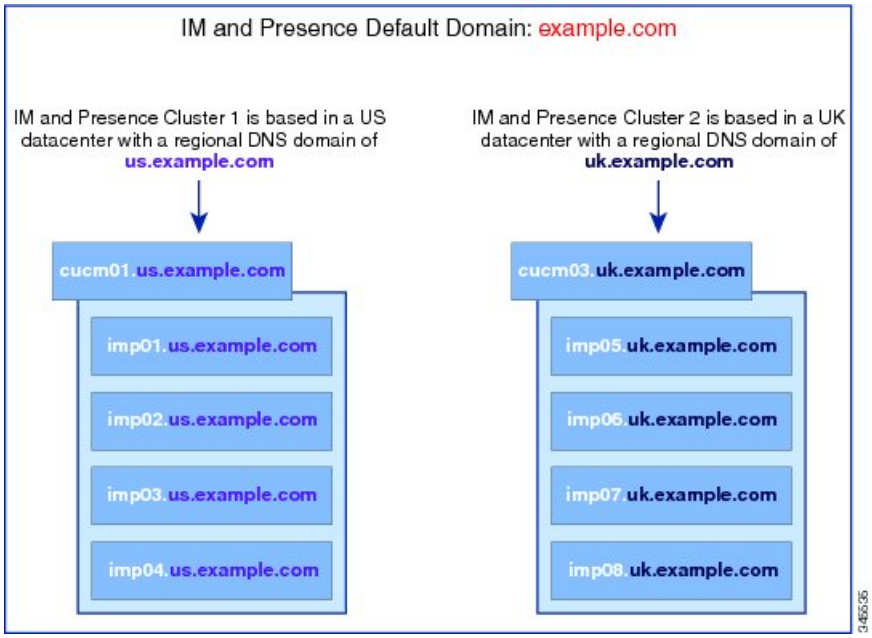
- Single Cluster where the DNS Domain is Different than the Unified Communications Manager Domain

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

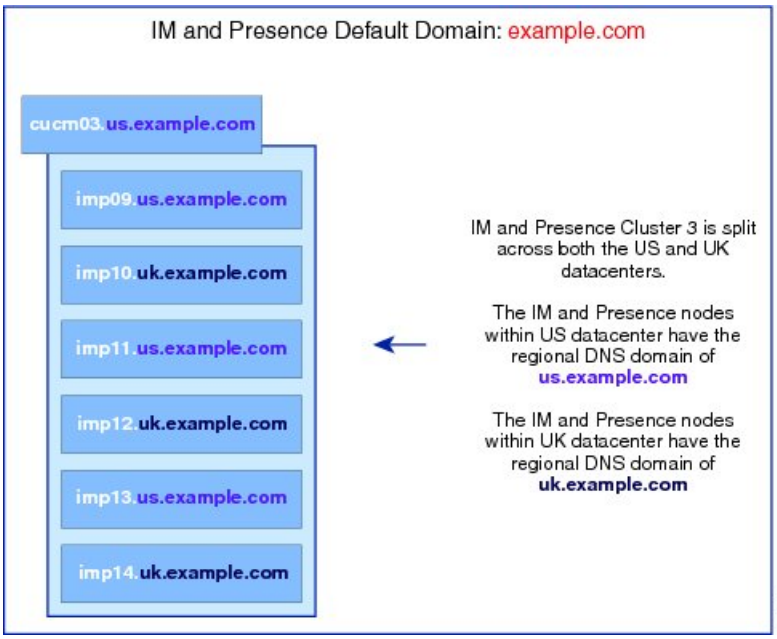
Multiple Cluster with Different DNS Domains and Subdomains

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



Single Cluster with Different DNS Domains or Subdomains

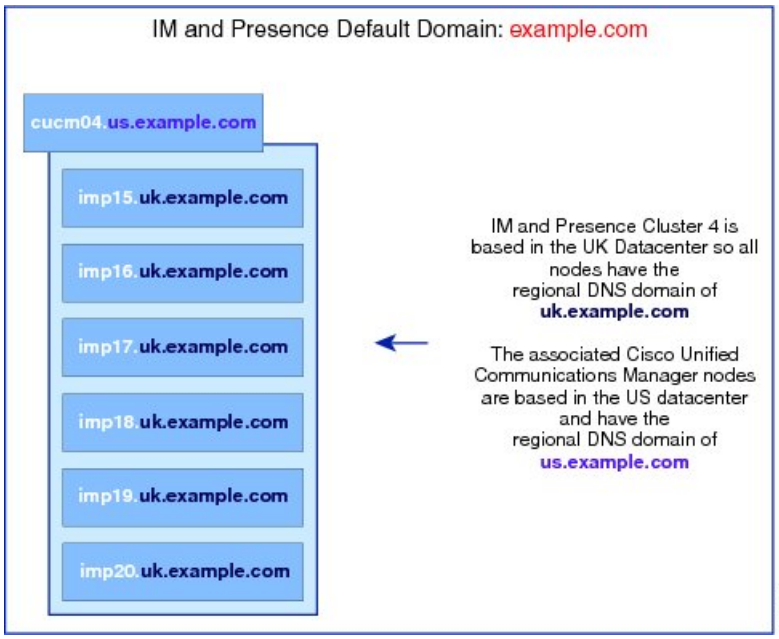
IM and Presence Service supports having the nodes within any IM and Presence Service cluster deployed across multiple DNS domains or subdomains. The diagram below highlights a sample deployment scenario that is supported.



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.

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

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



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, this service parameter is set to the DNS domain of the IM and Presence database publisher node. If the DNS domain of the IM and Presence database publisher node differs from the DNS domain of the Cisco Unified Communications Manager cluster, you must edit this service parameter to use the domain of the Cisco Unified Communications Manager cluster.

Configure the Domain Prerequisites

- All IM and Presence Service and Cisco Unified Communications Manager nodes and clusters must support multiple domains to use this feature. Ensure that all nodes in the IM and Presence Service clusters are operating using Release 10.0 or greater.
- Ensure that you configure Directory URIs for addressing. For more information, see "Configure URI Dialing" in 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

Configure the Domain Task Flow

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

Procedure

	Command or Action	Purpose
Step 1	Disable High Availability, on page 25	If high availability is enabled, you must temporarily disable it. Changing the default domain requires you to stop services temporarily; if you stop the services while high availability is enabled, a system failover will occur.
Step 2	Deactivate IM and Presence Services, on page 26	Stop essential services prior to changing the domain.
Step 3	Configure the Default Domain on IM and Presence Service , on page 27	Configure the default domain value for the IM and Presence Service cluster. This procedure is applicable for both DNS and non-DNS deployments.
Step 4	Perform any of these tasks: • Add or Update IM Address Domains, on page 27 • Delete IM Address Domains , on page 28	Optional. Complete these tasks only if you want to add, edit, or delete administrator-managed domains on your local cluster.

	Command or Action	Purpose
Step 5	Regenerate XMPP Client and TLS Certificates, on page 29	If you are using TLS XMPP Federation, proceed to generate new XMPP client and TLS certificates.
Step 6	Start IM and Presence Services, on page 29	After completing your domain configuration, restart services.
Step 7	Enable High Availability for Presence Redundancy Groups, on page 30	If you had high availability configured, enable it once more. **Note** Make sure that the services that you started are running on all cluster nodes before you enable high availability.

Disable High Availability

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

Note The **Presence Redundancy Group Details** page shows all the active JSM sessions, even when the high availability is disabled in the cluster.

Before you begin

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

Procedure

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

Step 2 Click **Find** and select the group.

Step 3 On the Presence Redundancy Group Configuration window, uncheck the **Enable High Availability** check box.

Step 4 Click **Save**.

Step 5 Repeat this procedure for each Presence Redundancy Group.

Step 6 When you are done, wait at least two minutes to sync the new HA settings across the cluster before you make any further changes

What to do next

Deactivate IM and Presence Services, on page 26

Deactivate IM and Presence Services

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

Before you begin

Make sure that High Availability is disabled. For details, see Disable High Availability, on page 25.

Procedure

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

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

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

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

Step 4 Click **Stop**.

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

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

- **Cisco SIP Proxy**
- **Cisco Presence Engine**

Step 7 Click **Save**.

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

What to do next

Configure the default domain for the IM and Presence Service:

- Configure the Default Domain on IM and Presence Service , on page 27

Otherwise, if the default domain is already configured, complete one of these tasks to add, edit, or delete domains.

- Add or Update IM Address Domains, on page 27
- Delete IM Address Domains , on page 28

Configure the Default Domain on IM and Presence Service

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

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

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

Before you begin

Make sure that High Availability is disabled, and essential IM and Presence Services are stopped. For details, Deactivate IM and Presence Services, on page 26.

Procedure

Step 1 Log in to the IM and Presence Service database publisher node.

Step 2 From **Cisco Unified CM IM and Presence Administration**, choose **Presence** > **Settings** > **Advanced Configuration**.

Step 3 Choose **Default Domain**.

Step 4 In the **Domain Name** field, enter the new presence domain and click **Save**.

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

What to do next

If you are using TLS XMPP Federation, proceed to Regenerate XMPP Client and TLS Certificates, on page 29.

Add or Update IM Address Domains

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

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

Before you begin

Make sure that High Availability is disabled, and essential IM and Presence Services are stopped. For details, Deactivate IM and Presence Services, on page 26

Procedure

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

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

Step 2 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**.

Each domain name 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.

What to do next

If you are using TLS XMPP Federation, proceed to Regenerate XMPP Client and TLS Certificates, on page 29.

Delete IM Address Domains

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

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

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

Before you begin

Make sure that High Availability is disabled, and essential IM and Presence Services are stopped. For details, Deactivate IM and Presence Services, on page 26.

Procedure

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

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

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

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

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

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

What to do next

If you are using TLS XMPP Federation, proceed to Regenerate XMPP Client and TLS Certificates, on page 29.

Regenerate XMPP Client and TLS Certificates

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

Procedure

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

Step 2 Click **Find** to generate a list of the certificates.

Step 3 Click on the **cup-xmpp-s2s** certificate.

Step 4 In the **Certificate Details** window, click **Regenerate**.

Start IM and Presence Services

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

Before you begin

Regenerate XMPP Client and TLS Certificates, on page 29

Procedure

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

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

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

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

Step 4 Click **Restart**.

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

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

- **Cisco SIP Proxy**
- **Cisco Presence Engine**

Step 7 Click **Save**.

What to do next

Enable High Availability for Presence Redundancy Groups, on page 30

Enable High Availability for Presence Redundancy Groups

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

Before you begin

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

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

You should use the Cisco Real-Time Monitoring Tool (RTMT) to monitor performance counter `"Cisco Presence Engine" ActiveJsmSessions` on both Publisher and Subscriber in the following stages:

- after restarting the Publisher or Subscriber
- after restarting Cisco XCP Router
- after restarting Cisco Presence Engine

Make sure that before enabling High Availability, the number of `"Cisco Presence Engine" ActiveJsmSessions` must be the same as number of assigned users to the node.

Note You must enable High Availability only after users `ActiveJsmSessions` creation progress is completed.

Procedure

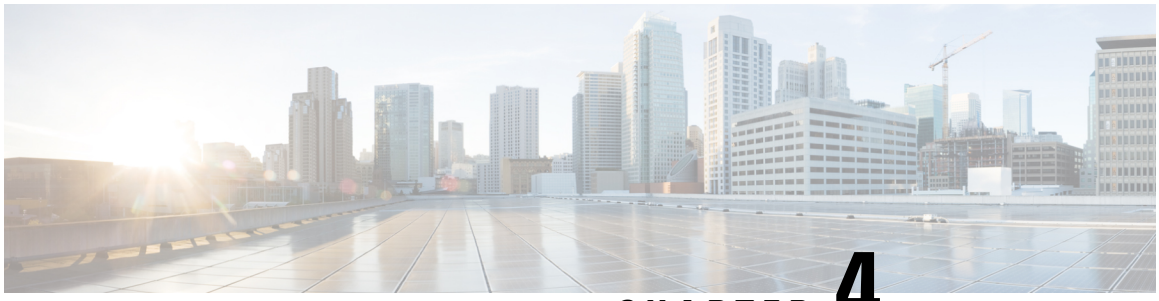
Step 1 From the Cisco Unified CM Administration user interface, choose **System** > **Presence Redundancy Groups**.

Step 2 Click **Find** and select the group.
The **Presence Redundancy Group Configuration** window displays.

Step 3 Check the **Enable High Availability** check box.

Step 4 Click **Save**.

Step 5 Repeat this procedure on each Presence Redundancy Group.



CHAPTER 4

Configure IPv6

Configure IPv6 Overview

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

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

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

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

For more information about using the Command Line Interface to configure IPv6 parameters, see the *Administration Guide for Cisco Unified Communications Manager* and the *Command Line Interface Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Configure IPv6 Task Flow

Procedure

	Command or Action	Purpose
Step 1	Enable IPv6 on Eth0 for IM and Presence Service, on page 34	Enable IPv6 on the Eth0 port of each IM and Presence Service node in the cluster. You must reboot each node to apply the changes.
Step 2	Enable IPv6 Enterprise Parameter, on page 35	After you enable IPv6 on the Eth0 port, you must enable the IPv6 enterprise parameter for the IM and Presence Service cluster.
Step 3	Restart Services , on page 35	You must restart IM and Presence services to apply the changes.
Step 4	Assign IPv6 Addresses to IM and Presence Nodes, on page 36	Assign IPv6 addresses to your IM and Presence Service nodes.

Enable IPv6 on Eth0 for IM and Presence Service

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

Procedure

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

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

Step 3 Choose the **Address Source**:

- Router Advertisement
- DHCP
- Manual Entry

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

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

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

Step 5 Click **Save**.

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

What to do next

Enable IPv6 Enterprise Parameter, on page 35

Enable IPv6 Enterprise Parameter

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

Before you begin

Enable IPv6 on Eth0 for IM and Presence Service, on page 34

Procedure

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

Step 2 In the **Enterprise Parameters Configuration** window, choose **True** in the IPv6 panel.

Step 3 Click **Save**.

What to do next

Restart Services , on page 35 to apply the changes.

Restart Services

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

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

Before you begin

Enable IPv6 Enterprise Parameter, on page 35

Procedure

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

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

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

Step 4 Click **Restart**.

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

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

- **Cisco SIP Proxy**
- **Cisco Presence Engine**

Step 7 Click **Save**.

Assign IPv6 Addresses to IM and Presence Nodes

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

Before you begin

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

Procedure

Step 1 Log in to the Cisco Unified Communications Manager publisher node

Step 2 From Cisco Unified CM Administration, choose **System** > **Server**.

Step 3 Complete one of the following tasks:

- To add a new server, click **Add New**.
- To update an existing server, click on the server that you want to edit.

Step 4 If you are adding a new server, from the **Server Type** drop-down menu, select **CUCM IM and Presence** and click **Next**.

Step 5 Enter the **IPv6 Address** for the server.

Step 6 Click **Save**.

Step 7 Repeat for each IM and Presence Service cluster node.

Disable IPv6 on Eth0 for IM and Presence Service

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

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

Procedure

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

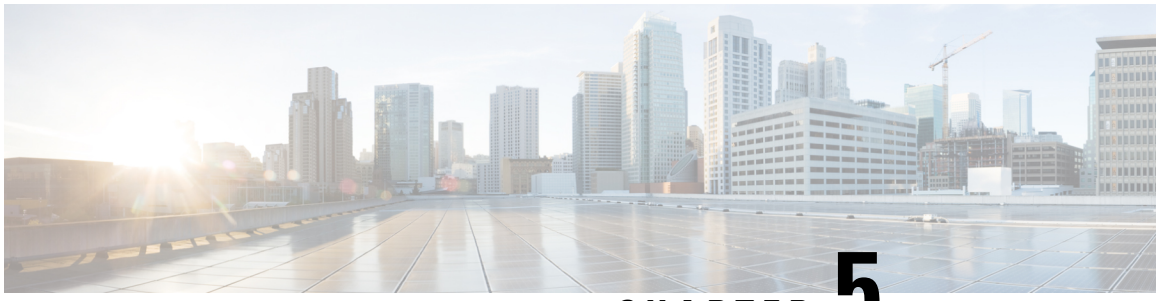
Step 2 In the Ethernet IPv6 Configuration window, uncheck the **Enable IPv6** check box.

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

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

Step 4 Click **Save**.

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



CHAPTER 5

Configure IM Addressing Scheme

IM Addressing Scheme Overview

The IM and Presence Service supports two IM addressing schemes:

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

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

IM Address Using User@Default_Domain

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

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

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

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

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

Although you can map the UserID to the email address, that does not mean the IM URI equals the email address. Instead it becomes *<email-address>@Default_Domain*. For example,

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.

IM Address Using Directory URI

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

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

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

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

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

For details on provisioning directory URIs from an external LDAP Directory, see Configure LDAP Directory, on page 73.

Multiple IM Domains

IM and Presence Service supports IM addressing across multiple IM address domains and automatically lists all domains in the system. You can add, edit, or delete domains. For information on configuring IM domains, see Configure the Domain Overview, on page 21.

If you are interoperating with Cisco Expressway, see the *Cisco Expressway Administrator Guide* at http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html.

IM Addressing Scheme Prerequisites

The IM and Presence Service default domain and the IM address scheme that you use must be consistent across all IM and Presence Service clusters. Before you begin, Configure the Default Domain on IM and Presence Service , on page 27.

The IM address scheme you set affects all user JIDs and cannot be performed in a phased manner without disrupting communication between clusters that may have different settings.

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

Configure IM Addressing Scheme Task Flow

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

Procedure

	Command or Action	Purpose
Step 1	Verify User Provisioning, on page 42	Verify that end users are correctly provisioned and that there are no duplicate or invalid users.
Step 2	Disable High Availability, on page 42	You must temporarily disable high availability for the presence redundancy group. Configuring the IM addressing scheme requires you to stop services temporarily; if you stop the services while high availability is enabled, a system failover will occur.
Step 3	Stop Services, on page 43	Prior to updating your IM addressing scheme configuration stop essential IM and Presence Services. Make sure to stop services in the prescribed order.
Step 4	Assign IM Addressing Scheme, on page 43	Use this procedure to configure a new domain and IM address scheme, or to update an existing domain and address scheme.
Step 5	Restart Services, on page 45	Once your IM addressing scheme is configured, restart services. You must do this prior to updating user address information or provisioning new users. Make sure to follow the prescribed order when you restart services.
Step 6	Enable High Availability, on page 46	You can enable high availability for the presence redundancy groups after you have configured the IM addressing scheme and restarted IM and Presence services. All services must be running on IM and Presence database publisher nodes and subscriber nodes before you enable high availability.
Step 7	If you chose **Directory URI** as the IM addressing scheme: • Assign the LDAP Source for Directory URIs, on page 47 • Manually Assign a Directory URI, on page 47	Optional. If you are syncing users from an external LDAP directory, set the LDAP source field for your directory URI values. For non-LDAP users, you must provision directory URIs manually. You can do this on a user-by-user basis, or via the Bulk Administration Tool.

Verify User Provisioning

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

Procedure

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Diagnostics** > **System Troubleshooter**. The System Troubleshooter runs.

Step 2 In the **User Troubleshooter** section, verify that end users are correctly provisioned and that there are no duplicate or invalid users.

What to do next

Disable High Availability, on page 42

Disable High Availability

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

Note The **Presence Redundancy Group Details** page shows all the active JSM sessions, even when the high availability is disabled in the cluster.

Before you begin

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

Procedure

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

Step 2 Click **Find** and select the group.

Step 3 On the Presence Redundancy Group Configuration window, uncheck the **Enable High Availability** check box.

Step 4 Click **Save**.

Step 5 Repeat this procedure for each Presence Redundancy Group.

Step 6 When you are done, wait at least two minutes to sync the new HA settings across the cluster before you make any further changes

What to do next

Stop Services, on page 43

Stop Services

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

Before you begin

Disable High Availability, on page 42

Procedure

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

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

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

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

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

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

- **Cisco XCP Router**

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

What to do next

Assign IM Addressing Scheme, on page 43

Assign IM Addressing Scheme

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

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

Before you begin

Stop Services, on page 43

Procedure

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

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

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

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

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

Step 4 Click **Save.**

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

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

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

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

What to do next

If you configured user@default_domain as the addressing scheme, and you are not using the Directory URI, then proceed to Restart Services, on page 45.

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

- Assign the LDAP Source for Directory URIs, on page 47
- Manually Assign a Directory URI, on page 47

IM Address Examples

Sample IM address options that are available for IM and Presence Service.

IM and Presence Service Default Domain: cisco.com **User:** John Smith **User ID:** js12345 **Mail ID:** jsmith@cisco-sales.com **SIPURI:** john.smith@webex.com

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

Restart Services

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

Before you begin

- Assign IM Addressing Scheme, on page 43
- If you configured Directory URI as the addressing scheme, complete one of the following options before you restart services:
  - Assign the LDAP Source for Directory URIs, on page 47
  - Manually Assign a Directory URI, on page 47

Procedure

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

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

- **Cisco XCP Router**

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

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

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

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

a) **Cisco Client Profile Agent**

b) **Cisco Sync Agent**

What to do next

Enable High Availability, on page 46

Enable High Availability

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

Before you begin

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

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

Procedure

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

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

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

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

Step 4 Click **Restart**.

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

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

- **Cisco SIP Proxy**
- **Cisco Presence Engine**

Step 7 Click **Save**.

Assign the LDAP Source for Directory URIs

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

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

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

Before you begin

Assign IM Addressing Scheme, on page 43

Procedure

Step 1 From Cisco Unified CM Administration, select **System** > **LDAP** > **LDAP Directory**.

Step 2 From the **Directory URI** drop-down list, select one of the following options:

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

Note The directory URI isn't provisioned until the LDAP sync occurs. For details on configuring an LDAP Directory sync, see Configure LDAP Directory, on page 73.

What to do next

Restart Services, on page 45

Manually Assign a Directory URI

If you are not using LDAP, you can use this procedure to enter a Directory URI manually on a user-by-user basis.

Note You can also use the Bulk Administration Tool to provision directory URIs for a large number of end users via a csv file. For Bulk Administration details, see the *Bulk Administration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

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

Before you begin

Assign IM Addressing Scheme, on page 43

Procedure

Step 1 In **Cisco Unified CM Administration**, choose **User Management** > **End User**.

Step 2 Enter the appropriate search criteria and click **Find**.

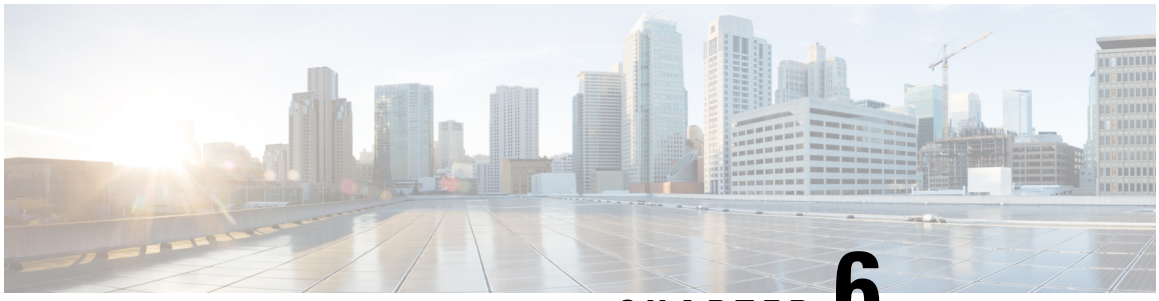
Step 3 Select the end user that you want to configure.

Step 4 In the **User Information** area, enter a directory URI in the **Directory URI** field.

Step 5 Click **Save**.

What to do next

Restart Services, on page 45



CHAPTER 6

Configure Redundancy and High Availability

Presence Redundancy Group Overview

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

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

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

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

High Availability

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

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

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

You can configure high availability using two different modes:

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

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

Presence Redundancy Group Prerequisites

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

Presence Redundancy Group Task Flow

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

Procedure

	Command or Action	Purpose
Step 1	Verify Database Replication, on page 51	Ensure that database replication is setup in the IM and Presence Service cluster.
Step 2	Verify Services, on page 51	Make sure critical services are running on the nodes that you plan to add to a presence redundancy group.
Step 3	Configure a Presence Redundancy Group, on page 52	Provide redundancy and recovery for IM and Presence Service clients and applications.
Step 4	Configure Heartbeat Interval for Failover, on page 53	Optional. Each node in the presence redundancy group monitors the status, or heartbeat, of its

	Command or Action	Purpose
		peer node. You can configure the intervals by which each node monitors its peer.
Step 5	Enable High Availability, on page 54	Optional. Follow this procedure if you did not enable high availability when you configured the presence redundancy group.
Step 6	Configure User Assignment Mode, on page 55	Configure how you want the Sync Agent to distribute users across various nodes in the IM and Presence Service cluster. This setting affects how your system handles failover and load balancing.

Verify Database Replication

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

Procedure

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

- From a remote system, use SSH to connect securely to the Cisco Unified Operating System. In your SSH client, enter your **ssh *adminname@hostname*** and enter your password.
- From a direct connection to the serial port, enter your credentials at the prompt that displays automatically.

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

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

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

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

What to do next

Verify Services, on page 51

Verify Services

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

Before you begin

Verify Database Replication, on page 51

Procedure

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

Step 2 From the **Server** list, choose the appopriate node and click **Go**.

Step 3 In the **IM and Presence Services** area, ensure that the following services are started:

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

Step 4 From the **Related Links** drop-down list, select **Control Center - Network Services** and click **Go**.

Step 5 In the **IM and Presence Services** area, ensure that the following services are started:

- **Cisco SIP Proxy**
- **Cisco Presence Engine**

What to do next

Configure a Presence Redundancy Group, on page 52

Configure a Presence Redundancy Group

Use Cisco Unified Communications Manager to configure redundancy for IM and Presence Service nodes.

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

Before you begin

- Verify Services, on page 51
- Ensure that the IM and Presence Service nodes you are adding to a presence redundancy group are running the same software version.

Procedure

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

Step 2 Click **Add New**.

Step 3 Enter a unique name for the presence redundancy group.

You can enter a maximum of 128 alphanumeric characters, including underscore (_) and dash (-).

Step 4 Enter a description of the group.

You can enter a maximum of 128 alphanumeric characters including symbols, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), forward slash (\), or angle brackets (<>).

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

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

Step 7 Click **Save**.

What to do next

Configure Heartbeat Interval for Failover, on page 53

Configure Heartbeat Interval for Failover

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

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

Procedure

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

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

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

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

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

- **Keep Alive (Heartbeat) Timeout**—This parameter specifies the duration in seconds that the heartbeat can be lost with the peer before failover is initiated. the default is 60.
- **Keep Alive (HeartBeat) Interval**—This parameter specifies the interval in seconds between keep alive (heart beat) messages being sent to the peer. The default is 15.
- **Enable monitoring of XCP Authentication Service** — Use this parameter to configure the system to monitor the Cisco XCP Authentication Service and initiate automatic failover to a peer node when the service fails on a node. In the **Enable monitoring of XCP Authentication Service** field set the value of service parameter to **TRUE**.

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

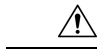
- **Client Re-Login Lower Limit**—This parameter specifies the minimum number of seconds which CUPC 8.5 (and higher) should wait before attempting to re-login to this server. The default is 120.
- **Client Re-Login Upper Limit**—This parameter specifies the maximum number of seconds which CUPC 8.5 (and higher) should wait before attempting to re-login to this server. The default is 537.

Step 6 Click **Save**.

What to do next

If you did not enable high availability when you configured the presence redundancy group, Enable High Availability, on page 54 now.

Enable High Availability



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

Before you begin

- Configure a Presence Redundancy Group, on page 52
- Ensure that replication is set up in the IM and Presence Service cluster.
- Ensure that all critical services are running.

Procedure

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

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

Step 3 Choose the presence redundancy group that you configured.

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

Step 5 Click **Save**.

Configure User Assignment Mode

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

Procedure

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

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

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

Step 3 Click **Save**.

Initiate Manual Failover, Fallback, or Recovery

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

- Manual failover—When you initiate a manual failover, the **Cisco Server Recovery Manager** stops the critical services on the failed node. All users from the failed node are disconnected and must re-login to the backup node. Critical services will not be restarted unless we invoke manual fallback.
- Manual fallback—When you initiate a manual fallback, the **Cisco Server Recovery Manager** restarts critical services on the primary node and disconnects all users that had been failed over. Those users must then re-login to their assigned node.
- Manual recovery—A manual recovery is necessary when both nodes in the presence redundancy group are in the failed state. In this case, the IM and Presence Service restarts the **Cisco Server Recovery Manager** service on both nodes in the presence redundancy group.

Procedure

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

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

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

- Click **Failover** to initiate failover of an active node.

- Click **Fallback** to initate fallback of a failed over node.
- Click **Recover** if both nodes are failed over and you want to recover them.

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

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

Node State Definitions

Table 4: 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.

State	Description
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 5: 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.

Node 1		Node 2		
State	**Reason**	**State**	**Reason**	**Cause/Recommended Actions**
Taking Back	Initialization	Falling Back	On Admin Request	The administrator restarts the SRM service on node 1 while taking back, but before the heartbeat on node 2 times out. After the taking back process is complete, both nodes are in Normal state.
Taking Back	Automatic Fallback	Falling Back	Automatic Fallback	Automatic Fallback has been initiated from node 2 to node 1 and is currently in progress.
Failed Over	Initialization or Critical Services Down	Running in Backup Mode	Critical Service Down	Node 1 transitions to Failed Over state when 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.

IM and Presence Failover Enhancement to Nearly Zero Downtime

Prerequisites:

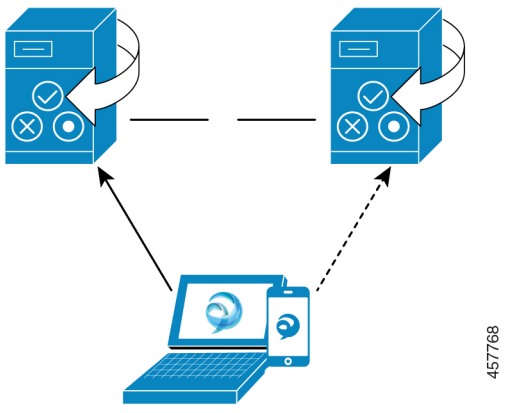
- Release compatibility: Cisco Unified CM and IM and Presence release 14, Jabber release 14 and Expressway 14, in case of Mobile and Remote Access users.

IM and Presence Service eliminates the service outage during the High Availability failover event, and allows seamless transition of Cisco Jabber clients to the secondary/backup server.

From release 14, IM and Presence Service supports dual connection with Jabber clients. When enabled on the client side, this type of connection ensures much shorter (nearly zero) service downtime during High Availability failover events.

You can enable this feature with some additional configuration in the Jabber client. For more information on how to enable dual connection in Jabber, see *EnableDualConnections* and *Inactive_Connection_Activation_Timer* parameters in the Parameters Reference Guide for Cisco Jabber 14.

Figure 2: IM Presence Failover Enhancement



In case of failover, this enhancement helps minimize the downtime to nearly zero. This is accomplished by enabling Cisco Jabber client to maintain dual connection with IM and Presence nodes. An active connection is maintained with the primary node that is created during client login process. The inactive connection with the backup node is created after random number of seconds between the values of *Client Re-Login Lower Limit* and *Client Re-Login Upper Limit*. These limits are configured as the service parameters for the Cisco Server Recovery Manager service.

When a failover happens, Jabber client activates the 'inactive' connection to communicate to the server. Since an inactive connection is already created on the backup node, it results the Jabber downtime to minimal.

Note Because of Cisco Jabber client limitation, this failover enhancement (for Jabber) will not work with the unrestricted (XU) version of the IM and Presence service. This is because the secure TLS connection between XMPP clients like Jabber and the IM and Presence service is disabled in the unrestricted version.

In restricted version, the **Enable XMPP Client to IM/P Service Secure Mode** option is enabled by default in the **Security Settings** page (**System** > **Security** > **Settings**) that enables failover enhancement to work with Jabber. We recommend not to turn off this mode if you want to use failover enhancement. See CSCvx94284 for more information on this limitation.

How to Check if Dual Registration is Established

To ensure that the dual registration is established, consider a scenario where you have assigned X users on the primary node and Y on the secondary node. When you check the *JsmSessionsClient* and *JsmSessionsClientInactive* counters on the primary node, you can see the total number of users connected to the *JsmSessionsClient* is X and *JsmSessionsClientInactive* is Y. At the same time, on the secondary node, the total number of users connected to the *JsmSessionsClient* is Y and *JsmSessionsClientInactive* is X.

How to Disable Dual Registration

You can disable dual registration by disabling HA on the client side without disabling HA in the server. Moreover, if you disable HA then the dual registration will not be offered from the server to the client and the client cannot try to establish inactive connection. For more information on how to enable dual connection in Jabber, see *EnableDualConnections* and *Inactive_Connection_Activation_Timer* parameters in the Parameters Reference Guide for Cisco Jabber 14.

Counters to Monitor Zero Downtime During Upgrade

To track the upgrade process to ensure zero downtime, you can monitor the following counters via the Real-Time Monitoring Tool:

Table 6: Counters to monitor zero downtime during upgrade

Counter	Description
ActiveJsmSessions	This counter provides the number of active users assigned to the publisher node. During the failover, it shows zero for the primary (upgraded) node and adds up the active users from the primary node to the backup node.
InactiveJsmSessions	This counter provides the number of active users assigned to the subscriber node.

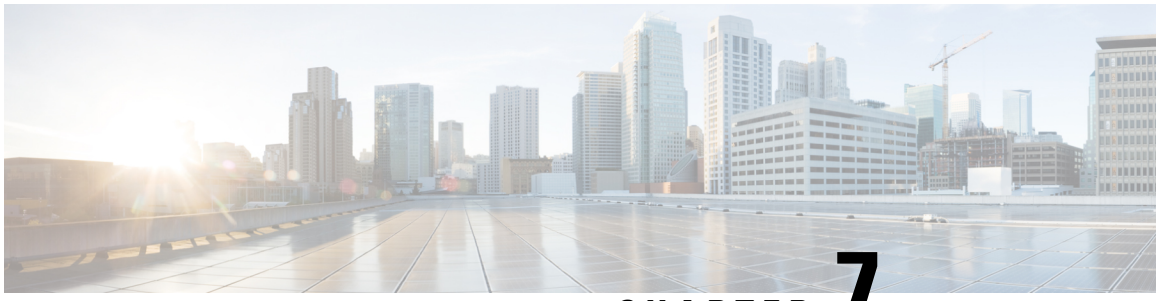
Counter	Description
JsmSessionsComposed	This counter represents the number of Composed sessions active for the JSM.
JsmSessionsClientInactive	This counter represents the number of Client sessions inactive for the JSM.
JsmSessionsClient	This counter represents the number of Client sessions active for the JSM.
JsmSessionsClientInactive	This counter represents the number of Client sessions inactive for the JSM.

Redundancy Interactions and Restrictions

Feature	Interaction
Adding Users	You cannot add new users to an IM and Presence Service cluster while one of the cluster nodes is in a failover state.
Multiple Device Messaging	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.

Feature	Interaction
Push Notifications High Availability	High Availability is supported for Push Notifications deployments as of 11.5(1)SU3. If Push Notifications is enabled, and a node fails over, the following occurs for Cisco Jabber on iPhone and iPad clients: • For Cisco Jabber clients in foreground mode, the Jabber client logs in automatically to the backup node, which takes over until the main node recovers. There is no interruption in services, either when the backup node takes over, or when the main node recovers. • For Cisco Jabber clients in background mode, the backup node takes over, but there is a delay before any Push Notifications are sent. Because the Jabber client is in background mode, it does not have an active connection to the network so it doesn't log in automatically to the backup node. The backup node must recreate JSM sessions for all failed over users who were in background mode before any Push Notifications can be sent. The length of the delay depends on the system load. Testing has shown that for a 15,000 user OVA with users evenly distributed in an HA pair, it takes 10-20 minutes for Push Notifications to be sent following a failover. This delay is observed when the backup node takes over, and again after the main node recovers. **Note** In the event of a node failure or unexpected crash of the Cisco XCP Router, the user's IM session, including the IM history, is maintained without the need for any user action. However, if the Cisco Jabber on iPhone or iPad client was in suspended mode, it will be unable to retrieve unread messages that were queued on the server when it crashed.
Temporary presence status of a user	The temporary presence status of a user displays the stale presence status after Failover, Fallback, and user moves. This is because the subscription to temporary presence will be deleted and the user must re-subscribe to temporary presence to see the valid temporary presence status of the user. For example, If User A is subscribed to user B's temporary presence and a failover occurs on the IM and Presence node where User B is assigned, then user B displays offline to User A even after User B re-logins to the backup node. It is because the subscription to temporary presence of User B is deleted and User A is not aware of the deletion. User A must re-subscribe to temporary presence of User B again. When User A deletes search of User B from Jabber client, User A needs to wait at least 30 seconds before It tries to search the temporary presence of User B. If not, then User A sees the stale presence of User B. Jabber client must wait for at least 30 seconds between two searches for same user to get a valid temporary presence status.

Feature	Interaction
IM and Presence status	When a user is moved from one Presence Redundancy Group to another, The user has to be logged out from Jabber session, for the IM and Presence status to be visible in the current Presence Redundancy Group which the user has moved into.



CHAPTER 7

Configure User Settings

End User Settings Overview

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

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

Service Profiles

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

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

- For LDAP Synchronized Users—If you have imported end users from an LDAP directory, you can assign the service profile to a feature group template and then apply that feature group template to your end users. The settings in the template get applied to all synchronized users.
- For Active Local Users (i.e. non-LDAP users)—To apply settings to a large number of users at once, use the Bulk Administration Tool to apply service profile settings via a csv file or spreadsheet. For details on how to use the Bulk Administration Tool at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

  Otherwise, you can configure user settings manually, on a user-by-user basis.

Feature Group Template Overview

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

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

- User Profile—contains a set of common phone and phone line settings. You must configure the user profile with a universal line template, which assigns the common phone line settings, and a universal device template, which assigns the common phone settings. These templates assist users who are set up for self-provisioning to configure their own phones.
- Service Profile—contains a group of common UC services, such as the IM and Presence Service, directory, or voicemail.

User Settings Prerequisites

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

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

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 Presence 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.

Configure User Settings Task Flow

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

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

Procedure

	Command or Action	Purpose
Step 1	Configure the User Assignment Mode, on page 69	Set the user assignment mode to balanced, active-stand-by, or none.
Step 2	Add an IM and Presence UC Service, on page 70	Set up an IM and Presence UC service on Cisco Unified Communications Manager.
Step 3	Configure a Service Profile, on page 70	Configure a service profile that contains the IM and Presence UC service that you added.
Step 4	Configure a Feature Group Template, on page 71	Configure a feature group template that includes the service profile that you set up in addition to other common feature settings.

What to do next

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

Configure the User Assignment Mode

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

Procedure

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

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

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

Step 3 Click **Save**.

What to do next

Add an IM and Presence UC Service, on page 70

Add an IM and Presence UC Service

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

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **UC Service**.

Step 2 Click **Add New**.

Step 3 From the **UC Service Type** drop-down list box, choose **IM and Presence**.

Step 4 From the **Product Type** drop-down list box, choose **Unified CM (IM and Presence)**.

Step 5 Enter a **Name** and **Description** for the IM and Presence service.

Step 6 In the **Hostname/IP Address** field, enter a hostname, IP address, or DNS SRV for the server that hosts the IM and Presence Service.

Step 7 Click **Save**.

What to do next

To enable users for the IM and Presence Service, assign the UC Service to a Service Profile and assign that profile to you users.

Configure a Service Profile, on page 70.

Configure a Service Profile

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

Before you begin

Add an IM and Presence UC Service, on page 70

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Service Profile**.

Step 2 Do either of the following

- Click **Find** and select an existing profile
- Click **Add New** to create a new profile

Step 3 In the **IM and Presence Profile** section, select the **Primary** IM and Presence server.

Step 4 Complete the remaining fields in the **Service Profile Configuration** window. For help with the fields and their settings, see the online help

Step 5 Click **Save**.

What to do next

Configure a Feature Group Template, on page 71

Configure a Feature Group Template

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

Before you begin

Configure a Service Profile, on page 70

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Feature Group Template**.

Step 2 Click **Add New**.

Step 3 Enter a **Name** and **Description** for the Feature Group Template.

Step 4 Check the **Home Cluster** check box if you want to use the local cluster as the home cluster for all users whom use this template.

Step 5 Check the **Enable User for Unified CM IM and Presence** check box to allow users whom use this template to exchange instant messaging and presence information.

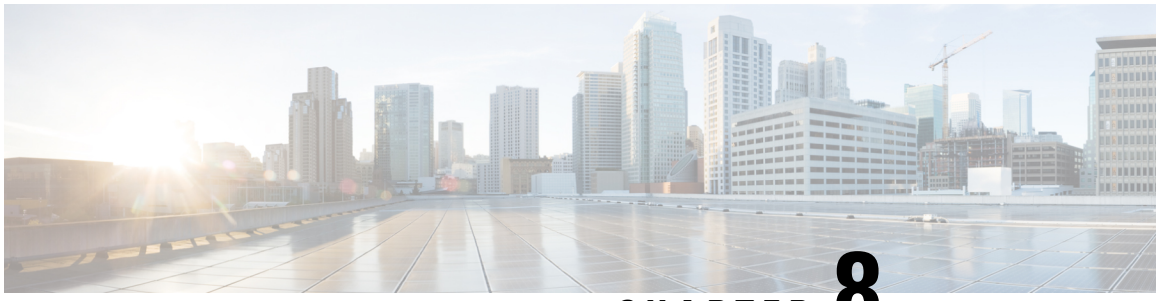
Step 6 From the drop-down list, select a **Services Profile** and **User Profile**.

Step 7 Complete the remaining fields in the **Feature Group Template Configuration** window. Refer to the online help for field descriptions.

Step 8 Click **Save**.

What to do next

Configure an LDAP Directory sync that includes this feature group template. When you complete the LDAP Sync, the IM and Presence settings in the template get applied to synchronized users. See LDAP Synchronization Configuration Task Flow, on page 75.



CHAPTER 8

Configure LDAP Directory

LDAP Synchronization Overview

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

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

See the *Compatibility Matrix for Cisco Unified Communications Manager and the IM and Presence Service* for information on the supported LDAP directories.

LDAP synchronization advertises the following functionalities:

- **Importing End Users**—You can use LDAP synchronization during the initial system setup to import your user list from a company LDAP directory into the Unified Communications Manager database. If you've preconfigured items such as feature group templates, user profiles, service profiles, universal device and line templates, you can apply configurations to your users, and assign configured directory numbers and directory URIs during the sync process. The LDAP synchronization process imports the list of users and user-specific data and applies the configuration templates that you've set up.

Note You cannot make edits to an LDAP synchronization once the initial synchronization has occurred already.

- **Scheduled Updates**—You can configure Unified Communications Manager to synchronize with multiple LDAP directories at scheduled intervals to ensure that the database is updated regularly and user data is up-to-date.

- **Authenticate End Users**—You can configure your system to authenticate end user passwords against the LDAP directory rather than the Cisco Unified Communications Manager database. LDAP authentication provides companies with the ability to assign a single password to end users for all company applications. This functionality does not apply to PINs or application user passwords.
- **Directory Server User Search for Cisco Mobile and Remote Access Clients and Endpoints**—You can search a corporate directory server even when operating outside the enterprise firewall. When this feature is enabled, the User Data Service (UDS) acts as a proxy and sends the user search request to the corporate directory instead of sending it to the Unified Communications Manager database.

LDAP Authentication for End Users

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

Directory Server User Search for Cisco Mobile and Remote Access Clients and Endpoints

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

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

Use this feature to achieve the following results:

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

To configure this feature, you must enable the **Enable user search to Enterprise Directory Server** option in the **LDAP Search Configuration** window, and configure the LDAP directory server details. For details, see the Configure Enterprise Directory User Search, on page 80 procedure.

LDAP Synchronization Prerequisites

Prerequisite Tasks

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

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

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

LDAP Synchronization Configuration Task Flow

Use the following tasks to pull a user list from the external LDAP directory and import it into the Unified Communications Manager database.

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

Procedure

	Command or Action	Purpose
Step 1	Activate the Cisco DirSync Service, on page 76	Log in to Cisco Unified Serviceability and activate the Cisco DirSync service.
Step 2	Enable LDAP Directory Synchronization, on page 76	Enable LDAP directory synchronization in Unified Communications Manager.
Step 3	Create an LDAP Filter, on page 77	**Optional**. Create an LDAP filter if you want Unified Communications Manager to synchronize only a subset of users from your corporate LDAP directory.
Step 4	Configure LDAP Directory Sync, on page 77	Configure settings for the LDAP directory sync such as field settings, LDAP server locations, synchronization schedules, and assignments for access control groups, feature group templates, and primary extensions.
Step 5	Configure Enterprise Directory User Search, on page 80	**Optional**. Configure the system for enterprise directory server user searches. Follow this

	Command or Action	Purpose
		procedure to configure phones and clients in your system to perform user searches against an enterprise directory server instead of the database.
Step 6	Configure LDAP Authentication, on page 81	**Optional**. If you want to use the LDAP directory for end user password authentication, configure LDAP authentication settings.
Step 7	Customize LDAP Agreement Service Parameters, on page 82	**Optional**. Configure the optional LDAP Synchronization service parameters. For most deployments, the default values are sufficient.

Activate the Cisco DirSync Service

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

Procedure

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

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

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

Step 4 Click **Save**.

Enable LDAP Directory Synchronization

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

Note If you have already synced the LDAP directory once, you can still sync new users from your external LDAP directory, but you cannot add new configurations in Unified Communications Manager to the LDAP directory sync. You also cannot add edits to underlying configuration items such as the feature group template or user profile. If you have already completed one LDAP sync, and want to add users with different settings, you can use Bulk Administration menus such as Update Users or Insert Users.

Procedure

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

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

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

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

Step 5 Click **Save**.

Create an LDAP Filter

You can create an LDAP filter to limit your LDAP synchronization to a subset of users from your LDAP directory. When you apply the LDAP filter to your LDAP directory, Unified Communications Manager imports only those users from the LDAP directory who match the filter.

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

Procedure

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

Step 2 Click **Add New** to create a new LDAP filter.

Step 3 In the **Filter Name** text box, enter a name for your LDAP filter.

Step 4 In the **Filter** text box, enter a filter. The filter can contain a maximum of 1024 UTF-8 characters and must be enclosed in parentheses ().

Step 5 Click **Save**.

Configure LDAP Directory Sync

Use this procedure to configure Unified Communications Manager to synchronize with an LDAP directory. LDAP directory synchronization allows you to import end user data from an external LDAP directory into the Unified Communications Manager database such that it displays in End User Configuration window. If you have setup feature group templates with universal line and device templates, you can assign settings to newly provisioned users and their extensions automatically.

Tip If you are assigning access control groups or feature group templates, you can use an LDAP filter to limit the import to the group of users with the same configuration requirements.

Procedure

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

Step 2 Perform one of the following steps:

- Click **Find** and select an existing LDAP directory.
- Click **Add New** to create a new LDAP directory.

Step 3 In the **LDAP Directory Configuration** window, enter the following:

a) In the **LDAP Configuration Name** field, assign a unique name to the LDAP directory.
b) In the **LDAP Manager Distinguished Name** field, enter a user ID with access to the LDAP directory server.
c) Enter and confirm the password details.
d) In the **LDAP User Search Space** field, enter the search space details.
e) In the **LDAP Custom Filter for Users Synchronize** field, select either **Users Only** or **Users and Groups**.
f) (Optional). If you want to limit the import to only a subset of users who meet a specific profile, from the **LDAP Custom Filter for Groups** drop-down list, select an LDAP filter.

Step 4 In the **LDAP Directory Synchronization Schedule** fields, create a schedule that Unified Communications Manager uses to synchronize data with the external LDAP directory.

Step 5 Complete the **Standard User Fields to be Synchronized** section. For each End User field, choose an LDAP attribute. The synchronization process assigns the value of the LDAP attribute to the end user field in Unified Communications Manager.

Step 6 If you are deploying URI dialing, make sure to assign the LDAP attribute that will be used for the user's primary directory URI address.

Step 7 In the **Custom User Fields To Be Synchronized** section, enter custom user field name with the required LDAP attribute.

Step 8 To assign the imported end users to an access control group that is common to all the imported end users, do the following

a) Click **Add to Access Control Group**.
b) In the pop-up window, click the corresponding check box for each access control group that you want to assign to the imported end users.
c) Click **Add Selected**.

Step 9 If you want to assign a feature group template, select the template from the **Feature Group Template** drop-down list.

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

Step 10 If you want to assign a primary extension by applying a mask to imported telephone numbers, do the following:

a) Check the **Apply mask to synced telephone numbers to create a new line for inserted users** check box.
b) Enter a **Mask**. For example, a mask of 11XX creates a primary extension of 1145 if the imported telephone number is 8889945.

Step 11 If you want to assign primary extensions from a pool of directory numbers, do the following:

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

Step 12 (Optional) In the Jabber Endpoint Provisioning section, select one of the required Jabber devices for auto provisioning from the following drop-down in case you want to create a Jabber device:

- Cisco Dual Mode for Android (BOT)
- Cisco Dual Mode for iPhone (TCT)
- Cisco Jabber for Tablet (TAB)
- Cisco Unified Client Services Framework (CSF)

Note The **Write back to LDAP** option allows you to write the Primary DN chosen from Unified CM back to the LDAP server. LDAP attributes available for write back are: **telephoneNumber**, **ipPhone**, and **mobile**.

Step 13 In the **LDAP Server Information** section, enter the hostname or IP address of the LDAP server.

Step 14 If you want to use TLS to create a secure connection to the LDAP server, check the **Use TLS** check box.

Note Sometimes, when we try to synchronize users through the secure port after restarting tomcat, the users will not be synchronized. You must restart the Cisco DirSync service for the user synchronization to happen successfully.

Step 15 Click **Save**.

Step 16 To complete an LDAP sync, click **Perform Full Sync Now**. Otherwise, you can wait for the scheduled sync.

Note When users are deleted in LDAP, they will automatically be removed from Unified Communications Manager after 24 hours. Also, if the deleted user is configured as a mobility user for any of the following devices, these inactive devices will also be automatically deleted:

- Remote Destination Profile
- Remote Destination Profile Template
- Mobile Smart Client
- CTI Remote Device
- Spark Remote Device
- Nokia S60
- Cisco Dual Mode for iPhone
- IMS-integrated Mobile (Basic)
- Carrier-integrated Mobile
- Cisco Dual Mode for Android

Configure Enterprise Directory User Search

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

Before you begin

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

Procedure

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

Step 2 To enable user searches to be performed using an enterprise LDAP directory server, check the **Enable user search to Enterprise Directory Server** check box.

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

Step 4 Click **Save**.

Note To search conference rooms represented as Room objects in OpenLDAP Server, configure the custom filter as (| (objectClass=intOrgPerson)(objectClass=rooms)). This allows Cisco Jabber client to search conference rooms by their name and dial the number associated with the room.

Conference rooms are searchable provided **givenName** or **sn** or **mail** or **displayName** or **telephonenumber** attribute is configured in the OpenLDAP server for a room object.

LDAP Attributes for UDS Search of Directory Server

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

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

UDS Users Response Tag	LDAP Attribute
userName	• samAccountName • uid
firstName	givenName

UDS Users Response Tag	LDAP Attribute
lastName	sn
middleName	• initials • middleName
nickName	nickName
displayName	displayName
phoneNumber	• telephonenumber • ipPhone
homeNumber	homephone
mobileNumber	mobile
email	mail
directoryUri	• msRTCSIP-primaryuseraddress • mail
department	• department • departmentNumber
manager	manager
title	title
pager	pager

Configure LDAP Authentication

Perform this procedure if you want to enable LDAP authentication so that end user passwords are authenticated against the password that is assigned in the company LDAP directory. This configuration applies to end user passwords only and does not apply to end user PINs or application user passwords.

Procedure

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

Step 2 Check the **Use LDAP Authentication for End Users** check box to use your LDAP directory for user authentication.

Step 3 In the **LDAP Manager Distinguished Name** field, enter the user ID of the LDAP Manager who has access rights to the LDAP directory.

Step 4 In the **Confirm Password** field, enter the password for the LDAP manager.

Step 5 In the **LDAP User Search Base** field, enter the search criteria.

Step 6 In the **LDAP Server Information** section, enter the hostname or IP address of the LDAP server.

Step 7 If you want to use TLS to create a secure connection to the LDAP server, check the **Use TLS** check box.

Step 8 Click **Save**.

What to do next

Customize LDAP Agreement Service Parameters, on page 82

Customize LDAP Agreement Service Parameters

Perform this procedure to configure the optional service parameters that customize the system-level settings for LDAP agreements. If you do not configure these service parameters, Unified Communications Manager applies the default settings for LDAP directory integration. For parameter descriptions, click the parameter name in the user interface.

You can use service parameters to customize the below settings:

- **Maximum Number of Agreements**—Default value is 20.
- **Maximum Number of Hosts**—Default value is 3.
- **Retry Delay On Host Failure (secs)**—Default value for host failure is 5.
- **Retry Delay On HotList failure (mins)**—Default value for hostlist failure is 10.
- **LDAP Connection Timeouts (secs)**—Default value is 5.
- **Delayed Sync Start time (mins)**—Default value is 5.
- **User Customer Map Audit Time**

Procedure

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

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

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

Step 4 Configure values for the Cisco DirSync service parameters.

Step 5 Click **Save**.

LDAP Directory Service Parameters

Service Parameter	Description
Maximum Number Of Agreements	The maximum number of LDAP directories that you can configure. The default setting is 20.

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

Convert LDAP Synchronized User to Local User

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

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

Procedure

Step 1 In Cisco Unified CM Administration, choose **End Users** > **End User Management**.

Step 2 Click **Find** and select the end user.

Step 3 Click the **Convert to Local User** button.

Step 4 Make your updates in the **End User Configuration** window.

Step 5 Click **Save**.

Assign LDAP Synchronized Users to an Access Control Group

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

Before you begin

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

Procedure

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

Step 2 Click **Find** and select a configured LDAP Directory.

Step 3 Click the **Add to Access Control Group** button.

Step 4 Select the access control groups that you want to apply to the end users in this LDAP directory.

Step 5 Click **Add Selected**.

Step 6 Click **Save**

Step 7 Click **Perform Full Sync**.
Cisco Unified Communications Manager syncs with the external LDAP directory and synchronized users get inserted into the correct access control group.

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

LDAP Directory Integration for Contact Searches on XMPP Clients

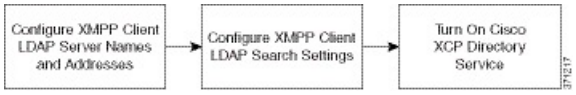
These topics describe how to configure the LDAP settings on IM and Presence Service to allow users of third-party XMPP client to search and add contacts from the LDAP directory.

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 3: 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 7: 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.

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 8: 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).

Field	Setting
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.

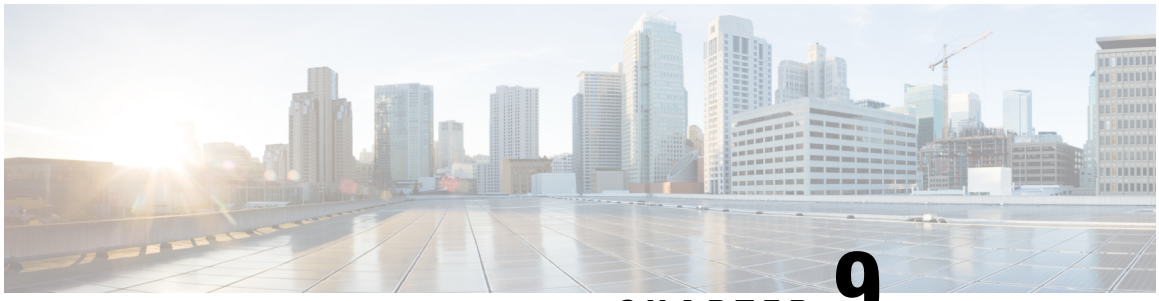
Procedure

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 9

Configure Cisco Unified Communications Manager for IM and Presence Service

Integration Overview

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

Cisco Unified Communications Manager Integration Prerequisites

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

The table below lists essential configuration tasks for IM and Presence Service integration. Refer to the online help for descriptions of fields and their options.

Table 9: Required Configuration on Cisco Unified Communications Manager

Task	Description
Modify the User Credential Policy	We recommend that you set an expiration date on the credential policy for users. The only type of user that does not require a credential policy expiration date is an Application user. Cisco Unified Communications Manager does not use the credential policy if you are using an LDAP server to authenticate your users on Cisco Unified Communications Manager. **Cisco Unified CM Administration** > **User Management** > **User Settings** > **Credential Policy Default**
Configure the phone devices, and associate a Directory Number (DN) with each device	Enable **Allow Control of Device from CTI** to allow the phone to interoperate with the client. **Cisco Unified CM Administration** > **Device** > **Phone**
Configure the users, and associate a device with each user	Ensure that the user ID value is unique for each user. **Cisco Unified CM Administration** > **User Management** > **End User**
Associate a user with a line appearance	For details, see: **Cisco Unified CM Administration** > **Device** > **Phone**
Add users to CTI-enabled user group	To enable desk phone control, you must add the users to a CTI-enabled user group. **Cisco Unified CM Administration** > **User Management** > **User Group**
Certificate exchange	The certificate exchange between Cisco Unified Communications Manager and the IM and Presence Service is handled automatically during the installation process. However, if there is an issue and you need to complete the certificate exchange manually, refer to Certificate Exchange with Cisco Unified Communications Manager, on page 135.

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.

SIP Trunk Configuration on Cisco Unified Communications Manager

Complete these tasks to configure the SIP trunk connection to Cisco Unified Communications Manager.

Procedure

	Command or Action	Purpose
Step 1	Configure a SIP Trunk Security Profile, on page 93	Configure a SIP Trunk Security Profile for the trunk connection between Cisco Unified Communications Manager and the IM and Presence Service.
Step 2	Configure SIP Trunk for IM and Presence Service, on page 94	Assign the SIP Trunk Security Profile to a SIP trunk and configure the trunk connection between Cisco Unified Communications Manager and IM and Presence Service.
Step 3	Configure SRV Cluster Name, on page 95	Optional. Complete this procedure only if you are using DNS SRVs on the SIP trunk between Cisco Unified Communications Manager and the IM and Presence Service and you use an SRV address other than the IM and Presence default domain. In this case, configure the **SRV Cluster Name** service parameter. Otherwise, you can skip this task.
Step 4	Configure the Presence Gateway, on page 96	On the IM and Presence Service, assign Cisco Unified Communications Manager as a presence gateway, thereby allowing the systems to exchange Presence information.
Step 5	Configure a SIP PUBLISH Trunk, on page 96	Optional. Use this procedure to configure a SIP PUBLISH trunk for IM and Presence. When you turn on this setting, Cisco Unified Communications Manager publishes phone presence for all line appearances that are associated with users licensed on Cisco Unified Communications Manager for the IM and Presence Service.
Step 6	Verify Services on Cisco Unified Communications Manager, on page 97	Verify that required services are running on Cisco Unified Communications Manager.
Step 7	Configure Phone Presence from Off-Cluster Cisco Unified Communications Manager, on page 97	Configure Cisco Unified Communications Manager as a TLS Peer subject of the IM and Presence Service. TLS is required if you want to allow phone presence from a Cisco Unified Communications Manager that is outside of the IM and Presence Service cluster.

Configure a SIP Trunk Security Profile

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

Procedure

Step 1 In **Cisco Unified CM Administration** > **System** > **Security** > **SIP Trunk Security Profile**, click **Find**.

Step 2 Click **Non Secure SIP Trunk Profile**.

Step 3 Click **Copy**.

Step 4 Enter a **Name** for the profile. For example, `IMP-SIP-Trunk-Profile`.

Step 5 Complete the following settings:

- The **Device Security Mode** is set to **Non Secure**.
- The**Incoming Transport Type** is set to **TCP+UDP**.
- The**Outgoing Transport Type** is set to **TCP**.

Step 6 Check the following check boxes:

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

Step 7 Click **Save**.

What to do next

Configure SIP Trunk for IM and Presence Service, on page 94

Configure SIP Trunk for IM and Presence Service

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

Before you begin

Configure a SIP Trunk Security Profile, on page 93

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Trunk**

Step 2 Click **Add New**.

Step 3 From the **Trunk Type** drop-down list box, choose **SIP Trunk**.

Step 4 From the **Device Protocol** drop-down list box, choose **SIP**.

Step 5 From the **Trunk Service Type** drop-down list box, choose **None**.

Step 6 Click **Next**.

Step 7 In the **Device Name** field, enter a name for the trunk. For example, `IMP-SIP-Trunk`.

Step 8 Select a **Device Pool** from the drop-down list box.

Step 9 In the **SIP Information** section, assign the trunk to the IM and Presence Service by entering the address information for the IM and Presence cluster:

- If you are using a DNS SRV record for the IM and Presence Service, check the **Destination Address is an SRV** check box and enter the SRV in the **Destination Address** field.
- Otherwise, in the **Destination Address** field, enter the IP address or FQDN of the IM and Presence publisher node. Click the **(+)** button to add additional nodes. You can enter up to 16 nodes.

a) In the **Destination Address** field, enter the IP Address, FQDN, or DNS SRV of 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_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.

Step 10 For the **Destination Port**, enter `5060`

Step 11 From the **SIP Trunk Security Profile** drop-down list box, choose the SIP trunk security profile that you created in the previous task.

Step 12 From the **SIP Profile** drop-down list box, choose a profile. for example, the **Standard SIP Profile**

Step 13 Click **Save**.

What to do next

If you are using DNS SRVs on the SIP trunk between Cisco Unified Communications Manager and the IM and Presence Service and you use an address other than the IM and Presence default domain, Configure SRV Cluster Name, on page 95.

Otherwise, Configure a SIP PUBLISH Trunk, on page 96.

Configure SRV Cluster Name

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

Procedure

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

Configure a SIP PUBLISH Trunk

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

Procedure

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Presence** > **Settings** > **Standard Configuration**.
Step 2 From the **CUCM IM and Presence Publish Trunk** drop-down, select the SIP trunk that you configured on Cisco Unified Communications Manager for the IM and Presence Service.
Step 3 Click **Save**.

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

What to do next

Verify Services on Cisco Unified Communications Manager, on page 97

Configure the Presence Gateway

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

Procedure

Step 1 From **Cisco Unified CM IM and Presence Administration** > **Presence** > **Gateways**.
Step 2 Click **Add New**.
Step 3 From the **Presence Gateway** drop-down list box, choose **CUCM**.
Step 4 Enter a **Description**.

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

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

Step 6 Click **Save**.

What to do next

Configure a SIP PUBLISH Trunk, on page 96

Verify Services on Cisco Unified Communications Manager

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

Procedure

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

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

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

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

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

Configure Phone Presence from Off-Cluster Cisco Unified Communications Manager

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

Procedure

	Command or Action	Purpose
Step 1	Add Cisco Unified Communications Manager as TLS Peer, on page 98	Add Cisco Unified Communications Manager as a TLS peer of the IM and Presence Service.

	Command or Action	Purpose
Step 2	Configure a TLS Context for Unified Communications Manager, on page 98	Add the Cisco Unified Communications Manager TLS poeer

Add Cisco Unified Communications Manager as TLS Peer

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

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration** > **System** > **Security** > **TLS Peer Subjects**, click **Add New**.

Step 2 Enter the IP Address of the external Cisco Unified Communications Manager in the **Peer Subject Name** field.

Step 3 Enter the name of the node in the **Description** field.

Step 4 Click **Save**.

What to do next

Configure TLS Context, on page 154

Configure a TLS Context for Unified Communications Manager

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

Before you begin

Add Cisco Unified Communications Manager as TLS Peer, on page 98

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration** > **System** > **Security** > **TLS Context Configuration**, click **Find**.

Step 2 Click **Default_Cisco_UP_SIP_Proxy_Peer_Auth_TLS_Context**.

Step 3 From the list of available TLS peer subjects, choose the TLS peer subject that you configured for Cisco Unified Communications Manager.

Step 4 Move this TLS peer subject to Selected TLS Peer Subjects.

Step 5 Click **Save**.

Step 6 Restart the Cisco OAMAgent on all cluster nodes:

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

b) From the **Server** drop-down list box, choose the IM and Presence server and click **Go**

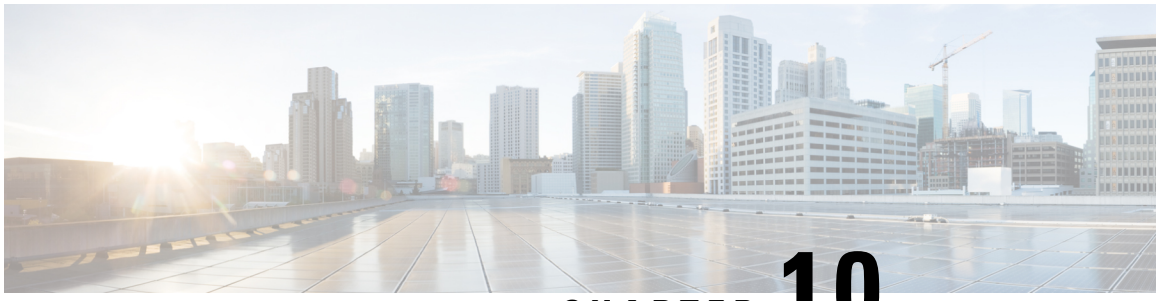
c) Under **IM and Presence Services**, select **Cisco OAMAgent** and click **Restart**.
d) Restart the service on all cluster nodes.

Step 7 After the OAM Agent restarts, restart the Cisco Presence Engine.

a) Choose **Tools** > **Control Center - Feature Services**.
b) From the **Server** drop-down list box, choose the IM and Presence node and click **Go**.
c) Under **IM and Presence Services**, select **Cisco Presence Engine** and click **Restart**.
d) Restart the service on all cluster nodes.

What to do next

Verify Services on Cisco Unified Communications Manager, on page 97



CHAPTER 10

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.

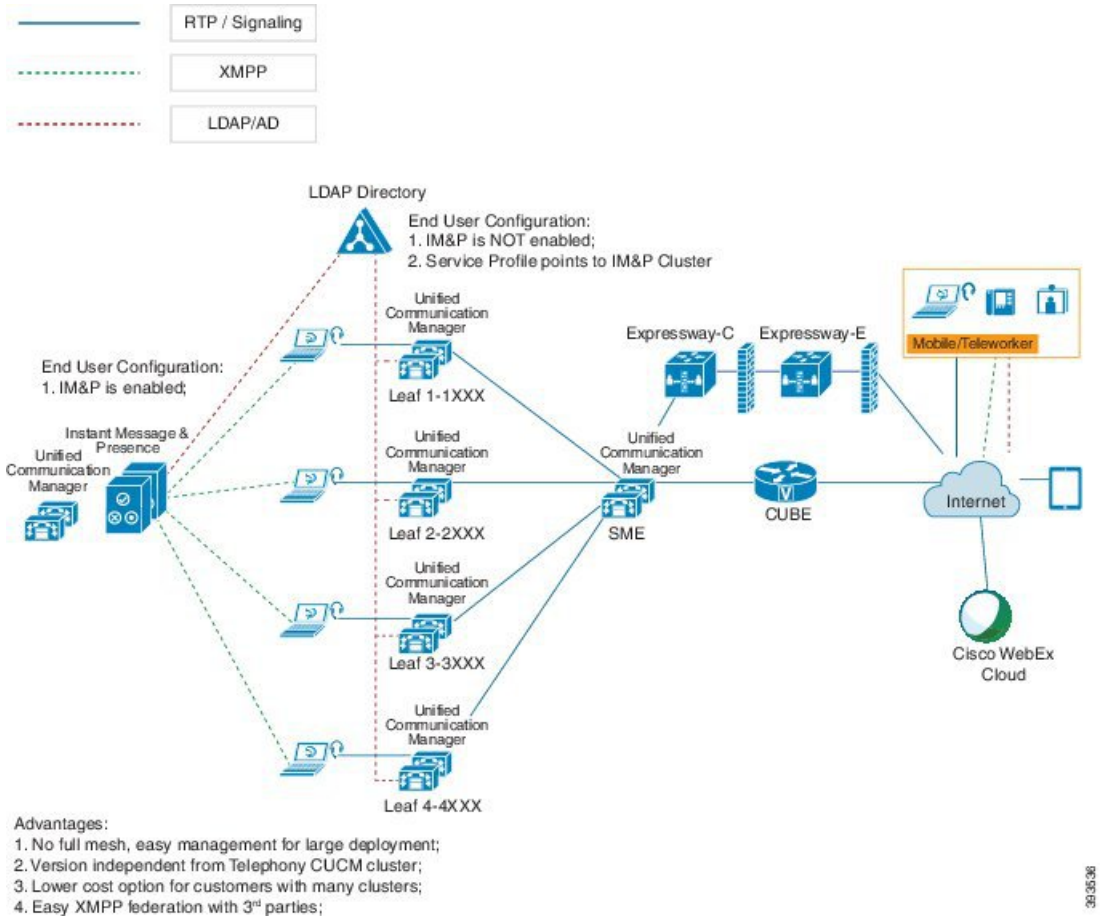
Setup Phase	Differences with Standard Deployments
Configuration Phase	Compared to standard (decentralized) deployments, the following extra configurations are required to set up the IM and Presence Service Central Deployment: • Users must be synced into both the telephony cluster and the IM and Presence 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 4: IM and Presence Service Centralized Cluster Architecture

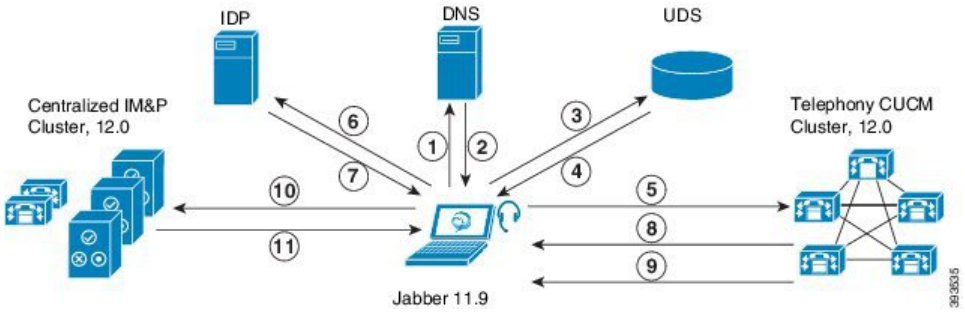


Centralized Cluster Use Case

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 5: 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 10: 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 108		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 109		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 110		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 110		Add your remote telephony clusters to the IM and Presence central cluster.
Step 5		Configure an IM and Presence UC Service, on page 111	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 112	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 112	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 114	Configuring OAuth in the telephony cluster will enable the feature for the central cluster.
Step 9		Configure an ILS Network, on page 114	If more than one telephony cluster exists, you must configure ILS.

	IM and Presence Central Cluster	Remote Telephony Clusters	Purpose
Step 10		Mobile and Remote Access Configuration	Configuration of Mobile and Remote Access in case of centralized deployment.

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.
- You must restart the Cisco XCP Authentication Service when you make a new entry to the centralized deployment in the IM and Presence administrator console.

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 110.

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 109

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 108

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 110

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 111

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 112.

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 112

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 Mobile and Remote Access 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 114

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**.

Note When OAuth keys are regenerated, you must restart the Cisco XCP Authentication Service on all IM and Presence nodes for Jabber OAuth login to work.

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 115	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 115	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 117	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 115

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 115

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 117

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.

Mobile and Remote Access 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 Mobile and Remote Access on all telephony leaf clusters in Expressway-C. Choose **Configuration → Unified Communications → Unified CM Servers**.

To configure Mobile and Remote Access 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 11: 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 12: 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 Mobile and Remote Access Configuration , Please refer :** https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

Upgrades with IM and Presence Central Deployments Require a Resync

If you have an IM and Presence Centralized Deployment and you upgrade the IM and Presence central cluster, or any remote telephony peer clusters, you must resynchronize your clusters after the upgrade is completed. You can resync your clusters from the **Centralized Deployment** window of Cisco Unified CM IM and Presence Administration by selecting your cluster peers and clicking the **Save and Synchronize** button.

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**).

Integrate Phone Presence in Centralized Deployment

In the centralized deployment, you can get the phone presence information from a remote Unified CM cluster by configuring multiple SIP Trunks in the centralized IM and Presence node.

Unlike in the standard deployment where you can configure only one Unified CM cluster as the presence gateway, the system derestricts this limitation in the centralized deployment. It allows the administrators to add multiple CUCM clusters as presence gateways in the IM and Presence node. This helps get the phone presence information from the remote Unified CM clusters.

The following procedure provides steps to configure SIP trunks and other additional settings in the remote Cisco Unified CM clusters and the corresponding IM and Presence node.

Procedure

Step 1 From the **Cisco Unified CM Administration** user interface, do the following:

a) Choose **Device** > **Trunk**. Add a new SIP Trunk and point it to the IM and Presence publisher node as a leaf cluster.
b) Choose **System** > **Service Parameter Configuration**, choose **Call Manager**. In the **IM and Presence Publish Trunk** field, enter the IP address of the leaf cluster trunk that you added in the previous step.
c) Enable presence for all users available in the cluster. You can set the **Enable user for Unified CM IM and Presence (Configure IM and Presence in the associated UC service profile)** checkbox for all users in the **End User Configuration** page in one attempt using a BAT file in the backend.

Step 2 From **Cisco Unified CM IM and Presence Administration**, do the following:

a) In the **Cisco Unified CM IM and Presence Administration** user interface, choose **Presence** > **Presence Gateway** and select the IP address of the remote CUCM cluster from the drop-down list.

Note Ensure that you delete the remote Unified CM cluster from the **Presence Gateway Configuration** window, before deleting it form the **Centralized Deployment Page**.

To update the Remote CUCM cluster address in the **Centralized Deployment Page**, you need to:

- Delete the remote Unified CM cluster from the **Presence Gateway Configuration** window.
- Edit the CUCM address on the **Centralized Deployment Page.**

  .
- Re-add the Unified CM cluster in the **Presence Gateway Configuration** window.

b) Choose **System** > **Security** > **Incoming ACL** and create a new ACL by adding the IP address of the remote Cisco Unified CM.

Important This note is applicable for release 14SU1 onwards.

Note Create a new Incoming ACL by adding the IP address of all the remote Cisco Unified CM publisher and subscriber nodes from where IM and Presence is expecting publish SIP messages.

c) Choose **System** > **Security** > **TLS Peer Subject** and add the IP address of the remote Cisco Unified CM.

Important This note is applicable for release 14SU1 onwards.

Note Create a TLS Peer Subject and add the IP address of all the remote Cisco Unified CM publisher and subscriber nodes from where IM and Presence is expecting publish SIP messages.

d) Choose **System** > **Security** > **TLS Context Configuration**. In the **TLS Peer Subject Mapping** section, select the TLS Peer Subject created for the remote Cisco Unified CM in the previous step from the **Available TLS Peer Subject** box and move it to the **Selected TLS Peer Subject** box.

Step 3 Restart the **Cisco OAMAgent** on all cluster nodes.

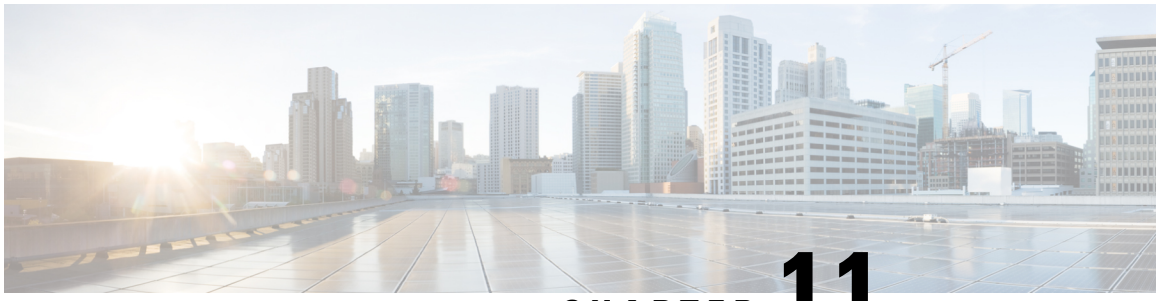
Step 4 Restart the **Cisco Presence Engine**.

Note In the IM and Presence Service centralized deployment, you can change the Cisco Jabber status to **Do Not Disturb (DND)**. The same status is reflected on the controlled Cisco IP Phone and Jabber device. However, the DND status change doesn't reflect in case of shared line, where more than one device is configured with the same directory number (DN) in a 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.

Feature	Interaction
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.



CHAPTER 11

Configure Advanced Routing

Advanced Routing Overview

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

- Intracluster connections between IM and Presence Service nodes within a cluster.
- Intercluster connections between IM and Presence Service clusters that share the same presence domain.
- SIP static routes for federation connections between different presence domains. Static routes are a fixed path and take precedence over dynamic routes.

Intracluster and Intercluster Connections

There are two modes to establish intercluster and intracluster connections:

- Multicast DNS (MDNS)—MDNS routing uses DNS records to set up the connections between the nodes. You can use MDNS routing when all nodes in the cluster are in the same multicast domain.
- Router-to-router (the default option)—Router-to-router uses IP address and user information to dynamically configure connections between the nodes. Use router-to-router connections when the nodes in the cluster are not in the same multicast domain, or when they are in different subnets.

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

Advanced Routing Prerequisites

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

MDNS Routing Prerequisites

The following prerequisites exist:

- You must have multicast DNS configured in the IOS network. When multicast DNS is disabled in the network, MDNS packets cannot reach the other nodes in a cluster. In some networks, multicast is enabled by default or enabled in a certain area of the network. For example, it may be enabled in an area that contains the nodes that form the cluster. In these networks, you do not need to perform any additional configuration in your network to use MDNS routing. If multicast DNS is disabled in your network, you must perform a configuration change to your network equipment to use MDNS routing.
- Make sure that all nodes are in the same multicast domain.

Router-to-Router Prerequisites

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

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

Advanced Routing Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure the Routing Communication Method, on page 125	The Routing Communication type determines the routing method the IM and Presence Service uses to establish router connections between cluster nodes. For single node IM and Presence Service deployments, we recommend that you leave the routing communication type at the default setting..
Step 2	Restart the Cisco XCP Router, on page 126	If you edited the Routing Communication Type, you must restart the Cisco XCP Router.
Step 3	Configure Secure Router-to-Router Communications, on page 126.	Optional. If you have Router-to-Router communication configured, you can configure secure TLS connections between XMPP routers in the same cluster or different clusters. **Note** You should enable this option only if the IM and Presence Service runs over an unsecure network as this option may degrade performance

	Command or Action	Purpose
Step 4	Configure the Cluster ID, on page 127	If you use MDNS routing, confirm that the Cluster ID is shared by all nodes within the cluster and that the value is unique for each cluster. If required, you can use this procedure to update the Cluster ID.
Step 5	Configure Throttling Rate for Presence Updates, on page 127	Optional. Configure the rate of availability (presence) changes sent to the Cisco XCP Router in messages per second. This setting helps to prevent an overload when the IM and Presence Service throttles the rate of availability (presence) changes to meet the configured value.
Step 6	Configure Static Routes, on page 128	Complete these tasks if you want to configure static routes.

Configure the Routing Communication Method

The Routing Communication type determines the routing method the IM and Presence Service uses to establish router connections between cluster nodes. For single node IM and Presence Service deployments, we recommend that you leave the routing communication type at the default setting.

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

Before you begin

If you want to use MDNS routing, MDNS must be enabled throughout your IOS network.

Procedure

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

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

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

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

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

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

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

Step 6 Click **Save**.

What to do next

If you edited this setting, you must Restart the Cisco XCP Router, on page 126

Restart the Cisco XCP Router

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

Before you begin

Configure the Routing Communication Method, on page 125

Procedure

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

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

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

Step 4 Click **Restart**.

What to do next

If you have Router-to-Router routing configured, Configure Secure Router-to-Router Communications, on page 126.

If you have MDNS routing configured, Configure the Cluster ID, on page 127.

Configure Secure Router-to-Router Communications

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

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

Procedure

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

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

Step 3 Click **Save**.

What to do next

Configure Throttling Rate for Presence Updates, on page 127

Configure the Cluster ID

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

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

Procedure

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

Step 2 Choose **Presence** > **Settings** > **Standard Configuration**.

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

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

Step 4 Click **Save**.
If you edited the **Cluster ID**, the new setting replicates to all cluster nodes.

What to do next

Configure Throttling Rate for Presence Updates, on page 127

Configure Throttling Rate for Presence Updates

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

Procedure

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

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

Step 3 From the **Service** drop-down list box, choose **Cisco Presence Engine**.

Step 4 In the **Clusterwide Parameters (Parameters that apply to all servers)** section, edit the **Presence Change Throttle Rate** service parameter. The valid range is 10 – 100 with a default setting of 50.

Step 5 Click **Save**.

What to do next

If you want to configure a SIP static route for federation connections, Configure Static Routes, on page 128.

Configure Static Routes

Procedure

	Command or Action	Purpose
Step 1	Configure SIP Proxy Server Settings, on page 128	Configure your SIP Proxy Server settings. For WAN Deployments, Cisco recommends that you enable TCP method event routing on IM and Presence Service.
Step 2	Configure Route Embed Templates on IM and Presence Service, on page 128	If your static route includes an embedded wildcard, you must configure a route embed template.
Step 3	Configure Static Routes on IM and Presence Service, on page 130	Configure static route settings.

Configure SIP Proxy Server Settings

Procedure

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

Step 2 Choose **On** for the Method/Event Routing Status. For WAN deployments, Cisco recommends that you configure TCP method event routing on IM and Presence Service.

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

Step 4 Click **Save**.

Configure Route Embed Templates on IM and Presence Service

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

Procedure

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

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

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

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

Step 5 Click **Save**.

What to do next

Configure Static Routes on IM and Presence Service, on page 130

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 13: Static Routes Set with Embedded Wildcards - Template A

Destination Pattern	Next Hop Destination
74..7812345*	1.2.3.4:5060
74..7867890*	5.6.7.8.9:5060
74..7811993*	10.10.11.37:5060

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

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

Sample Route Embed Template B

Route embed template: `471….xx*`

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

Table 14: 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 Static Routes on IM and Presence Service

Use this procedure to set up your static routes. For help with the fields and their settings, refer to the online help.

Procedure

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

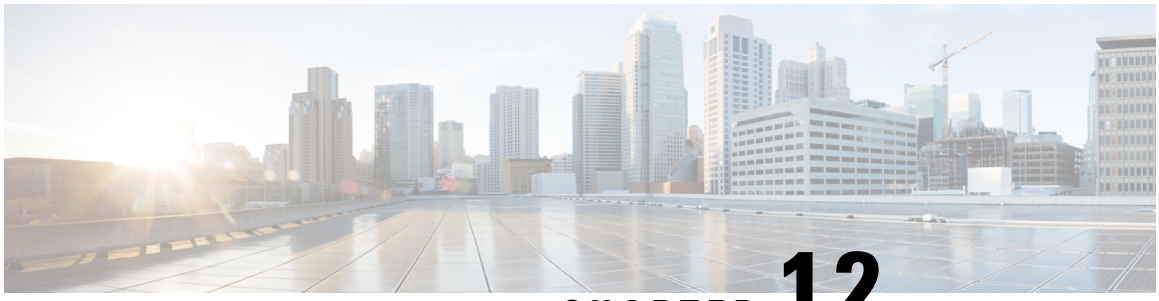
Static Route Parameters Settings

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

Table 15: Static Route Parameters Settings for IM and Presence Service

Field	Description
Destination Pattern	This field specifies the pattern of the incoming number, up to a maximum of 255 characters. The SIP proxy allows only 100 static routes to have an identical route pattern. If you exceed this limit, IM and Presence Service logs an error. Wildcard Usage You can use "." as a wildcard for a single character and "*" as a wildcard for multiple characters. IM and Presence Service supports embedded '.' wildcard characters in static routes. However, you must define route embed templates for static routes that contain embedded wildcards. Any static route that contains an embedded wildcard must match at least one route embed template. See the route embed template topic (referenced in the Related Topics section below) for information about defining route embed templates. For phones: • A dot can exist at the end of the pattern, or embedded in a pattern. If you embed the dot in a pattern, you must create a route embed template to match the pattern. • An asterisk can only exist at the end of the pattern. For IP addresses and host names: • You can use an asterisk as part of the a host name. • The dot acts as a literal value in a host name. An escaped asterisk sequence, *, matches a literal * and can exist anywhere.
Description	Specifies the description of a particular static route, up to a maximum of 255 characters.
Next Hop	Specifies the domain name or IP address of the destination (next hop) and can be either a Fully Qualified Domain Name (FQDN) or dotted IP address. IM and Presence Service supports DNS SRV-based call routing. To specify DNS SRV as the next hop for a static route, set this parameter to the DNS SRV name.
Next Hop Port	Specifies the port number of the destination (next hop). The default port is 5060. IM and Presence Service supports DNS SRV-based call routing. To specify DNS SRV as the next hop for a static route, set the next hop port parameter to 0.
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.

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



CHAPTER 12

Configure Certificates

Certificates Overview

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

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

- Self-signed Certificates—Self signed certificates are signed by the same server that issues the certificate. Within an enterprise, you may use self-signed certificates to connect with another internal system, provided none of those connections are travelling over an unsecure network. For example, the IM and Presence Service might generate self-signed certificates for an internal connection to Cisco Unified Communications Manager.
- CA-signed Certificates—These are certificates that are signed by a third-party Certificate Authority (CA). These can be signed by a public CA (such as Verisign, Entrust or Digicert) or a server (like Windows 2003, Linux, Unix, IOS) that controls the validity of the server/service certificate. CA-signed certificates are more secure than self-signed certificates and are typically used for any WAN connections. For example, a Federation connection with another enterprise or an intercluster peer configuration that uses WAN connections would require CA-signed certificates to build a trust relationship with the external system.

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

Multi-Server Certificates

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

Certificate Types in the IM and Presence Service

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

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

Table 16: 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	Presents the certificate to Expressway-C to get IM and Presence for SIP federated users. The IM and Presence proxy acts as both client and server. The Presence Engine uses these certificates for Exchange/Office 365 communication to get calendar presence. Presence Engine acts as a client only.

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.

Certificates Prerequisites

Configure the following items on Cisco Unified Communications Manager:

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

Certificate Exchange with Cisco Unified Communications Manager

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

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

Procedure

	Command or Action	Purpose
Step 1	Import Cisco Unified Communications Manager Certificate to IM and Presence Service, on page 136	Import a certificate from Cisco Unified Communications Manager into the IM and Presence Service.
Step 2	Download Certificate from IM and Presence Service, on page 137	Download a certificate from the IM and Presence Service. The certificate will need to be imported into Cisco Unified Communications Manager.
Step 3	Import IM and Presence Certificate to Cisco Unified Communications Manager, on page 137	To complete the certificate exchange, import the IM and Presence Service certificate into the Callmanager-trust store of Cisco Unified Communications Manager.

Import Cisco Unified Communications Manager Certificate to IM and Presence Service

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

Procedure

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

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

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

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

Step 5 Click **Submit**.

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

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

Step 6 Restart the Cisco SIP Proxy service:

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

b) From the **Server** drop-down list box, select an IM and Presence Service cluster node and click **Go**.

c) Choose **Cisco SIP Proxy** and click **Restart**.

What to do next

Download Certificate from IM and Presence Service, on page 137

Download Certificate from IM and Presence Service

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

Procedure

Step 1 From **Cisco Unified IM and Presence OS Administration**, choose **Security** > **Certificate Management** on IM and Presence Service.

Step 2 Click **Find**.

Step 3 Choose the `cup.pem` file.

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

Step 4 Click **Download** and save the file to your local computer.

Tip Ignore any errors that IM and Presence Service displays regarding access to the cup.csr file; The CA (Certificate Authority) does not need to sign the certificate that you exchange with Cisco Unified Communications Manager.

What to do next

Import IM and Presence Certificate to Cisco Unified Communications Manager, on page 137

Import IM and Presence Certificate to Cisco Unified Communications Manager

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

Before you begin

Download Certificate from IM and Presence Service, on page 137

Procedure

Step 1 Log into Cisco Unified OS Administration.

Step 2 Choose **Security** > **Certificate Management**

Step 3 Click **Upload Certificate**.

Step 4 From the Certificate Name menu, choose **Callmanager-trust**.

Step 5 **Browse** and select the certificate that you downloaded previously from the IM and Presence Service.

Step 6 Click **Upload File**.

Step 7 Restart the Cisco CallManager service:

a) From Cisco Unified Serviceability, choose **Tools** > **Control Center - Feature Services**.

b) From the **Server** drop-down list box, select a Cisco Unified Communications Manager node and click **Go**.

c) Select the **Cisco CallManager** service and click **Restart**.

Install Certificate Authority (CA) on IM and Presence Service

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

Procedure

	Command or Action	Purpose
Step 1	Upload CA Root Certificate Chain, on page 138	Use this procedure to upload the CA root certificate chain from the third-party Certificate Authority to the IM and Presence Service.
Step 2	Restart Cisco Intercluster Sync Agent Service, on page 139	After you have uploaded certificates, restart the Cisco Intercluster Sync Agent service.
Step 3	Verify CA Certificates Have Synchronized to Other Clusters, on page 139	Verify that your CA certificate chain has replicated to all peer clusters.

Upload CA Root Certificate Chain

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

- Root Certificate > Intermediate 1 Certificate > Intermediate 2 Certificate

Procedure

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

Step 2 Choose **Security** > **Certificate Management**.

Step 3 Click **Upload Certificate/Certificate chain**.

Step 4 From the **Certificate Name** drop-down list, choose one of the following:

- If you are uploading a CA-signed tomact certificate, choose **tomcat-trust**

- If you are uploading a CA-signed cup-xmpp certificate or a CA signed cup-xmpp-s2s, choose **cup-xmpp-trust**

Step 5 Enter a **Description** for the signed certificate.

Step 6 Click **Browse** to locate the file for the Root Certificate.

Step 7 Click **Click Upload File**.

Step 8 Upload each intermediate certificate in the same way using the **Upload Certificate/Certificate chain** window. For each intermediate certificate, you must enter the name of the preceding certificate in the chain.

What to do next

Restart Cisco Intercluster Sync Agent Service, on page 139

Restart Cisco Intercluster Sync Agent Service

After you upload the Root and Intermediate certificates to the IM and Presence database publisher node, you must restart the Cisco Intercluster Sync Agent service on that node. This restart ensures that the CA certificates are synced immediately to all other clusters.

Procedure

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

Step 2 From the **Server** drop-down list box, select the IM and Presence Service node on which you imported the certificate and click **Go**.

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

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

What to do next

Verify Intercluster Syncing, on page 142

Verify CA Certificates Have Synchronized to Other Clusters

After the Cisco Intercluster Sync Agent service has restarted, you must ensure that the CA certificate(s) have been correctly synchronized to other clusters. Complete the following procedure on each of the other IM and Presence database publisher nodes.

Note The information in the following procedure also applies to certificates ending in `-ECDSA`.

Procedure

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

Step 2 Under **Inter-clustering Troubleshooter**, find the test **Verify that each TLS-enabled inter-cluster peer has successfully exchanged security certificates** and verify that 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 Certificates to IM and Presence Service

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

Before you begin

To use CA-signed certificates that are signed by a third-party Certificate Authority (CA), you must already have installed that CA's root certificate chain on the IM and Presence Service. For details, Install Certificate Authority (CA) on IM and Presence Service, on page 138.

Procedure

	Command or Action	Purpose
Step 1	Upload Certificates, on page 141	Upload signed certificates to the IM and Presence Service.
Step 2	Restart Cisco Tomcat Service, on page 142	(Tomcat certificates only). Restart the Cisco Tomcat Service.

	Command or Action	Purpose
Step 3	Verify Intercluster Syncing, on page 142	(Tomcat certificates only). After the Cisco Tomcat service has restarted for all affected nodes within the cluster, you must verify that intercluster syncing is operating correctly.
Step 4	Restart the Cisco XCP Router service on all nodes, on page 143	If you uploaded certificates to the cup-xmpp store, restart the Cisco XMP Router on all cluster nodes.
Step 5	Restart Cisco XCP XMPP Federation Connection Manager Service, on page 143	(XMPP Federation only). If you uploaded certificates to the cup-xmpp store for XMPP Federation, restart the Cisco XCPXMPP Federation Connection Manager Service.
Step 6	Enable Wildcards in XMPP Federation Security Certificates, on page 143	(XMPP Federation only). If you uploaded certificates to the cup-xmpp store for XMPP Federation over TLS, you must enable wildcards for XMPP security certificates. This is required for group chat.

Upload Certificates

Use this procedure to upload certificates to each IM and Presence Service node.

Note Cisco recommends that you sign all required tomcat certificates for a cluster and upload them at the same time. This process reduces the time to recover intercluster communications.

Note The information in the following procedure also applies to certificates ending in `-ECDSA`.

Before you begin

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

Procedure

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

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

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

Step 4 Enter a Description for the signed certificate.

Step 5 Click **Browse** to locate the file to upload.

Step 6 Click **Upload File**.

Step 7 Repeat for each IM and Presence Service node.

What to do next

Restart the Cisco Tomcat service.

Restart Cisco Tomcat Service

After you upload tomcat certificates to each IM and Presence Service node, you must restart the Cisco Tomcat service on each node.

Procedure

Step 1 Log into the admin CLI.

Step 2 Run the following command: `utils service restart Cisco Tomcat.`

Step 3 Repeat for each node.

What to do next

Verify that intercluster syncing is operating correctly.

Verify Intercluster Syncing

After the Cisco Tomcat service has restarted for all affected nodes within the cluster, you must verify that intercluster syncing is operating correctly. Complete the following procedure on each IM and Presence database publisher node in the other clusters.

Procedure

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

Step 2 Under **Inter-clustering Troubleshooter**, find the test **Verify that each TLS-enabled inter-cluster peer has successfully exchanged security certificates** test and verify that is has passed.

Step 3 If the test shows an error, note the intercluster peer IP address; it should reference the cluster on which you uploaded the CA certificate(s). Continue with the following steps to resolve the issue.

Step 4 Choose **Presence** > **Inter-Clustering** and click the link associated with the intercluster peer that was identified on the System Troubleshooter page.

Step 5 Click **Force Manual Sync**.

Step 6 Check the **Also resync peer's Tomcat certificates** checkbox and click **OK**.

Step 7 Allow 60 seconds for the Inter-cluster Peer Status panel to auto-refresh.

Step 8 Verify that the **Certificate Status** field shows "Connection is secure".

Step 9 If the **Certificate Status** field does not show "Connection is secure", restart the Cisco Intercluster Sync Agent service on the IM and Presence database publisher node and then repeat steps 5 to 8.

- To restart the service from the admin CLI run the following command: utils service restart Cisco Intercluster Sync Agent.
- Alternatively, you can restart this service from the Cisco Unified IM and Presence Serviceability GUI.

Step 10 Verify that the Certificate Status now shows "Connection is secure". This means that intercluster syncing is now re-established between this cluster and the cluster for which the certificates were uploaded.

Restart the Cisco XCP Router service on all nodes

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

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

Procedure

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.

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.

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".

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

Procedure

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

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

Step 3 Click **Save**.

What to do next

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

Generate a CSR

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

Procedure

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

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

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

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

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

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

Step 7 Download the CSR to a local computer:

a) Click **Download CSR**.

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

c) **Download CSR**

What to do next

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

Certificate Signing Request Key Usage Extensions

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

Table 17: Cisco Unified Communications Manager CSR Key Usage Extensions

	Multi server	Extended Key Usage			Key Usage				
		Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)	IP security end system (1.3.6.1.5.5.7.3.5)	Digital Signature	Key Encipherment	Data Encipherment	Key Cert Sign	Key Agreement
CallManager CallManager-ECDSA	Y	Y	Y		Y	N	Y		
CAPF (publisher only)	N	Y	N		Y	N		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	N	Y		
TVS	N	Y	Y		Y	Y	Y		

Table 18: IM and Presence Service CSR Key Usage Extensions

	Multi server	Extended Key Usage			Key Usage				
		Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)	IP security end system (1.3.6.1.5.5.7.3.5)	Digital Signature	Key Encipherment	Data Encipherment	Key Cert Sign	Key Agreement
cup cup-ECDSA	N	Y	Y	Y	Y	Y	Y		
cup-xmpp cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		

Note Ensure that 'Data Encipherment' bit is not changed or removed as part of the CA-signing certificate process.

Generate a Self-Signed Certificate

Use this procedure to generate a self-signed certificate.

Procedure

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

Delete Self Signed Trust Certificates from IM and Presence Service

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

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

Before you begin

Important If you added CA-signed certificates, make sure that you have waited 30 minutes for the Cisco Intercluster Sync Agent Service to perform its periodic clean-up task on a given IM and Presence Service node.

Procedure

Step 1 From Cisco Unified IM and Presence Operating System Administration, choose**Security** > **Certificate Management**.
Step 2 Click **Find**.

The **Certificate List** appears.

Note The certificate name is composed of two parts, the service name and the certificate type. For example tomcat-trust where tomcat is the service and trust is the certificate type.

The self-signed trust certificates that you can delete are:

- Tomcat and Tomcat-ECDSA — tomcat-trust
- Cup-xmpp and Cup-xmpp-ECDSA — cup-xmpp-trust
- Cup-xmpp-s2s and Cup-xmpp-s2s-ECDSA — cup-xmpp-trust
- Cup and Cup-ECDSA — cup-trust
- Ipsec — ipsec-trust

Step 3 Click the link for the self-signed trust certificate you wish to delete.

Important Be certain that you have configured a CA-signed certificate for the service associated with the service trust store.

A new window appears that displays the certificate details.

Step 4 Click **Delete**.

Note The **Delete** button appears only if you have the authority to delete that certificate.

Step 5 Repeat the above procedure for each IM and Presence Service node in the cluster and on any intercluster peers to ensure complete removal of unnecessary self-signed trust certificates across the deployment.

What to do next

If the service is Tomcat, you must check for the IM and Presence Service node's self signed tomcat-trust certificate on the Cisco Unified Communications Manager node. See, Delete Self-Signed Tomcat-Trust Certificates from Cisco Unified Communications Manager, on page 147.

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

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

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

Before you begin

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

Procedure

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

The **Certificate List** window appears.

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

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

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

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

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

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

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

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

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

Certificate Monitoring Task Flow

Complete these tasks to configure the system to monitor certificate status and expiration automatically.

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

Procedure

	Command or Action	Purpose
Step 1	Configure Certificate Monitor Notifications, on page 149	Configure automatic certificate monitoring. The system periodically checks certificate statuses and emails you when a certificate is approaching expiration.
Step 2	Configure Certificate Revocation via OCSP, on page 149	Configure the OCSP so that the system revokes expired certificates automatically.

Configure Certificate Monitor Notifications

Configure automated certificate monitoring for Unified Communications Manager or the IM and Presence Service. The system periodically checks the status of certificates and emails you when a certificate is approaching expiration.

Note The **Cisco Certificate Expiry Monitor** network service must be running. This service is enabled by default, but you can confirm the service is running in Cisco Unified Serviceability by choosing **Tools** > **Control Center - Network Services** and verifying that the **Cisco Certificate Expiry Monitor Service** status is **Running**.

Procedure

Step 1 Log in to Cisco Unified OS Administration (for Unified Communications Manager certificate monitoring) or Cisco Unified IM and Presence Administration (for IM and Presence Service certificate monitoring).

Step 2 Choose **Security** > **Certificate Monitor**.

Step 3 In the **Notification Start Time** field, enter a numeric value. This value represents the number of days before certificate expiration where the system starts to notify you of the upcoming expiration.

Step 4 In the **Notification Frequency** fields, enter the frequency of notifications.

Step 5 Optional. Check the **Enable E-mail notification** check box to have the system send email alerts of upcoming certificate expirations..

Step 6 Check the **Enable LSC Monitoring** check box to include LSC certificates in the certificate status checks.

Step 7 In the **E-mail IDs** field, enter the email addresses where you want the system to send notifications. You can enter multiple email addresses separated by a semicolon.

Step 8 Click **Save**.

Note The certificate monitor service runs once every 24 hours by default. When you restart the certificate monitor service, it starts the service and then calculates the next schedule to run only after 24 hours. The interval does not change even when the certificate is close to the expiry date of seven days. It runs every 1 hour when the certificate either has expired or is going to expire in one day.

What to do next

Configure the Online Certificate Status Protocol (OCSP) so that the system revokes expired certificates automatically. For details, seeConfigure Certificate Revocation via OCSP, on page 149

Configure Certificate Revocation via OCSP

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

Before you begin

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

Procedure

Step 1 Log in to Cisco Unified OS Administration (for Unified Communications Manager certificate revocation) or Cisco Unified IM and Presence Administration (for IM and Presence Service certificate revocation).

Step 2 Choose **Security** > **Certificate Revocation**.

Step 3 Check the **Enable OCSP** check box, and perform one of the following tasks:

- If you want to specify an OCSP responder for OCSP checks, select the **Use configured OCSP URI** button and enter the URI of the responder in the **OCSP Configured URI** field.
- If the certificate is configured with an OCSP responder URI, select the **Use OCSP URI from Certificate** button.

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

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

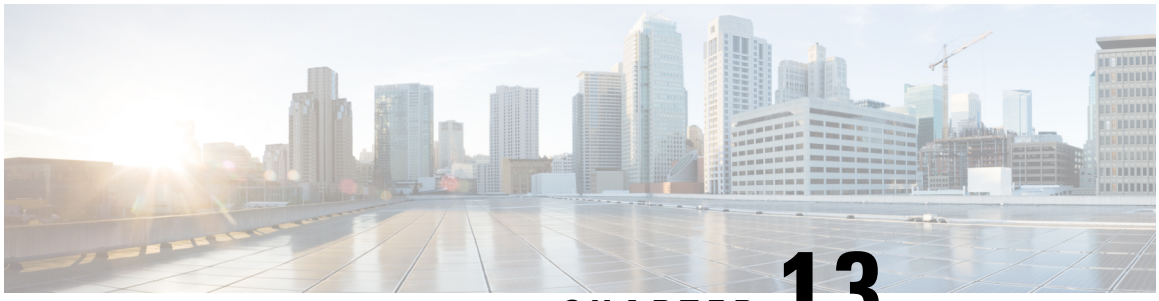
Step 6 Click **Save**.

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

a) From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.
b) Under **Certificate Revocation and Expiry**, set the **Certificate Validity Check** parameter to **True**.
c) Configure a value for the **Validity Check Frequency** parameter.

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

d) Click **Save**.



CHAPTER 13

Configure Security Settings

Security Overview

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

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

Security Settings Configuration Task Flow

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

Procedure

	Command or Action	Purpose
Step 1	Create Login Banner, on page 152	Create a login banner that users must acknowledge when they log in to any IM and Presence Service interface.
Step 2	Configure Secure XMPP Connections , on page 152	Complete these tasks to configure XMPP security.
Step 3	Configure TLS Peer Subject, on page 153	Configure these tasks if you want to set up TLS peers.
Step 4	Configure TLS Context, on page 154	Configure a TLS Context and TLS ciphers for your TLS peers.
Step 5	FIPS Mode, on page 154	If you want your deployment to be FIPS-compliant, you can enable FIPS mode.

	Command or Action	Purpose
		For added security, you can also enable Enhanced Security mode and Common Compliance mode.

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 filemust be uploaded to each IMand Presence Service node separately.

Configure Secure XMPP Connections

Use this procedure to enable secure XMPP connections using TLS.

Procedure

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

Step 2 Check the appropriate check box to enable the following XMPP security settings:

Table 19: XMPP Security Settings for the IM and Presence Service

Settings	Description
Enable XMPP Client To IM/P Service Secure Mode	When enabled, the IM and Presence Service establishes a secure TLS connection with XMPP client applications in a cluster. This setting is enabled by default. We recommend that you do not turn off this secure mode unless the XMPP client application can protect the client login credentials in nonsecure mode. If you do turn off the secure mode, verify that you can secure the XMPP client-to-node communication in some other way.
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.

Step 3 Click **Save**.

What to do next

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

SIP Security Settings Configuration on IM and Presence Service

Configure TLS Peer Subject

When you import an IM and Presence Service certificate, IM and Presence Service automatically attempts to add the TLS peer subject to the TLS peer subject list, and to the TLS context list. Verify the TLS peer subject and TLS context configuration is set up to your requirements.

Procedure

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

Step 2 Click **Add New**.

Step 3 Perform one of the following actions for the Peer Subject Name:

a) Enter the subject CN of the certificate that the node presents.

b) Open the certificate, look for the CN and paste it here.

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

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

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

Before you begin

Configure TLS Peer Subject, on page 153

Procedure

Step 1 In **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, select the TLS peer subject that you configured.

Step 5 Use the > arrow to move this TLS peer subject to **Selected TLS Peer Subjects**.

Step 6 Configure the **TLS Cipher Mapping** options:

a) Review the list of TLS ciphers that are available in the **Available TLS Ciphers** and **Selected TLS Ciphers** boxes.

b) If you want to enable a TLS cipher that isn't currently selected, use the > arrow to move the cipher to **Selected TLS Ciphers**.

Step 7 Click **Save**.

Step 8 Restart the Cisco SIP Proxy service:

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

b) From the **Server** drop-down list box, select an IM and Presence Service cluster node and click **Go**.

c) Select the **Cisco SIP Proxy** service and click **Restart**.

FIPS Mode

The IM and Presence Service contains a set of enhanced system security modes that allows your system to operate in a stricter set of security guidelines and risk management controls around items such as cryptography, data and signaling encryption, and audit logging.

- FIPS Mode—The IM and Presence Service can be configured to operate in FIPS mode, which allows your system to comply with FIPS or Federal Information Processing Standards, a US and Canadian government standard for cryptographic modules.
- Enhanced Security Mode—Enhanced Security Mode runs on a FIPS-enabled system and provides additional risk management controls such as data encryption requirements, a stricter credential policy, user authentication for contact searches, and stricter audit logging requirements.
- Common Criteria Mode—Common Criteria mode also runs on a FIPS-enabled system providing additional controls that allows your system to comply with Common Criteria guidelines such as TLS and the use of X.509 v3 certificates.

Note If the external database is MSSQL, for the services like Message Archiver, Text Conference Manager, and File Transfer Manager to work in the Common Criteria mode, you must perform the following:

1. Configure the server hosting the MSSQL database to support TLS 1.1 or higher.
2. Re-upload the database certificate to the IM and Presence service.
3. Check the **Enable SSL** checkbox in the **External Database Configuration** page. Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **External Server Setup** > **External Databases** to configure the external database.

Important This note is applicable for Release 12.5(1)SU7 only.

If you have multiserver SAN certificate configuration on the cluster, and move the cluster to FIPS and Common Criteria mode. It will convert multiserver SAN certificates to self-signed certificates.

If the old multiserver SAN certificate remains on Unified Communications Manager servers in the FIPS and Common Criteria mode, it needs to be deleted manually.

For details on how to enable FIPS Mode, Enhanced Security Mode, and Common Criteria Mode in Cisco Unified Communications Manager and the IM and Presence Service, refer to the "FIPS Mode Setup" chapter of the *Security Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

FIPS for Outlook Calendar Integration

When FIPS mode is enabled on IM and Cisco Presence Service server, only NTLMv2 is supported to get the Exchange Web Services information. If FIPS mode is disabled, then both NTLMv1 and NTLMv2 are supported as per the existing behavior. Basic Authentication is supported in both the cases regardless of enabling or disabling FIPS mode.

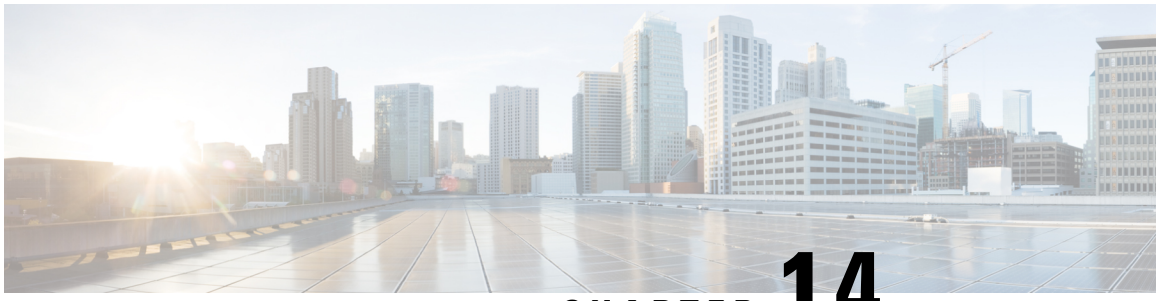
A new service parameter for Presence Engine service named **FIPS Mode Exchange Server Authentication** is introduced to validate the type of authentication used by the Presence Engine to establish a connection with Exchange Server through the Microsoft Outlook Calendar Integration feature.

You can set the **FIPS Mode Exchange Server Authentication** service parameter to either **Auto** or **Basic Only**.

Service parameter set to **Auto**: The Presence Engine negotiates NTLMv2 first and falls back to "Basic Authentication" only if NTLMv2 negotiation fails. NTLMv1 will not be negotiated in FIPS Mode.

Service parameter set to **Basic Only**: The Presence Engine is forced to use "Basic Authentication" even though the Exchange Server is configured to allow both NTLM and Basic Authentication.

Note Any changes in the service parameter setting requires restart of the Cisco Presence Engine.



CHAPTER 14

Configure Intercluster Peers

Intercluster Peers Overview

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

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

For sizing and performance recommendations for intercluster deployments, see the chapter "Collaboration Instant Messaging and Presence" in the *Cisco Collaboration System Solution Reference Network Designs (SRND)* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/design/guides/UCgoList.html#48016

Intercluster Peers Prerequisites

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

- Configure the system topology and assign your users as required for all clusters.
- For the intercluster peer connection to work properly, the following ports must be left open if there is a firewall between the two clusters:
  - 8443 (AXL)
  - 7400 (XMPP)
  - 5060 (SIP) Only if SIP federation is being used
- 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.

Note Intercluster peering is not supported when the IM and Presence Service is deployed on a Cisco Business Edition 6000 server.

Intercluster Peers Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Check User Provisioning, on page 158	Verify that end users are correctly provisioned before you configure intercluster peers.
Step 2	Enable the Cisco AXL Web Service, on page 159	The Cisco AXL Web Service must be active on all local and remote IM and Presence nodes. Use this procedure to verify the service is running.
Step 3	Enable the Sync Agent, on page 159	Enable the Sync Agent on the database publisher node of each intercluster peer.
Step 4	Configure Intercluster Peers, on page 160	Complete this task on the database publisher node in each cluster to set up intercluster peers.
Step 5	Verify the Intercluster Sync Agent is On, on page 162	The Intercluster Sync Agent must be running on all nodes in the IM and Presence Service cluster. Use this procedure to verify that the Intercluster Sync Agent parameter is running.
Step 6	Verify Intercluster Peer Status, on page 162	Verify that the intercluster peer configuration works.
Step 7	Update Intercluster Sync Agent Tomcat Trust Certificates, on page 163	If the tomcat certificate status for an intercluster peer is out-of-sync, update the Tomcat trust certificate.
Step 8	Enable Auto Recovery for Intercluster Peer Periodic Syncing Failure, on page 163	Use this procedure to enable auto recovery for intercluster periodic syncing failure.
Step 9	Configure Intercluster Peer Sync Interval, on page 164	Use this procedure to set the time interval for intercluster peer syncing.
Step 10	Disable Certificate Sync for Intercluster Peer Periodic Sync, on page 165	Use this procedure to configure disable/enable of certificates sync as part of Intercluster periodic sync.

Check User Provisioning

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

Procedure

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Diagnostics** > **System Troubleshooter**. The System Troubleshooter runs.

Step 2 In the **User Troubleshooter** section, verify that end users are correctly provisioned and that there are no duplicate or invalid users.

What to do next

Enable the Cisco AXL Web Service, on page 159

Enable the Cisco AXL Web Service

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

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

Procedure

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

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

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

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

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

What to do next

Enable the Sync Agent, on page 159

Enable the Sync Agent

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

Procedure

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

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

Step 3 Under **IM and Presence Services**, verify that the **Cisco Sync Agent** status is **Running**.

Step 4 If the service is not running, select the service and click **Restart**.

Step 5 Repeat this procedure in each cluster

What to do next

After the Cisco Sync Agent completes the user sync from Cisco Unified Communications Manager,Configure Intercluster Peers, on page 160

Configure Intercluster Peers

Use this procedure on the database publisher node for both the local and remote cluster to set up an intercluster peer relationship.

Before you begin

- Confirm that the Sync Agent has completed the user synchronization from Cisco Unified Communications Manager on the local and remote cluster. If you configure the intercluster peer connection before the Sync Agent completes the user sync, the status of the intercluster peer connection displays as **Failed**.
- Make sure that you have the AXL username and password for the intercluster application user on the remote IM and Presence Service node.

Procedure

Step 1 In Cisco Unified CM IM and Presence Administration, choose **Presence** > **Inter-Clustering**.

Step 2 Click **Add New**.

Step 3 In the **Peer Address** field, enter the node name of the remote cluster's database publisher node. This field may be an IP address, hostname or FQDN, but must match the actual node name that defines the server.

Note

- To verify the type of address the node name uses, log in to the Cisco Unified CM IM and Presence Administration on the remote cluster and choose **System** > **Presence Topology**. This window displays the node name and server details for each cluster node.
- Split-brain scenario may occur in a cluster that is part of multicluster environment. For example, there is a cluster A, and its multicluster peers are cluster B, C, D, and E. Nodes in cluster A must be able to reach DNS during split-brain scenario, because they have to communicate with other clusters B, C, D, and E in a multicluster environment during split-brain scenario.

  During split-brain scenario, If the nodes in cluster A cannot reach DNS then the IP addresses of A,B,C,D, and E cluster nodes should be set as node names, and NOT the hostnames and FQDNs.

  If the nodes in cluster A,B,C,D, and E are defined with FQDNs or hostnames, and they are not able to reach DNS during split-brain scenario, then service outages such as loss of IM Presence updates and loss of IM history occurs between clusters A and B,C,D,E.

Step 4 Enter the AXL credentials.

Step 5 Select the preferred **Protocol** for SIP communication.

Note Cisco recommends that you use **TCP** (the default setting) as the intercluster trunk transport for all IM and Presence Service clusters. You can change this setting if it suits your network configuration and security needs.

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 do the following. Otherwise, you can skip this step:

a) From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**.
b) From the **Server** drop-down list box, choose an IM and Presence node and click **Go**.
c) Select **Cisco XCP Router** and click **Restart**.
d) Repeat these steps on all cluster nodes

Step 8 Repeat this procedure on the database publisher node of each remote peer cluster.

Tip If you choose **TLS** as the intercluster transport protocol, the IM and Presence Service attempts to automatically exchange certificates between intercluster peers to establish a secure TLS connection. IM and Presence Service indicates whether the certificate exchange is successful in the intercluster peer status section.

What to do next

Verify the Intercluster Sync Agent is On, on page 162

Restart the XCP Router Service

Restart the Cisco XCP Router service on all nodes in the local cluster, as well as all nodes in the remote cluster.

Before you begin

Configure Intercluster Peers, on page 160

Procedure

Step 1 From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**.
Step 2 From the **Server** list, choose the node on which you want to reactivate services and click **Go**.
Step 3 In the **IM and Presence Services** area, select **Cisco XCP Router**.
Step 4 Click **Restart**.

What to do next

Verify the Intercluster Sync Agent is On, on page 162

Verify the Intercluster Sync Agent is On

The Intercluster Sync Agent network service synchronizes user information between intercluster peers. Use this procedure to confirm that the service is running on all cluster nodes in each intercluster peer.

Procedure

Step 1 From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**.
Step 2 From the **Server** menu, choose an IM and Presence Service node and click **Go**.
Step 3 Confirm that the **Cisco Intercluster Sync Agent** displays a status of **Running**.
Step 4 If the service is not running, select the service and click **Start**.
Step 5 Repeat this procedure for all cluster nodes on each intercluster peer.

What to do next

Verify Intercluster Peer Status, on page 162

Verify Intercluster Peer Status

Use this procedure to confirm that your intercluster peer configurations are working properly.

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **Presence** > **Inter-Clustering**.
Step 2 Choose the peer address from the search criteria menu.
Step 3 Click **Find**.
Step 4 In the Intercluster Peer Status window:

a) Verify that there are check marks beside each of the result entries for the intercluster peer.
b) Make sure that the **Associated Users** value equals the number of users on the remote cluster.
c) If you chose **TLS** as the intercluster transport protocol, the **Certificate Status** item displays the status of the TLS connection, and indicates if IM and Presence Service successfully exchanged security certificates between the clusters. If the certificate is out-of-sync, you need to manually update the tomcat-trust certificate (as described in this module). For any other certificate exchange errors, check the Online Help for a recommended action.

Step 5 Run the System Troubleshooter:

a) From Cisco Unified CM IM and Presence Administration, choose **Diagnostics** > **System Troubleshooter**.
b) In the **Inter-Clustering Troubleshooter** section, verify that there are check marks beside the status of each of the intercluster peer connection entries.

What to do next

Update Intercluster Sync Agent Tomcat Trust Certificates, on page 163

Update Intercluster Sync Agent Tomcat Trust Certificates

If a connection error appears occurs on the local cluster, and the corrupt Tomcat trust certificates are associated with the remote cluster, use this procedure to update the Tomcat trust certificate.

If the tomcat certificate status for an intercluster peer is out-of-sync, you must update the Tomcat trust certificate. In an intercluster deployment, this error can occur if you reuse an existing intercluster peer configuration to point to a new remote cluster. This error can also occur in a fresh IM and Presence Service installation, if you change the IM and Presence Service host or domain name, or if you regenerate the Tomcat certificate.

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **Presence** > **Inter-Clustering**.

Step 2 Click **Force Sync** to synchronize certificates with the remote cluster.

Step 3 In the confirmation window that displays, choose **Also resync peer's Tomcat certificates**.

Step 4 Click **OK**.

Note If there are any certificates that have not synced automatically, go to the Intercluster Peer Configuration window. All certificates marked with an X are the missing certificates which you need to copy manually.

Enable Auto Recovery for Intercluster Peer Periodic Syncing Failure

Use this procedure to Enable this service parameter, if you want Cisco Intercluster Sync Agent to raise an “InterClusterSyncAgentPeerPeriodicSyncingFailure” alarm and to restart automatically, when Intercluster peer periodic sync is stuck for more than 2 hours.

Procedure

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

Step 2 From the Server list, choose the IM and Presence node on which you want to set the "General Inter Cluster Sync Agent Parameters".

Step 3 From the **Service** list, choose **Cisco Intercluster Sync Agent (Active)**.

Step 4 Set the **Enable Auto Recovery for Inter-Cluster Peer Periodic Syncing Failure** service parameter to **Enabled**.

Step 5 Click **Save**.

Note If the "Enable Auto Recovery for Inter-cluster Peer Periodic Syncing Failure" service parameter is set to Enabled and if periodic sync is stuck for more than 2 hours then :

- ***InterClusterSyncAgentPeerPeriodicSyncingFailure*** Alarm will be generated.
- ***Cisco Intercluster Sync Agent*** service will be restarted automatically.

If "Enable Auto Recovery for Inter-cluster Peer Periodic Syncing Failure" is Disabled then :

- ***InterClusterSyncAgentPeerPeriodicSyncingFailure*** Alarm will be generated.
- ***Cisco Intercluster Sync Agent*** service will not be restarted automatically.

Configure Intercluster Peer Sync Interval

Use this procedure to set the time interval for intercluster peer syncing. The service parameter **Inter Cluster Peer Periodic Sync Interval (mins)** allows you to configure the time interval for dynamic ICSA periodic sync. The default setting for the intercluster peer sync interval is 30 minutes.

Procedure

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

Step 2 From the Server list, choose the IM and Presence node on which you want to set the "General Inter Cluster Sync Agent Parameters".

Step 3 From the **Service** list, choose **Cisco Intercluster Sync Agent (Active)**.

Step 4 Set the **Inter Cluster Peer Periodic Sync Interval (mins)** service parameter to the desired interval. The range is 30 – 1444 minutes with a default of 30 minutes.

Step 5 Click **Save**.

Note The new setting takes effect following the next intercluster sync.

If the intercluster peer sync fails, the Cisco Intercluster Sync Agent service restarts following the completion of four sync periods. For example, if the parameter is set to 40 minutes, the service restarts after 160 minutes (4*40).

Disable Certificate Sync for Intercluster Peer Periodic Sync

Use this procedure to disable certificates sync as part of the intercluster sync process. The service parameter **Certificate Sync during Inter-Cluster Periodic Sync** allows the administrator to disable or enable certificates sync as part of the intercluster periodic sync. The default value of this service parameter is **Perform certificate sync**.

Procedure

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

Step 2 From the Server list, choose the IM and Presence node on which you want to set the **General Inter Cluster Sync Agent Parameters**.

Step 3 From the **Service** list, choose **Cisco Intercluster Sync Agent (Active)**.

Step 4 Set the service parameter **Certificate Sync during Inter-Cluster Periodic Sync** to **Do not perform certificate sync**.

Step 5 Click **Save**.

Note If you encounter performance degradation or high CPU spikes in your deployment that is related to certificate sync during intercluster periodic sync, you can use this procedure to set the service parameter.

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.

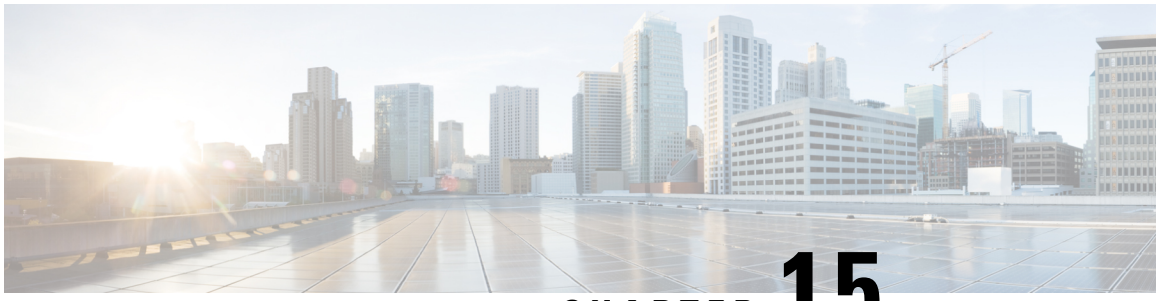
Step 4 Click **Delete**.

Step 5 Repeat these steps on the peer cluster.

Note The IM and Presence Service is enhanced to prevent restart of XCP router on each node within the IM and Presence cluster after deleting an intercluster peer. This enhancement helps the administrator manage large-scale clusters effectively by significantly reducing the overhead caused by sequential restart of nodes while ensuring uninterrupted Jabber service.

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.
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.
Intercluster Sync Agent resource shortage in multi cluster deployment	ICSA requires more resources in multi cluster deployment with large number of clusters. In case you face any issues with ICSA or SRM due to resource shortage. We recommend you to change the below mentioned Cisco SIP Proxy Service Parameters from default value of 20 to a new value of 10. • Maximum no. of processes • Maximum no. of spare processes • Maximum no. of processes Restart the SIP Proxy Service for the changes to take effect. Restart SRM and ICSA services.
Intercluster Sync Agent and DNS	Intercluster Sync Agent uses DNS to resolve all CUCM and IM&P servers listed in peer cluster's tomcat certificate (SAN entries). If the DNS resolution fails, Intercluster Sync Agent will not connect to the remote peer.



CHAPTER 15

Configure Push Notifications

Push Notifications Overview

When your cluster is enabled for Push Notifications, Unified Communications Manager 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 feature.

How Push Notifications Work

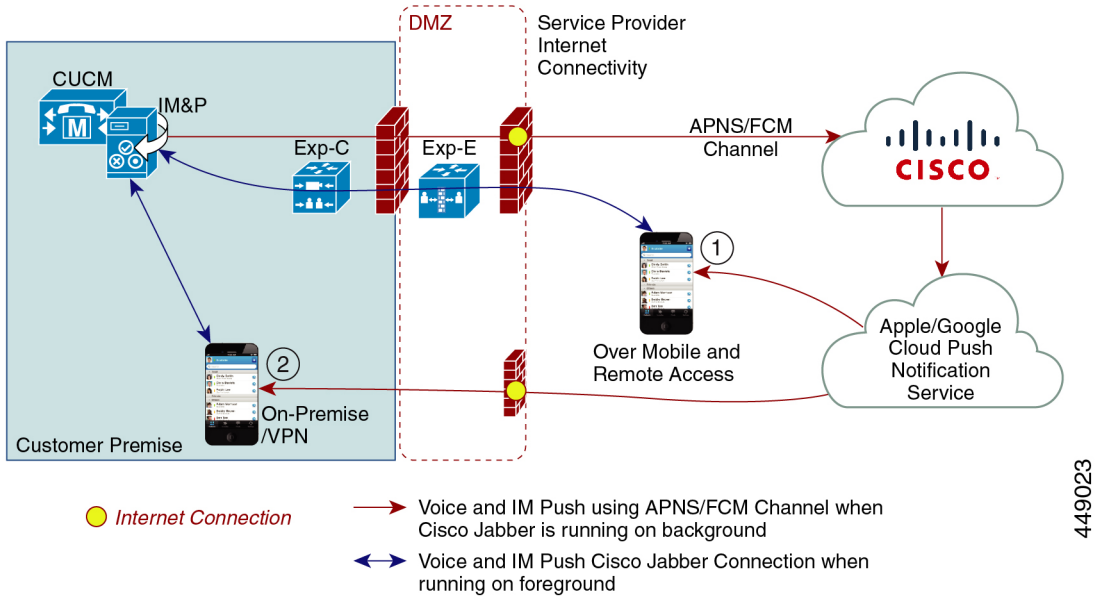
At startup, clients that are installed on Android and iOS platform devices register to Unified Communications Manager, the IM and Presence Service and to the Google and Apple cloud. With Mobile and Remote Access deployments, the clients registers to the on-premises servers through Expressway. So as long as the Cisco Jabber and Cisco Webex client remains in foreground mode,Unified Communications Manager 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 Unified Communications Manager 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 6: 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 Mobile and Remote Access 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 Unified Communications Manager 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** Unified Communications Manager sends voice and video calls to Cisco Jabber or Cisco Webex clients directly using the standard SIP communications channel. For calls, Unified Communications Manager 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

How Push Notifications Work in iOS13

In iOS13, Apple processes Push Notifications for suspended apps with type **VoIP** differently in comparison with iOS12. From July 2020, all new apps and app updates are built with iOS 13 SDK.

Cisco Unified Communications Manager and the IM and Presence Service use VOIP notification channel for Pushing both Voice and IM messages.

- For all audio video calls, the CUCM server sends a push notification of type "**VoIP**"
- For all messages, the IM&P server sends a push notification of type "**message**"

CUCM considers VoIP push Notifications as high priority notifications and delivers without delay.

The following diagrams display how Apple processes push notifications in **iOS12** and **iOS13**.

Image Here

Image Here

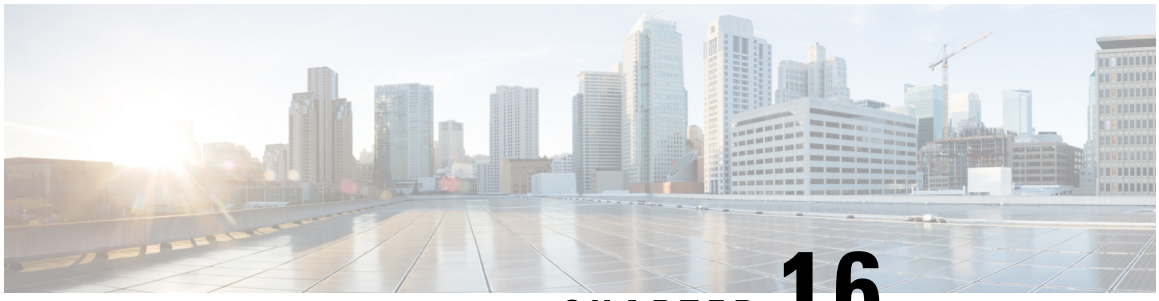
For a detailed description of what happens with each use case and between the versions, see the following table:

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 III

Configure Features



CHAPTER 16

Configure Availability and Instant Messaging

Availability and Instant Messaging Overview

IM and Presence Service allows your users to share their availability status with their contacts.

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

Instant messaging capabilities include:

Instant Message Forking

When a user sends an instant message to a contact who is signed into multiple instant message clients, IM and Presence Service delivers the instant message to each client. IM and Presence Service continues to fork instant messages to each client, until the contact replies. Once the contact replies, IM and Presence Service only delivers instant messages to the client on which the contact replied.

Offline Instant Messaging

When a user sends an instant message to a contact who is not signed in (offline), IM and Presence Service stores the instant message and delivers it after the offline contact signs back in to their instant message client.

Broadcast Instant Messaging

Allows a user to send an instant message to multiple contacts at the same time, for example, when a user wants to send a notification to a large group of contacts.

Please note that not all instant message clients support broadcasting.

Maximum Contact List Size

Configure the maximum contact list size for a user; this is the number of contacts the user can add to their contact list. This setting applies to the contact list on Cisco Jabber client applications and on third-party client applications.

Users who reach the maximum number of contacts are unable to add new contacts to their contact list, nor can other users add them as a contact. If a user is close to the maximum contact list size, and the user adds a group of contacts that pushes the contact list over the maximum number, IM and Presence Service does not add the surplus contacts. For example, if the maximum contact list size on IM and Presence Service is 200. A user has 195 contacts and attempts to add 6 new contacts to the list, IM and Presence Service adds five contacts and does not add the sixth contact.

Tip The System Troubleshooter in **Cisco Unified CM IM and Presence Administration** indicates if there are users who have reached the contact list limit.

Availability and Instant Messaging Prerequisites

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

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

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

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

Availability and Instant Messaging Task Flow

Perform the following tasks to configure availability and instant messaging on IM and Presence Service.

Procedure

	Command or Action	Purpose
Step 1	Configure Presence Sharing, on page 177	Use this procedure to configure the cluster-wide setting for Presence and IM availability sharing. Presence sharing allow your users to be able to view each other's IM availability status.
Step 2	Configure Ad-Hoc Presence Subscriptions, on page 178	Configure ad-hoc presence subscriptions. This setting allows users to temporarily view the presence status of other users whom are not on their contact list.

	Command or Action	Purpose
Step 3	Enable Instant Messaging, on page 179	Configure the system to allow users to exchange instant messages.

Configure Presence Sharing

Use this procedure to configure the cluster-wide setting for Presence and IM availability sharing. Presence sharing allow your users to be able to view each other's IM availability status.

Note When availability sharing is turned off:

- Users can view their own availability status in the client application, but the status for other users is greyed out.
- When users enter a chat room, their availability status displays as **Unknown**.

Procedure

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

Step 2 To enable cluster-wide Presence sharing, check the **Enable availability sharing** check box.

Note Individual Cisco Jabber users can enable or disable this setting for their own Jabber client, by reconfiguring the policy settings within their Cisco Jabber client.

Step 3 If you want users to be able to view the Presence of other users without requiring the other user's approval, check the **Allow user to view the availability of other users without being prompted for approval** check box. Otherwise, all Presence requests must be authorized by the other user.

Note Individual end users can override this setting by reconfiguring the policy settings within their Cisco Jabber client.

Step 4 Configure maximum values for the **Maximum Contact List Size** and **Maximum Watchers (per user)** settings. If you don't want to use maximums, check the **No Limit** check box for each.

Step 5 Optional. If you want Cisco Jabber users to be able to temporarily subscribe the Presence status of other users whom are not on their contact list, check the **Enable ad-hoc presence subscriptions** check box and configure the additional ad-hoc presence settings.

Step 6 Complete any additional settings in the **Presence Settings** window. Refer to the online help for help with the fields and their settings.

Step 7 Click **Save**.

Step 8 Restart the **Cisco XCP Router** and **Cisco Presence Engine** services:

a) Log in to Cisco Unified IM and Presence Serviceability and choose **Tools** > **Control Center - Feature Services**

b) Select the **Cisco Presence Engine** service and click **Restart**.

c) Choose **Tools** > **Control Center - Network Services**.

d) Select the **Cisco XCP Router** service and click **Restart**.

Note Depending on which fields you edited, you may not need to restart services. Refer to the online help for information on the fields that you edited.

What to do next

Enable Instant Messaging, on page 179

Configure Ad-Hoc Presence Subscriptions

Ad-hoc presence subscriptions allow users to temporarily view the presence status of other users whom are not on their contact list.

Before you begin

Configure Presence Sharing, on page 177

Procedure

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

Step 2 To turn on ad-hoc presence subscriptions for Cisco Jabber users, check the **Enable ad-hoc presence subscriptions** check box.

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 an ad-hoc presence subscription, the availability status that displays may not be current.

Step 5 Click **Save**.

Note You do not have to restart any services on IM and Presence Service for this setting. However, Cisco Jabber users must sign out, and sign back in to retrieve the latest ad-hoc presence subscriptions settings on IM and Presence Service.

What to do next

Enable Instant Messaging, on page 179

Enable Instant Messaging

Configure the system to allow users to exchange instant messages.

Before you begin

Configure Presence Sharing, on page 177

Procedure

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

Step 2 Check the **Enable instant messaging** check box.

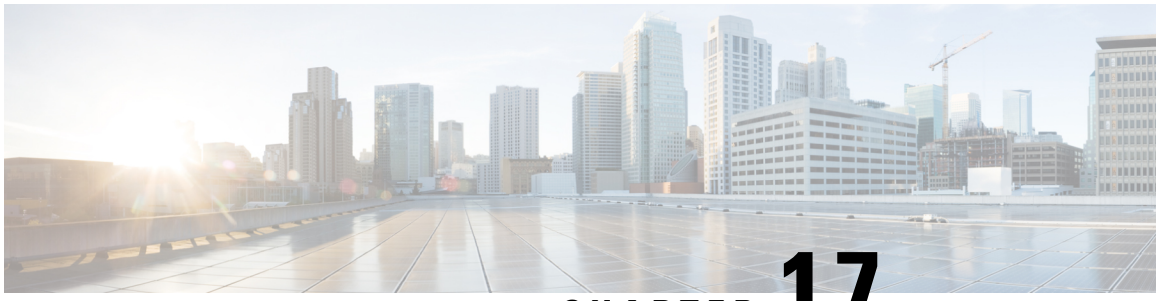
Step 3 Check the check box options that meet your deployment needs. For field descriptions, refer to the online help:

- **Suppress offline instant messaging**
- **Allow clients to log instant message history (on supported clients only)**
- **Allow cut & paste in instant messages**

Step 4 Click **Save**.

Availability and Instant Messaging Interactions and Restrictions

Feature	Restriction
Availability Sharing	If you turn off this setting, users can view only their own availability status. Availability information is not shared to other users in the cluster. In addition, availability information received from outside the cluster is not shared either.
Instant Messages	If Cisco XCP Router shuts down abruptly or if the user stops/restarts it, the instant messages that were sent at the beginning or during the outage period may not be delivered to the destination user. Warning messages may not be sent to the user who sent the messages. For more details, the administrator can check for error log lines containing "Dropping packet after jsm db shutdown" at the Cisco XCP Router trace files rtr-jsm-1.



CHAPTER 17

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

Persistent chat rooms are supported by both desktop and mobile Jabber clients, including both IOS and Android clients. For mobile clients, you must be running a minimum Jabber release of 12.1(0).

Group Chat Prerequisites

Ad Hoc Chat Prerequisites

If you are deploying ad hoc chat rooms, make sure that instant messaging is enabled. For details, see Enable Instant Messaging, on page 179.

Persistent Chat Prerequisites

If you are deploying persistent chat rooms:

- Make sure that instant messaging is enabled. For details, see Enable Instant Messaging, on page 179.
- 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 183	Add system administrators to manage the persistent chat system.
Step 2	Configure Chat Room Settings, on page 184	Configure basic chat room settings. Optionally, enable Persistent Chat.
Step 3	Restart the Cisco XCP Text Conference Manager, on page 185	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 185	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 186	In the IM and Presence Service, set up a connection to your external database.
Step 6	Windows Authentication for MSSQL Database for Persistent Chat, on page 186	While setting up a connection to MSSQL external database, you can enable Windows authentication.
Step 7	Migrate persistent chat rooms from one external database to another	In the IM and Presence Service, migrate all the persistent chat rooms and groups from your existing external database to another of the same database type or different types. For more information on how to perform the external database migration, see the "Migrate Persistent Chat Rooms from One External Database to Another" section of the Cisco IM and Presence Database Setup Guide 12.5(1)SU2 Release.

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 184

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 185

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 High Availability for Persistent Chat Task Flow, on page 198.

Otherwise, Set up External Database for Persistent Chat, on page 185.

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 186

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.

Windows Authentication for MSSQL Database for Persistent Chat

To enable Windows authentication for MSSQL external database for Persistent Chat.

Before you begin

Important Supported from Release 14SU2 onwards.

To configure external database connection, see Add External Database Connection, on page 186.

Procedure

	Command or Action	Purpose
Step 1	From the **Database Type** drop-down, select the type of external database as **Microsoft SQL Server**.	
Step 2	Check the **Enable Windows Authentication** check box.	

	Command or Action	Purpose
Step 3	In the **Domain** field, enter the Windows domain name.	
Step 4	Enter the **User Name** and **Password** information of the Windows user.	**Note** By using Windows authentication, Windows groups can be created at the domain level, and a login can be created on MSSQL server for the entire group.

Group Chat and Persistent Chat Interactions and Restrictions

Table 20: 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 only** 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. **Note** When you configure Ad hoc chat rooms as private on IM and Presence, persistent chat rooms also become private.

Persistent Chat Examples (without HA)

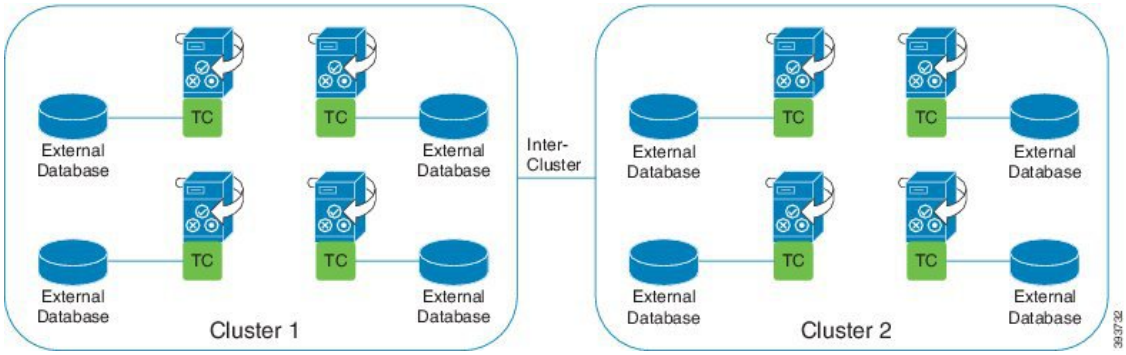
The following two examples illustrate the Persistent Chat feature along with intercluster peering where High Availability for Persistent Chat is not deployed.

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.

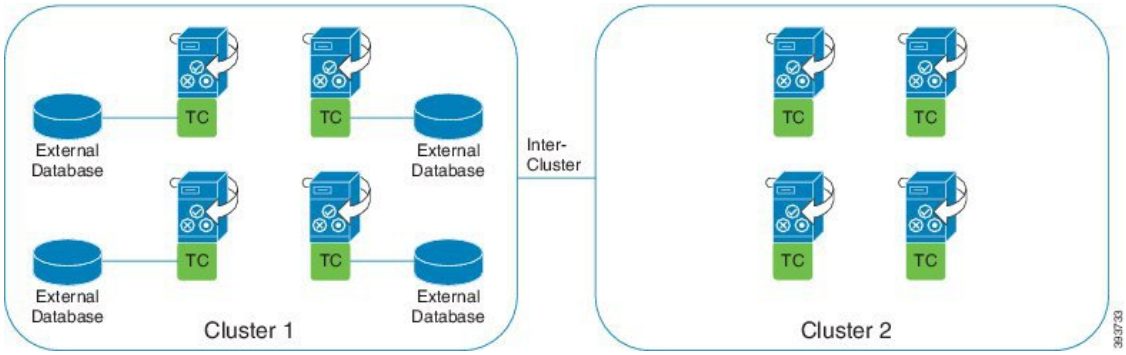
The Cisco Text Conferencing service is running on all nodes in either cluster, allowing all users in either cluster to join persistent chat rooms that are hosted on any node in either cluster.



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 21: 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 22: 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 23: 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

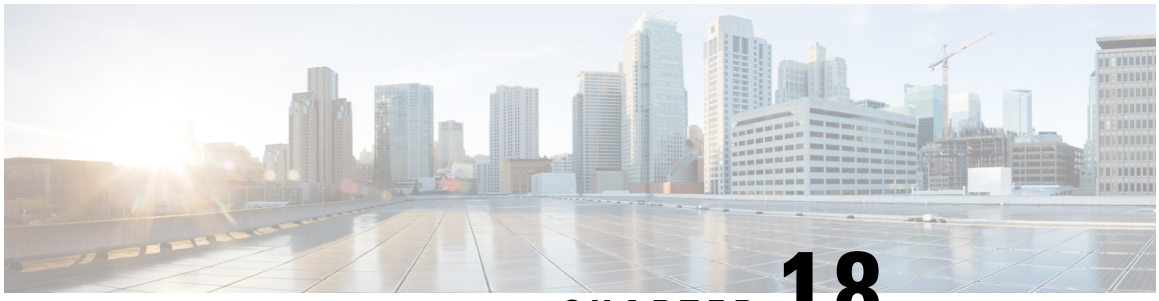
Current Number of Rooms Supported = 5000

Current Rooms Supported per Time Slice = 31%

New Rooms Supported per Time Slice = 50%

Result:

New Rooms Supported = 5000 * 31/50 =3100



CHAPTER 18

Configure High Availability for Persistent Chat

High Availability for Persistent Chat Overview

High Availability (HA) for Persistent Chat is an optional feature that you can deploy if you are using Persistent Chat rooms and you have system redundancy configured with Presence Redundancy Groups.

High Availability for Persistent Chat adds redundancy and failover capability to your persistent chat rooms. In the event of an IM and Presence Service node failure or Text Conferencing (TC) service failure, all persistent chat rooms hosted by that service are automatically hosted by the backup node or TC service. After failover, Cisco Jabber clients can seamlessly continue to use the persistent chat rooms.

External Database

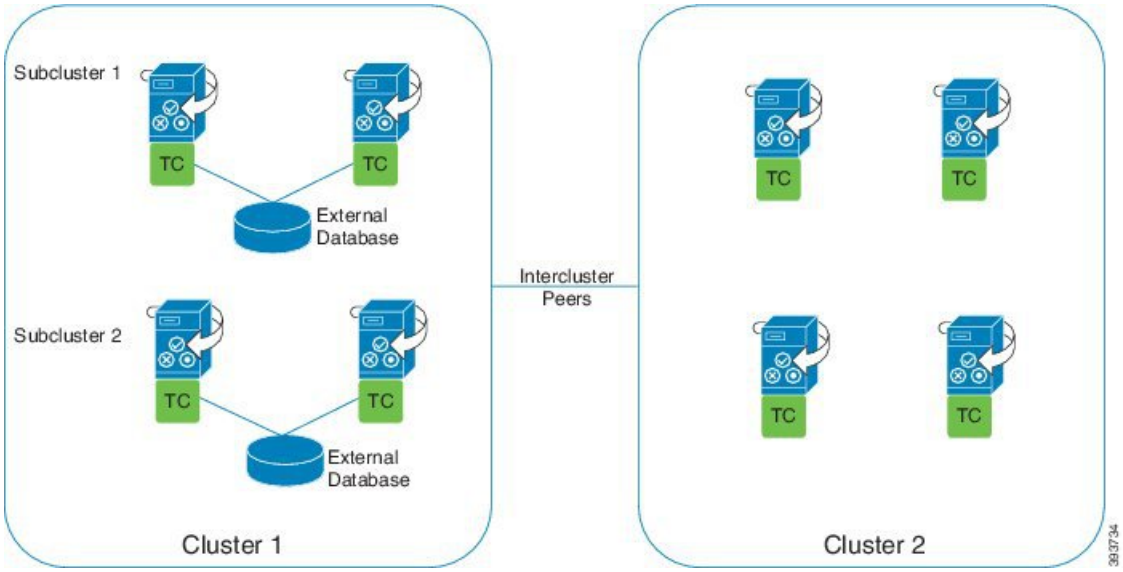
The main difference between the Persistent Chat (non-HA) and Persistent Chat HA setup is around the external database requirements:

- If Persistent Chat is deployed without HA, the external database connects to an individual chat node only. Each node that hosts persistent chat rooms requires a separate external database instance. If a chat node fails, persistent chat rooms that were hosted on that node become unavailable until the chat node comes back up.
- If High Availability for Persistent Chat is deployed, the external database instance connects to both nodes in a subcluster (Presence Redundancy Group). If a persistent chat node fails, the backup node in the subcluster takes over, allowing chat to continue uninterrupted.

High Availability for Persistent Chat - Intercluster Example

The following illustration displays an intercluster network where Persistent Chat High Availability is deployed in Cluster 1 only. With Persistent Chat High Availability, each subcluster hosts an external database. Cluster 2 does not have Persistent Chat High Availability enabled, so there is no external database requirement. However, because the Cisco Text Conference Manager service is running on all nodes, users in Cluster 2 can join persistent chat rooms that are hosted in Cluster 1.

Note In this example, only the chat rooms in Cluster 1 are configured to host persistent chat rooms. You can also add persistent chat support on the Cluster 2 nodes, along with external database instances. In this case, all users in either cluster would be able to join persistent chat rooms that are hosted on any node in either cluster.



Comparison of Persistent Chat (non-HA) and Persistent Chat HA Requirements

If you are deploying Persistent Chat Rooms, Cisco recommends that you deploy High Availability for Persistent Chat as well as this adds failover capability to your persistent chat rooms. However, it is not mandatory.

The following table discusses the differences between Persistent Chat deployed with and without High Availability.

Table 24: Comparison of Persistent Chat with and without High Availability

	Persistent Chat (without HA)	Persistent Chat HA
Database Requirements	You require a separate external database instance for each cluster node that hosts persistent chat rooms. These external database instances can be created on the same external database server. **Recommended:** For optimum performance and scalability, deploy a unique logical external database instance for each node or redundancy group an the IM and Presence cluster. However, this is not mandatory. **Minimum Requirement:** You must have at least one external database instance for Persistent Chat across an IM and Presence intercluster network. However, this deployment may be inadequate for high-use networks. **Supported Database Types** • PostgreSql (version 9.1 and above) • Oracle • Microsoft SQL Server	You require a separate external database instance for each subcluster (Presence Redundancy Group) that hosts persistent chat rooms. These external database instances can be created on the same external database server. **Recommended:** For optimum performance and scalability, deploy a separate external database instance for each subcluster within an IM and Presence cluster. However, this is not mandatory. **Minimum Requirement:** You require at least one external database instance for Persistent Chat HA across an IM and Presence intercluster network. However, this deployment may be inadequate for high-use networks. **Supported Database Types** • PostgreSql (version 9.1 and above) • Oracle • Microsoft SQL Server (as of 11.5(1)SU2)
Behavior when persistent chat node fails	• Persistent chat rooms hosted on the failed node are inaccessible until the node comes back up. • Users homed on the failed node fail over to the backup node in the subcluster, provided cluster redundancy is configured. However, they cannot access persistent chat rooms from the failed node.	• Persistent chat rooms failover to the backup node in the subcluster. Users can continue messaging with no interruption of services. • Any users homed on the failed node also fail over.

High Availability for Persistent Chat Prerequisites

Before you configure High Availability for Persistent Chat, make sure that:

- Persistent Chat rooms are enabled. For details, see Configure Chat Room Settings, on page 184.
- High availability is enabled in each Presence Redundancy Groups. For details, see Presence Redundancy Group Task Flow, on page 50.

- You have configured the external database. For database setup and support information, see the *Database Setup Guide for the IM and Presence Service.*

High Availability for Persistent Chat Task Flow

Procedure

	Command or Action	Purpose
Step 1	Set up External Database, on page 198	You require a separate external database instance for each subcluster where persistent chat rooms are hosted. These separate external database instances can be hosted on the same database server
Step 2	Add External Database Connection, on page 199	Configure a connection to the external database from the IM and Presence Service.
Step 3	Verify High Availability for Persistent Chat Settings, on page 199	Confirm your system settings for Persistent Chat High Availability.
Step 4	Start Cisco XCP Text Conference Manager Service, on page 200	If the Cisco XCP Text Conference Manager service was stopped on any nodes, use this precudure to start it.
Step 5	Merge External Databases, on page 200	Optional. If you are upgrading from an earlier release where you had Persistent Chat configured with multiple external databases, use this procedure to merge your external databases into a single database.

Set up External Database

To deploy High Availability for Persistent Chat, you require a separate external database instance for each subcluster where persistent chat rooms are hosted. These separate external database instances can be hosted on the same database server.

A subcluster is a redundant pair of IM and Presence nodes (Presence Redudancy Group). You can have a maximum of three subclusters in an IM and Presence cluster of 6 nodes. If HA for Persistent Chat is enabled in an IM and Presence cluster of 6 nodes, you will have three external database instances and three subcluster pairs.

You can use PostgreSQL, Oracle, or Microsoft SQL Server for the external database connection. For setup details, refer to the *Database Setup Guide for IM and Presence Service*.

What to do next

Add External Database Connection, on page 199

Add External Database Connection

Configure connections to the High Availability for Persistent Chat external database instances from the IM and Presence Service. Make sure that both nodes in the subcluster are assigned to the same unique logical external database instance.

Procedure

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Messaging** > **External Servers Setup** > **External Databases**.

Step 2 Click **Add New**.

Step 3 In the **Database Name** field, enter the name of external database instance.

Step 4 From the **Database Type** drop-down, select the type of external database that you are deploying.

Step 5 Enter the **User Name** and **Password information** for the database.

Step 6 In the **Hostname** field, enter the hostname or IP address of the database.

Step 7 Complete the remaining settings in the **External Database Settings** window. For help with the fields and their settings, refer to the online help.

Step 8 Click **Save**.

Step 9 Repeat this procedure to create connections to each external database instance.

What to do next

Verify High Availability for Persistent Chat Settings, on page 199

Verify High Availability for Persistent Chat Settings

Use this procedure to confirm that your system is set up for High Availability for Persistent Chat.

Note If you've already enabled High Availability for your Presence Redundancy Groups (subclusters) and your chat room configuration includes Persistent Chat then your High Availability for Persistent Chat may be completed.

Procedure

Step 1 Confirm that High Availability is enabled in each subcluster:

a) From Cisco Unified CM Administration, choose **System** > **Presence Redundancy Groups**.
b) Click **Find** and choose the Presence Redundancy Group that you want to check.
c) Verify that the **Enable High Availability** check box is checked. If the check box is unchecked, then check it.
d) Click **Save**.
e) Repeat these steps for each presence redundancy group in the cluster.

Step 2 Confirm that persistent chat is enabled:

a) From Cisco Unified CM Administration, choose **Messaging** > **Group Chat and Persistent Chat**.
b) Confirm that the **Enable Persistent Chat** check box is checked. If the check box is unchecked, then check it.
c) Click **Save**.

Step 3 From Cisco Unified CM Administration, confirm that the **Cisco XCP Text Conference Manager Service** is running on all cluster nodes.

a) Choose **System** > **Presence Topology**.
b) For each cluster node, click **view** to view the node details
c) Under **Node Status**, verify that the **Cisco XCP Text Conference Manager** service is **STARTED**.
d) In the left navigation bar, click **Presence Topology** to return to the cluster topology and and repeat the above steps until you've confirmed the status for all cluster nodes.

What to do next

If the **Cisco XCP Text Conference Manager Service** service needs to be enabled, Start Cisco XCP Text Conference Manager Service, on page 200.

Start Cisco XCP Text Conference Manager Service

Use this procedure to start the Cisco XCP Text Conference Manager service. This service must be running on all cluster nodes for users on those nodes to be able to join persistent chat rooms.

Procedure

Step 1 In **Cisco Unified IM and Presence Serviceability**, choose **Tools** > **Control Center - Feature Services**.
Step 2 From the **Server** drop-down list, choose the IM and Presence cluster node and click **Go**.
Step 3 Under **IM and Presence Services**, select **Cisco XCP Text Conference Manager** and click **Start**.
Step 4 Click **OK**.
Step 5 (Optional) Click **Refresh** if you want to verify that the service has fully restarted.

Merge External Databases

Use this procedure to merge external databases.

Note Microsoft SQL database is not supported for merging external databases.

Optional. If you have upgraded from a release prior to 11.5(1), and multiple external databases were used to manage redundancy, use the External Database Merge Tool to merge your external databases into a single database.

Example

If you have upgraded from a release prior to 11.5(1), and you had persistent chat configured with each persistent chat node connecting to a separate external database instance, use this procedure to merge the two databases in a subcluster into a single database that connects to both nodes.

Before you begin

- Ensure that the two source destination databases are assigned correctly to each IM and Presence Service node in the presence redundancy group. This verifies that both of their schemas are valid.
- Back up the tablespace of the destination database.
- Ensure that there is enough space in the destination database for the new merged databases.
- Ensure that the database users, created for the source and destination databases, have the permissions to run these commands:
  - `CREATE TABLE`
  - `CREATE PUBLIC DATABASE LINK`
- If your database users do not have these permissions, you can use these commands to grant them:
  - PostgreSQL:

    `CREATE EXTENTION`—This creates the dblink and requires super user or dbowner privileges. After this, you EXECUTE privilege for dblink by running following:

    ```
    GRANT EXECUTE ON FUNCTION DBLINK_CONNECT(text) to <user>

    GRANT EXECUTE ON FUNCTION DBLINK_CONNECT(text,text) to <user>
    ```

  - Oracle:

    ```
    GRANT CREATE TABLE TO <user_name>;

    GRANT CREATE PUBLIC DATABASE LINK TO <user_name>;
    ```

- If you are using a PostgreSQL external database, make sure that the following access is configured in the pg_hba.conf file:
  - The IM and Presence publisher node must have full access to each external database.
  - The external PostgreSQL database must have full access to each database instance. For example, if the external database is configured on 192.168.10.1 then each database instance must be configured in the pg_hba.conf file as `host dbName username 192.168.10.0/24 password`.

Procedure

Step 1 Sign in to **Cisco Unified CM IM and Presence Administration** on the IM and Presence Service publisher node.

Step 2 Stop the Cisco XCP Text Conference Service on the **System** > **Services** window for each IM and Presence Service node in the presence redundancy group.

Step 3 Click **Messaging** > **External Server Setup** > **External Database Jobs**.

Step 4 Click **Find** if you want to see the list of merge jobs. Choose **Add Merge Job** to add a new job.

Step 5 On the **Merging External Databases** window, enter the following details:

- Choose **Oracle** or **Postgres** from the **Database Type** drop-down list.
- Choose the IP address and hostname of the two source databases and the destination database that will contain the merged data.

If you chose Oracle as the **Database Type** enter the tablespace name and database name. If you chose Postgres as the **Database Type** you provide the database name.

Step 6 In the **Feature Tables** pane, the Text Conference(TC) check-box is checked by default. For the current release, the other options are not available.

Step 7 Click **Validate Selected Tables**.

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 **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.

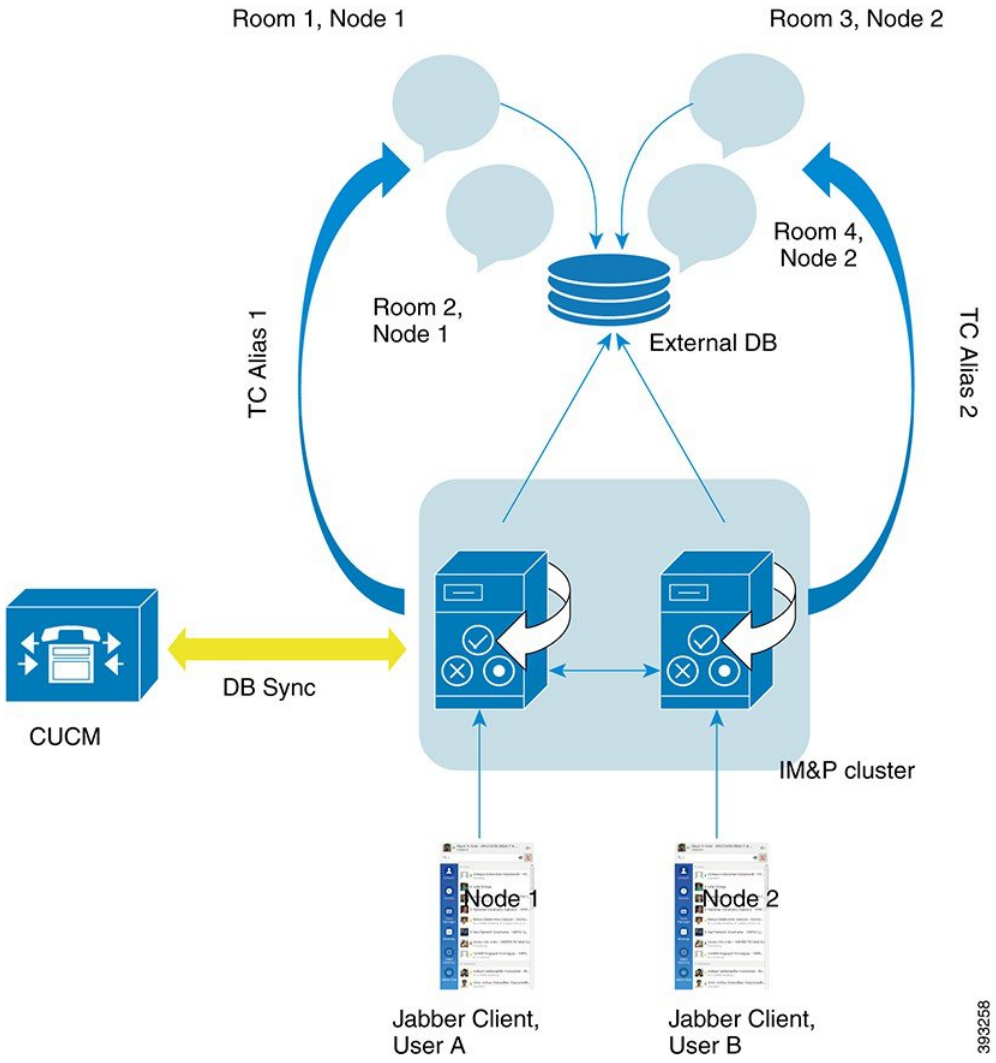
Step 12 You must reassign the newly merged external database (destination database) to the presence redundancy group

High Availability for Persistent Chat Use Cases

The following flows demonstrate the high availability for persistent chat flows for failover and failback. This example covers an IM and Presence cluster with two nodes. An IM and Presence cluster can have a maximum of 6 nodes, which allows for three subclusters. If persistent chat rooms are hosted on all nodes, you require three separate external database instances.

Note For this enhancement the Text Conferencing (TC) service has been made a critical service. As a result, the TC high availability failover flow remains the same even if the failover has been caused by the failure of another critical service on the node, such as the Cisco XCP Router service.

Figure 7: High Availability for Persistent Chat Structure



High Availability for Persistent Chat Failover Use Case

For this example, there are four users on four IM and Presence Service nodes with two High Availability (HA) pairs or subclusters. The users are assigned as follows:

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.

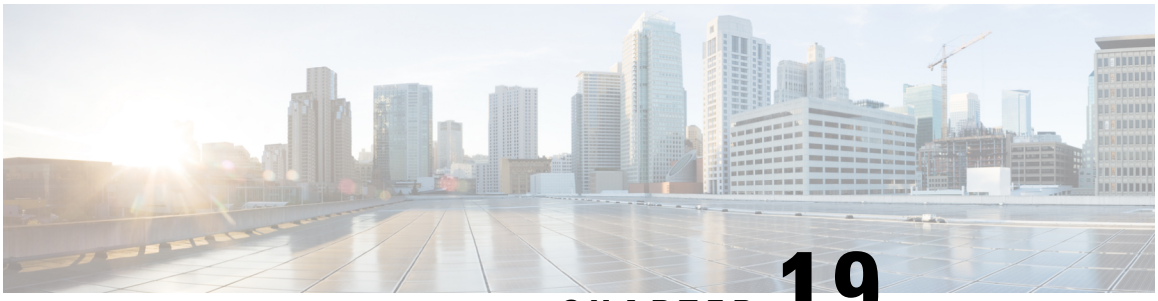
3. After 90 seconds, the Server Recovery Manager (SRM) determines the failure of the TC critical service and starts an automatic failover.
4. Node 1B takes over the users from 1A and transitions to the **Failed Over with Critical Services not Running** state, before transitioning to the HA state **Running 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 Persistent Chat Fallback Use Case

For this example there are four users on four IM and Presence Service nodes with two High Availability (HA) pairs or subclusters. The users are assigned as follows:

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.



CHAPTER 19

Configure Managed File Transfer

Managed File Transfer Overview

Managed File Transfer (MFT) allows an IM and Presence Service client, such as Cisco Jabber, to transfer files to other users, ad hoc group chat rooms, and persistent chat rooms. The files are stored in a repository on an external file server and the transaction is logged to an external database.

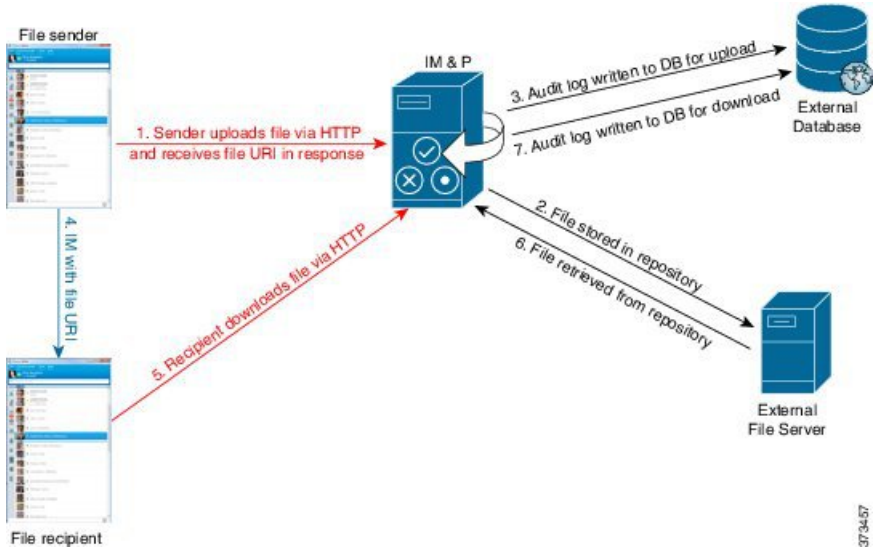
To deploy the Managed File Transfer feature, you must also deploy the following servers:

- **External database**—All file transfers get logged to the external database.
- **External File Server**—A copy of each transferred file gets saved to the repository on the external file server.

Note This configuration is specific to file transfers and has no impact on the message archiver feature for regulatory compliance.

For use cases, see Managed File Transfer Call Flow, on page 206

Managed File Transfer Call Flow



1. The sender uploads the file to the IM and Presence Service server via HTTP, and the server responds with a URI for the file.
2. The IM and Presence Service server sends the file to the file server repository for storage.
3. IM and Presence Service writes an entry to the external database log table to record the upload.
4. The sender sends an IM to the recipient. The IM includes the URI of the file.
5. The recipient sends an HTTP request to IM and Presence Service for the file. IM and Presence Service reads the file from the repository (6), records the download in the log table (7) and sends the file to the recipient.

The flow for transferring a file to a group chat or persistent chat room is similar, except the sender sends the IM to the chat room, and each chat room participant sends a separate request to download the file.

Note When a file upload occurs, the managed file transfer service is selected from all managed file transfer services available in the enterprise for the given domain. The file upload is logged to the external database and external file server associated with the node where this managed file transfer service is running. When a user downloads this file, the same managed file transfer service handles the request and logs it to the same external database and the same external file server, regardless of where this second user is homed.

Managed File Transfer Prerequisites

- You must also deploy an external database and external file server.
- Ensure that all clients can resolve the full FQDN of the IM and Presence Service node to which they are assigned. This is needed in order for Managed File Transfer to work.

External Database Prerequisites

Tip If you are also deploying persistent chat and/or message archiver, you can assign the same external database and file server for all features. Make sure when determining server capacity to consider the potential IM traffic, number of files transferred, and the file size.

Install and configure an external database. For details, including supported databases, see *Database Setup Guide for the IM and Presence Service*.

In addition follow these guidelines:

- You require one unique logical external database instance for each IM and Presence Service node in an IM and Presence Service cluster.
- The external database is supported on both virtualized and non-virtualized platforms.
- For a full list of the logged metadata, see the AFT_LOG Table in the "External Database Tools" chapter of the *Database Setup for IM and Presence Service on Cisco Unified Communications Manager*.
- If you are connecting to the external database using IPv6, check Configure IPv6 Task Flow, on page 34 for details on setting up IPv6.

External File Server Requirements

Follow these guidelines when setting up your external file server:

- Subject to file server capacity, each IM and Presence Service node requires its own unique Cisco XCP File Transfer Manager file server directory, however, nodes can share the same physical file server installation.
- The file server must support an ext4 file system, SSHv2, and SSH tools.
- The file server must support OpenSSH version between 4.9, 6.x, and 7.x.

Important This note is applicable for release 14SU3 onwards.

Note OpenSSH version 8.x is supported from release 14SU3 onwards.

- The network throughput between IM and Presence Service and the external file server must be greater than 60 megabytes per second.

  You can use the `show fileserver transferspeed` CLI command after you enable managed file transfer to determine your file server transfer speed. Be aware that if you run this command while the system is busy, it may impact the value returned by the command. For more information about this command, see the *Command Line Interface Guide for Cisco Unified Communications Solutions* at this link.

Partition Recommendations for External File Servers

Cisco recommends that you create one or more separate partitions that are dedicated to file transfer storage so that other applications that run on the server do not write to it. All file storage directories should be created on these partitions.

Consider the following:

- If you create partitions, be sure to consider that the IM and Presence Service default file size setting (0) allows files up to 4GB to be transferred. This setting can be lowered when you set up managed file transfer.
- Consider the number of uploads per day and the average file size.
- Ensure that the partition has sufficient disk space to hold the expected volume of files.
- For example, 12000 users transfer 2 files per hour with an average file size of 100KB = 19.2GB per 8 hour day.

Directory Structure for External File Servers

When the first file transfer occurs, timestamped subdirectories are automatically created, as described in this example:

- We create the path `/opt/mftFileStore/node_1/` on an IM and Presence Service node.
- The directory `/files/` is autogenerated.
- The three `/chat_type/` directories (`im`, `persistent`, `groupchat`) are autogenerated.
- The date directory `/YYYYMMDD/` is autogenerated.
- The hour directory `/HH/` is autogenerated. If more than 1,000 files are transferred within an hour, additional roll-over directories `/HH.n/` are created.
- The file is saved with an autogenerated encoded resource name, hereafter referred to as `file_name`.

In this example, our complete path to a file is:
`/opt/mftFileStore/node_1/files/chat_type/YYYYMMDD/HH/file_name`

Using our example path:

- Files transferred during one-to-one IM on August 11th 2014 between 15.00 and 15.59 UTC are in the following directory: `/opt/mftFileStore/node_1/files/im/20140811/15/file_name`

  Files transferred during persistent group chat on August 11th 2014 between 16.00 and 16.59 UTC are in the following directory:
  `/opt/mftFileStore/node_1/files/persistent/20140811/16/file_name`
- The 1001st file transferred during ad hoc chat on August 11th 2014 between 16.00 and 16.59 UTC is in the following directory:
  `/opt/mftFileStore/node_1/files/groupchat/20140811/16.1/file_name`
- If no file transfers occur inside of an hour, there are no directories created for that period.

Note The traffic between IM and Presence Service and the file server is encrypted using SSHFS, but the file contents are written to the file server in unencrypted form.

User Authentication for the External File Server

IM and Presence Service authenticates itself and the file server using SSH keys:

- IM and Presence Service public key is stored on the file server.
- During connection, SSHFS validates the IM and Presence Service private key. This ensures that the content of all files is encrypted.
- The file server public key is stored on IM and Presence Service. This allows the IM and Presence Service to ensure that it is connecting to the configured file server and minimizes man-in-the-middle attacks.

Note 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.

External File Server Requirements

Follow these guidelines when setting up your external file server:

- Subject to file server capacity, each IM and Presence Service node requires its own unique Cisco XCP File Transfer Manager file server directory, however, nodes can share the same physical file server installation.
- The file server must support an ext4 file system, SSHv2, and SSH tools.
- The file server must support OpenSSH version between 4.9, 6.x, and 7.x.

Important This note is applicable for release 14SU3 onwards.

Note OpenSSH version 8.x is supported from release 14SU3 onwards.

- The network throughput between IM and Presence Service and the external file server must be greater than 60 megabytes per second.

  You can use the `show fileserver transferspeed` CLI command after you enable managed file transfer to determine your file server transfer speed. Be aware that if you run this command while the system is busy, it may impact the value returned by the command. For more information about this command, see the *Command Line Interface Guide for Cisco Unified Communications Solutions* at this link.

Partition Recommendations for External File Servers

Cisco recommends that you create one or more separate partitions that are dedicated to file transfer storage so that other applications that run on the server do not write to it. All file storage directories should be created on these partitions.

Consider the following:

- If you create partitions, be sure to consider that the IM and Presence Service default file size setting (0) allows files up to 4GB to be transferred. This setting can be lowered when you set up managed file transfer.
- Consider the number of uploads per day and the average file size.
- Ensure that the partition has sufficient disk space to hold the expected volume of files.
- For example, 12000 users transfer 2 files per hour with an average file size of 100KB = 19.2GB per 8 hour day.

Directory Structure for External File Servers

When the first file transfer occurs, timestamped subdirectories are automatically created, as described in this example:

- We create the path `/opt/mftFileStore/node_1/` on an IM and Presence Service node.
- The directory `/files/` is autogenerated.
- The three `/chat_type/` directories (`im`, `persistent`, `groupchat`) are autogenerated.
- The date directory `/YYYYMMDD/` is autogenerated.
- The hour directory `/HH/` is autogenerated. If more than 1,000 files are transferred within an hour, additional roll-over directories `/HH.n/` are created.
- The file is saved with an autogenerated encoded resource name, hereafter referred to as `file_name`.

In this example, our complete path to a file is:
`/opt/mftFileStore/node_1/files/chat_type/YYYYMMDD/HH/file_name`

Using our example path:

- Files transferred during one-to-one IM on August 11th 2014 between 15.00 and 15.59 UTC are in the following directory: `/opt/mftFileStore/node_1/files/im/20140811/15/file_name`

  Files transferred during persistent group chat on August 11th 2014 between 16.00 and 16.59 UTC are in the following directory:
  `/opt/mftFileStore/node_1/files/persistent/20140811/16/file_name`
- The 1001st file transferred during ad hoc chat on August 11th 2014 between 16.00 and 16.59 UTC is in the following directory:
  `/opt/mftFileStore/node_1/files/groupchat/20140811/16.1/file_name`
- If no file transfers occur inside of an hour, there are no directories created for that period.

Note The traffic between IM and Presence Service and the file server is encrypted using SSHFS, but the file contents are written to the file server in unencrypted form.

User Authentication for the External File Server

IM and Presence Service authenticates itself and the file server using SSH keys:

- IM and Presence Service public key is stored on the file server.
- During connection, SSHFS validates the IM and Presence Service private key. This ensures that the content of all files is encrypted.
- The file server public key is stored on IM and Presence Service. This allows the IM and Presence Service to ensure that it is connecting to the configured file server and minimizes man-in-the-middle attacks.

Note 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.

Partitions Recommendations for External File Server

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.

External File Server 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. This ensures that the content of all files is encrypted.
- The file server public key is stored on IM and Presence Service. This allows the IM and Presence Service to ensure that it is connecting to the configured file server and minimizes man-in-the-middle attacks.

Note 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.

External File Server Directory Structure

When the first file transfer occurs, timestamped subdirectories are automatically created, as described in this example:

- We create the path `/opt/mftFileStore/node_1/` on an IM and Presence Service node.
- The directory `/files/` is autogenerated.
- The three `/chat_type/` directories (`im`, `persistent`, `groupchat`) are autogenerated.
- The date directory `/YYYYMMDD/` is autogenerated.
- The hour directory `/HH/` is autogenerated. If more than 1,000 files are transferred within an hour, additional roll-over directories `/HH.n/` are created.
- The file is saved with an autogenerated encoded resource name, hereafter referred to as `file_name`.

In this example, our complete path to a file is:
`/opt/mftFileStore/node_1/files/chat_type/YYYYMMDD/HH/file_name`

Using our example path:

- Files transferred during one-to-one IM on August 11th 2014 between 15.00 and 15.59 UTC are in the following directory: `/opt/mftFileStore/node_1/files/im/20140811/15/file_name`

  Files transferred during persistent group chat on August 11th 2014 between 16.00 and 16.59 UTC are in the following directory:
  `/opt/mftFileStore/node_1/files/persistent/20140811/16/file_name`
- The 1001st file transferred during ad hoc chat on August 11th 2014 between 16.00 and 16.59 UTC is in the following directory:
  `/opt/mftFileStore/node_1/files/groupchat/20140811/16.1/file_name`
- If no file transfers occur inside of an hour, there are no directories created for that period.

Note The traffic between IM and Presence Service and the file server is encrypted using SSHFS, but the file contents are written to the file server in unencrypted form.

Managed File Transfer Task Flow

Complete these tasks to set up the Managed File Transfer feature on IM and Presence Service, and to set up your external file server.

Before you begin

Set up both an external database and an external file server for Managed File Transfer. For requirements, see

- External Database Prerequisites, on page 207
- External File Server Requirements, on page 207

For details on how to configure an external database, see the *External Database Setup 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.

Procedure

	Command or Action	Purpose
Step 1	Add External Database Connection, on page 213	Configure a connection to the external database from the IM and Presence Service.
Step 2	Set up an External File Server, on page 214	Before setting up users, directories, ownership, permissions and other tasks on the file server, set up the external file server.
Step 3	Create User for the External File Server, on page 215	Set up a user for the external file server.
Step 4	Set up Directory for External File Server, on page 216	Set up the top level directory structure for the external file server.
Step 5	Obtain Public Key for the External File Server, on page 217	Obtain the external file server's public key.
Step 6	Provision External File Server on IM and Presence Service, on page 218	Obtain the following information for the external file server:
Step 7	Verify Cisco XCP File Transfer Manager Activation, on page 220	The Cisco XCP File Transfer Manager service must be active on each node where Managed File Transfer is enabled.
Step 8	Enable Managed File Transfer, on page 221	Enable Managed File Transfer on IM and Presence Service.
Step 9	Verify External Server Status, on page 222	Verify that there are no problems with the external database setup and with the external file server setup.

Add External Database Connection

Configure a connection to the external database from the IM and Presence Service. With Managed File Transfer, you require a unique logical external database instance for each IM and Presence Service cluster node.

Before you begin

Set up each external database. For details, see the *External Database Setup Guide for the IM and Presence Service* at:

https://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 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.

Set up an External File Server

Before setting up users, directories, ownership, permissions and other tasks on the file server, set up the external file server.

Before you begin

Review the design recommendations for the external file server. For details, see External File Server Requirements, on page 207.

Procedure

Step 1 Install a supported version of Linux.

Step 2 Verify the file server supports SSHv2 and OpenSSH 4.9 or later by entering one of the following commands as root:

```
# telnet localhost 22

Trying ::1...

Connected to localhost.

Escape character is '^]'.

SSH-2.0-OpenSSH_5.3
```

Or

```
# ssh -v localhost

OpenSSH_5.3p1, OpenSSL 1.0.0-fips 29 Mar 2010

debug1: Reading configuration data /root/.ssh/config ...

...debug1: Local version string SSH-2.0-OpenSSH_5.3

...
```

Step 3 To allow private/public key authentication, make sure that you have the following fields in the `/etc/ssh/sshd_config` file, set to *yes*.

- RSAAuthentication *yes*
- PubkeyAuthentication *yes*

If these are commented out in the file, the setting can be left alone.

Tip To enhance security, you can also disable password log in for the file transfer user (*mftuser* in our example). This forces logging in only by SSH public/private key authentication.

Step 4 Cisco recommends that you create one or more separate partitions that are dedicated to file transfer storage so that other applications that run on the server do not write to it. All file storage directories should be created on these partitions.

What to do next

Create User for the External File Server, on page 215

Create User for the External File Server

Set up a user for the external file server.

Before you begin

Set up an External File Server, on page 214

Procedure

Step 1 On the file server as root, create a user for the managed file transfer feature. This user owns the file storage directory structure (our example uses *mftuser*) and force creation of the home directory (**-m**).

```
# useradd -m mftuser

# passwd mftuser
```

Step 2 Switch to the managed file transfer user.

```
# 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 Directory for External File Server, on page 216

Set up Directory for External File Server

Set up the top level directory structure for the external file server.

You can create any directory structure that you want, with any directory names. Be certain to create a directory for each managed file transfer-enabled node. Later, when you enable Managed File Transfer on IM and Presence Service, you must assign each directory to a node.

Important You must create a directory for each node that has managed file transfer enabled.

Note A file server partition/directory is mounted in the IM and Presence Service directory that is used to store files.

Before you begin

Create User for the External File Server, on page 215

Procedure

Step 1 Switch back to the root user.

```
$ exit
```

Step 2 Create a top-level directory structure (our example uses `/opt/mftFileStore/`) to hold directories for all of the IM and Presence Service nodes that have Managed File Transfer enabled.

```
# mkdir -p /opt/mftFileStore/
```

Step 3 Give *mftuser* sole ownership of the `/opt/mftFileStore/` directory.

```
# chown mftuser:mftuser /opt/mftFileStore/
```

Step 4 Give the *mftuser* sole permissions to the `mftFileStore` directory.

```
# chmod 700 /opt/mftFileStore/
```

Step 5 Switch to the *mftuser*.

```
# su mftuser
```

Step 6 Create a subdirectory under `/opt/mftFileStore/` for each managed file transfer enabled node. (Later, when you enable managed file transfer, you assign each directory to a node.)

```
$ mkdir /opt/mftFileStore/{node_1,node_2,node_3}
```

Note
- These directories and paths will be used in the **External File Server Diectory** field that you configure when you provision the file server in Cisco Unified CM IM and Presence Administration.
- If you have multiple IM and Presence Service nodes writing to this file server, you must define a target directory for each node, as we did in our example for three nodes`{node_1,node_2,node_3}`.
- Within each node's directory, the transfer type subdirectories (`im`, `groupchat`, and `persistent`) are automatically created by IM and Presence Service, as are all subsequent directories.

What to do next

Obtain Public Key for the External File Server, on page 217

Obtain Public Key for the External File Server

Obtain the external file server's public key.

Before you begin

Set up Directory for External File Server, on page 216

Procedure

Step 1 To retrieve the file server's public key, enter:

```
$ ssh-keyscan -t rsa host
```

Where *host* is the hostname, FQDN, or IP address of the file server.

Warning

- To avoid a man-in-the-middle attack, where the file server public key is spoofed, you must verify that the public key value that is returned by the **ssh-keyscan -t rsa** *host* command is the real public key of the file server.
- On the file server go to the location of the `ssh_host_rsa_key.pub` file (in our system it is under `/etc/ssh/`) and confirm the contents of the public key file, minus the host (the host is absent in the `ssh_host_rsa_key.pub` file on the file server), matches the public key value returned by the command **ssh-keyscan -t rsa** *host*.

Step 2 Copy the result of the **ssh-keyscan -t rsa** *host* command, not what is in the `ssh_host_rsa_key.pub` file. Be certain to copy the entire key value, from the server hostname, FQDN, or IP address to the end.

Note In most cases the server key begins with the hostname or FQDN, although it may begin with an IP address.

For example, copy:

hostname ssh-rsa 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. You will need it later, when you provision the file server on the IM and Presence Service.

Note If you are unable to retrieve the public key, see Troubleshooting External File Server Public and Private Keys, on page 223 for further help.

What to do next

Provision External File Server on IM and Presence Service, on page 218

Provision External File Server on IM and Presence Service

You must configure one external file server instance for each node in your cluster that will have Managed File Transfer enabled.

The external file server instances do not need to be physical instances of the external file server. However, be aware that for a given hostname, you must specify a unique external file server directory path for each external file server instance. You can configure all the external file server instances from the same node.

Before you begin

Obtain Public Key for the External File Server, on page 217

Obtain the following information for the external file server:

- Hostname, FQDN, or IP address
- Public key

- Path to the file storage directory
- User name

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **Messaging** > **External Server Setup** > **External File Servers**.

Step 2 Click **Add New**.
The **External File Servers** window appears.

Step 3 Enter the server details. For help with the fields and their configuration options, see External File Servers Fields, on page 219.

Step 4 Click **Save**.

Step 5 Repeat this procedure until you have created a separate external file server instance for each cluster node where managed file transfer is enabled.

What to do next

Verify Cisco XCP File Transfer Manager Activation, on page 220

External File Servers Fields

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.

Field	Description
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.

Verify Cisco XCP File Transfer Manager Activation

The Cisco XCP File Transfer Manager service must be active on each node where Managed File Transfer is enabled.

This service can only starts if an external database and an external file server have been assigned, and if the service can connect to the database and mount the file server.

Before you begin

Provision External File Server on IM and Presence Service, on page 218

Procedure

Step 1 On any node in the cluster, log in to the **Cisco Unified IM and Presence Serviceability** user interface.

Step 2 Choose **Tools** > **Service Activation**.

Step 3 From the **Server** drop-down, choose a node where Managed File Transfer is enabled, and click **Go**.

Step 4 Confirm that the **Cisco XCP File Transfer Manager** service's **Activation Status** reads **Activated**.

Step 5 If the service is deactivated, check the **Cisco XCP File Transfer Manager** check box and click **Save**.

Step 6 Repeat this procedure for all cluster nodes where Managed File Transfer is enabled.

What to do next

Enable Managed File Transfer, on page 221

Enable Managed File Transfer

Enable Managed File Transfer on IM and Presence Service.

Procedure

Step 1 Sign in to **Cisco Unified CM IM and Presence Administration**, choose **Messaging** > **File Transfer**. The **File Transfer** window opens.

Step 2 In the File Transfer Configuration area, choose either **Managed File Transfer** or **Managed and Peer-to-Peer File Transfer** depending on your deployment. See File Transfer Options, on page 222

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).

Warning
- If the managed file transfer feature is configured and the File Transfer Type is changed to either **Disabled** or **Peer-to-Peer**, all managed file transfer settings are deleted.
- A node's keys are invalidated if the node is unassigned from the external database and file server.

b) On the external file server, if it was not left open, open the `~mftuser/.ssh/authorized_keys` file that you created under the *`mftuser`*'s home directory and (on a new line) append each node's public key.

Note The `authorized_keys` file must contain a public key for each managed file transfer enabled IM and Presence Service node that is assigned to the file server.

c) Save and close the `authorized_keys` file.

Step 7 (Optional) Configure the managed file transfer service parameters to define the threshold at which an RTMT alarm is generated for the external file server disk space.

Step 8 Restart the Cisco XCP Router service on all nodes where Managed File Transfer is enabled. See Restart Cisco XCP Router service.

What to do next

Verify External Server Status, on page 222

File Transfer Options

You can configure one of the following file transfer options on the File Transfer window:

File Transfer Option	Description
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.

Verify External Server Status

Verify that there are no problems with the external database setup and with the external file server setup.

Before you begin

Enable Managed File Transfer, on page 221

Procedure

Step 1 To verify the status of the external database:

a) In **Cisco Unified CM IM and Presence Administration**, choose **Messaging** > **External Server Setup** > **External Databases**.

b) Check the information provided in the External Database Status area.

Step 2 On the IM and Presence Service node where you need to verify that the external file server is assigned:

a) In **Cisco Unified CM IM and Presence Administration**, choose **Messaging** > **External Server Setup** > **External File Servers**.

b) Check the information provided in the External File Server Status area to verify that the ceonnection is trouble free.

Troubleshooting External File Server Public and Private Keys

When a server private/public key pair is generated the private key is usually written to `/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:

Procedure

Step 1 Enter the following command:

```
$ ssh-keygen -t rsa -b 2048
```

Step 2 Copy the file server's public key.

You must copy the entire string of text for the public key from the hostname, FQDN, or the IP address (for example, *hostname* ssh-rsa AAAAB3NzaC1yc...). In most Linux deployments the key contains the server's hostname or FQDN.

Tip If the output from the `$ ssh-keygen -t rsa -b 2048` command doesn't contain a hostname, then use the output from the following command instead: `$ ssh-keyscan` *hostname*

Step 3 For each IM and Presence Service node that is configured to use this file server, paste the public key into the **External File Server Public Key** field on the **External File Server Configuration** window.

Important Passwordless SSH must be configured for the managed file transfer feature. See the SSHD man page for full configuration instructions for passwordless SSH.

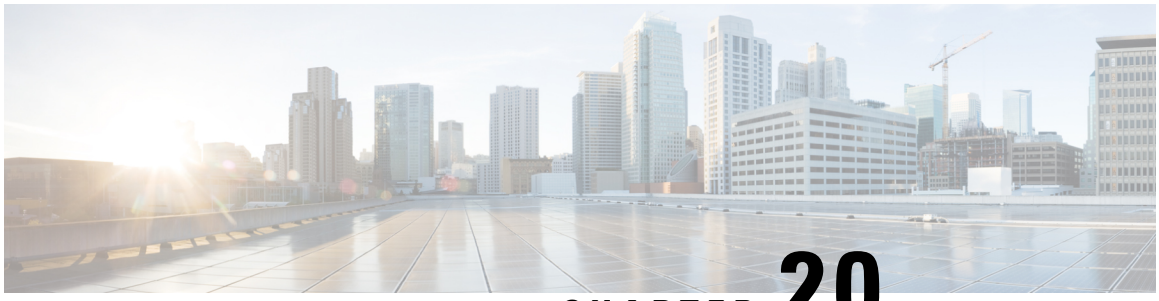
Note While checking the status from the publisher node to the subscriber node, and vice versa the information message "The diagnostics tests for this External File Server may be run from here." is displayed.

In the logs we see "pingable": "-7", which means we are viewing the status of other node where the external file server is not configured.

We configure external file server on the publisher node and the publisher nodes public key is shared in the external file server's "Authorized_key" file.

Administering Managed File Transfer

After you configure Managed File Transfer, you will need to administer the feature on an ongoing basis. For example, you will need to put a system in place for managing file server and database growth. Managed File Transfer Administration Overview, on page 273.



CHAPTER 20

Configure Multiple Device Messaging

Multiple Device Messaging Overview

With Multiple Device Messaging (MDM), you can have one-to-one instant message (IM) conversations tracked across all devices on which you are currently signed in. If you are using a desktop client and a mobile device, both of which are MDM-enabled, messages are sent, or carbon copied, to both devices. Read notifications are also synchronized on both devices as you participate in a conversation.

MDM lets you maintain an IM conversation while moving between any of your devices. For example, if you start an IM conversation on your desktop computer, but you have to leave your desk for a meeting, you can you can continue the IM conversation on your mobile device. Clients must be signed-in to be MDM-enabled. Signed-out clients do not display sent or received IMs or notifications.

MDM supports quiet mode, which helps to conserve battery power on your mobile devices. The Jabber client turns quiet mode on automatically when the mobile client is not being used. Quiet mode is turned off when the client becomes active again.

Multiple Device Messaging Prerequisites

Instant messaging must be enabled. For details, see Group Chat and Persistent Chat Task Flow, on page 182

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.

Configure Multiple Device Messaging

Multiple Device Messaging is enabled by default. You can use this procedure to disable the feature, or to turn it back on after it has been disabled.

Procedure

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

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

Step 3 From the **Service** drop-down list, choose **Cisco XCP Router (Active)**.

Step 4 From the **Enable Multi-Device Messaging** drop-down list, select either **Enabled** (the default value) or **Disabled**.

Step 5 Click **Save**.

Step 6 Restart the Cisco XCP Router service:

a) Log in to Cisco Unified IM and Presence Serviceability and choose **Tools** > **Control Center - Network Services**.

b) From the **Server** drop-down list box, select the IM and Presence publisher node.

c) Under **IM and Presence Services**, select **Cisco XCP Router** and click **Restart**.

Multiple Device Messaging Flow Use Case

This flow describes how messages and notifications are handled when a user, Alice, has MDM enabled on her laptop and mobile device.

1. Alice has a Jabber client open on her laptop, and is also using Jabber on her mobile device.
2. Alice receives an instant message (IM) from Bob.

   Her laptop receives a notification and displays a new message indicator. Her mobile device receives a new message with no notification.

Note IMs are always sent to all MDM-enabled clients. Notifications are displayed either on the active Jabber client only or, if no Jabber client is active, notifications are sent to all Jabber clients.

3. Alice chats with Bob for 20 minutes.

   Alice uses her laptop as normal to do this, while on her mobile device new messages are received and are marked as read. No notifications are sent to her mobile device.
4. When Alice receives three chat messages from a third user, Colin, Alice's devices behave as they did in step 2.
5. Alice does not respond, and closes the lid on her laptop. While on the bus home Alice receives another message from Bob.

In this case, both her laptop and mobile device receive a new message with notifications.

6. Alice opens her mobile device, where she finds the new messages sent from Bob and Colin. These messages have also been sent to her laptop.
7. Alice reads through her messages on her mobile device, and as she does so, messages are marked as read on both her laptop and on her mobile device.

Multiple Device Messaging Quiet Mode Use Case

This flow describes the steps Multiple Device Messaging uses to enable quiet mode on a mobile device.

1. Alice is using Jabber on her laptop and also on her mobile device. She reads a message from Bob and sends a response message using Jabber on her laptop.
2. Alice starts using another application on her mobile device. Jabber on her mobile device continues working in the background.
3. Because Jabber on her mobile device is now running in the background, quiet mode is automatically enabled.
4. Bob sends another message to Alice. Because Alice's Jabber on her mobile device in quiet mode, messages are not delivered. Bob's response message to Alice is buffered.
5. Message buffering continues until one of these triggering events occur:
   - An `<iq>` stanza is received.
   - A `<message>` stanza is received when Alice has no other active clients currently operating on any other device.

Note An active client is the last client that sent either an Available presence status or an instant message in the previous five minutes.

   - The buffering limit is reached.
6. When Alice returns to Jabber on her mobile device, it becomes active again. Bob's message, which had been buffered is delivered, and Alice is able to view it.

Multiple Device Messaging Interactions and Restrictions

The following table summarizes feature interactions and restrictions with the Multiple Device Messaging (MDM) feature.

Table 25: Multiple Device Messaging Interactions and Restrictions

Feature	Interaction or Restriction
Cisco Jabber Clients	MDM is supported by all Jabber clients from version 11.7 and higher.

Feature	Interaction or Restriction
Group Chat	Group chat is available for all MDM users, who have signed in from any device.
Message Archiver	MDM is compatible with the Message Archiver feature.
Managed File Transfer	File transfer is available for all MDM users, who have signed in from any device.
Mobile and Remote Access via Expressway	For Mobile and Remote Access clients that connect to IM and Presence Service via Cisco Expressway, you must be running at least Expressway X8.8 minimum to use MDM.
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.
Third-Party Clients	MDM is compatible with third-party clients that do not support the feature.

Counters for Multiple Device Messaging

Multiple Device Messaging (MDM) uses the following counters from the Cisco XCP MDM Counters Group:

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.
MDMBufferFlushPacketCount	The number of packets flushed in the last timeslice.
MDMBufferAvgQueuedTime	The average time in seconds before the MDM buffer is flushed.

Device Capacity Monitoring

When you enable Multiple Device Messaging (MDM) each user logged in from multiple device adds traffic load on the IM and Presence server. When the number of active logged in users reaches certain limit, this

results in resource shortage (memory consumption, CPU utilization) and in unexpected performance issues and failures.

The Device Capacity Monitoring feature helps address these issues by implementing additional counters to assist in monitoring the number of sessions created on the node.

The following Jabber Session Manager(JSM) sessions are created on IM&P Node:

- Composed JSM session — gets created when a user is assigned to a node.
- Active JSM session
  - On-premise User login.
  - Off-premise User login.
- Phantom JSM session — for push enabled users, which handles HA failover use cases.
- Spark Interop JSM session — for hybrid users.

The following counters are introduced to monitor the JSM sessions:

- **JsmClientSessionsActive**
- **JsmPhantomSessionsActive**
- **JsmHybridSessionsActive**

Additionally, a new counter **JSMSessionsExceedsThreshold** is introduced to monitor the JSM threshold limit, which is computed based on JSM session counters and OVA size.

If the threshold limit of this counter exceeds the default value of 80% for a period of 10 minutes, the system raises "**JSMSessionsExceedsThreshold**" alert in the Real-Time monitoring Tool (RTMT).

Configure alert value using the RTMT

You can use this procedure to configure **JSMSessionsExceedsThreshold** alert value using the RTMT.

Procedure

Step 1 Log in to **Real-Time Monitoring Tool (RTMT)**, choose **System** > **Tools** > **Alert Central**.

Step 2 Click **IM and Presence** and choose **JSMSessionsExceedsThreshold** Alert name.

Step 3 Right click on **JSMSessionsExceedsThreshold** and select **Set Alert/Properties**.

Step 4 Check the **Enable Alert** check box to enable the alert.

Step 5 Set the percentage limit for number of JSM session threshold exceed value, by default the value is 80%.

Step 6 Click **Save**.

Step 7 Set the Frequency and Schedule of the alert, By default the alert is triggered every 10 mins.

Step 8 Click **Next**.

Step 9 Click **Save**.

JSM sessions support per node

The following table lists the total number of JSM sessions that can be supported per node based on testing:

OVA Size	JSM Session Count is 1.5 times of OVA Capacity
5K OVA	7.5K

OVA Size	JSM Session Count is 1.5 times of OVA Capacity
15K OVA	22.5K
25K OVA	37.5K

Note If high availability is enabled and both nodes are in ACTIVE–ACTIVE configuration, then:

1. The total number of JSM sessions that can be supported per node would be 50% of the above mentioned capacity because there is a limitation in custom alarms that it can only be configured per node.
2. You must modify the **JSMSessionsExceedsThreshold** counter value based on HA configuration.

Suggested Action:

When a custom alert is raised, check the memory and CPU usage counters from the RTMT tool for the particular node. If memory and CPU usage counter's value exceeds the threshold limits, it is recommended to load balance the users between the IM&P nodes. Currently IM&P doesn't have a mechanism to automatically load balance users between the nodes.

User Session Report for Device Capacity Monitoring

Use this procedure to view the User Session Report. This report lets you view details of the active users logged in from multiple devices at the cluster, sub cluster, and node level.

Procedure

Step 1 Log in to **Cisco Unified IM and Presence Reporting**.

Step 2 Choose **System Reports** > **IM and Presence User Sessions Report**.

Step 3 Select the **Generate Report** (bar chart) icon in the reports window to generate the User Session Report for the current time.

Step 4 Click **OK**.

Step 5 Under the Column **Report Name**, click **IM and Presence User Sessions Report**.

Note
- This report generation may take approximately 2 or more minutes.
- This report displays the Presence Redundancy Group, Node Name, Count of users logged in from one or more devices, Total number of sessions at the cluster, sub cluster, and node level along with the date and timestamp of the report generated.

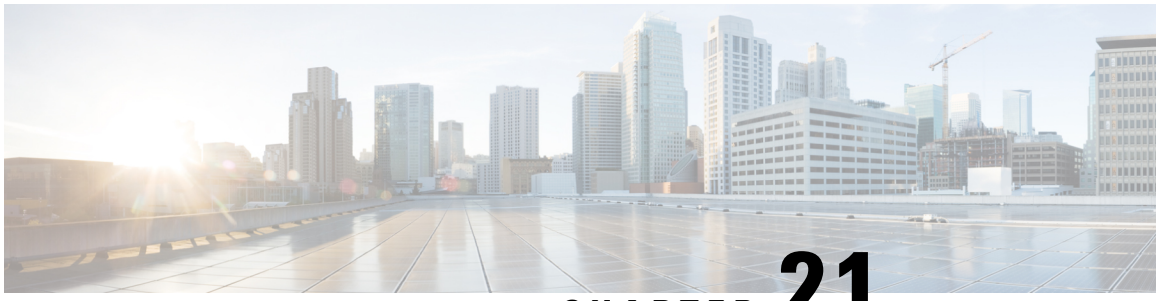
Step 6 Click **download** (green arrow) icon on the right side of the Reports window to download the User Session Report for cluster, subcluster, and node level in the CSV format.

Step 7 Click the values listed in the column **Count of users logged in from one or more devices**, to generate the detailed user based report for a particular node.

Step 8 Click **download** (green arrow) icon on the right side of the Reports window to download the detailed user level information per node in the CSV format.

Note When you hover over the column **Number of sessions**, the tooltip **device type** displays the type of device using which you have logged in.

For example, the device type can be Desktop, iPad, iPhone.



CHAPTER 21

Configure Enterprise Groups

Enterprise Groups Overview

When Enterprise Groups is configured, Cisco Unified Communications Manager includes user groups when it synchronizes its database with an external LDAP directory. In Cisco Unified CM Administration, you can view synced groups in the User Groups window.

This feature also helps administrators to:

- Provision users with similar characteristics traits with a comment set of features (for example, the sales and accounting teams).
- Target messages to all users in a specific group.
- Configure uniform access for all members of a specific group

This feature also helps Cisco Jabber users to quickly build contact lists of users who shares common traits. Cisco Jabber users can search the external LDAP Directory for user groups and then add them to their contact list. For example, a Jabber user can search the external LDAP directory and add the sales group to a contact list, thereby adding all of the sales team members into the contact list as well. If the group gets updated in the external directory, the user's contact list is updated automatically.

Enterprise Groups is supported with Microsoft Active Directory on Windows as the external LDAP directory.

Note If you disable the Enterprise Groups feature, Cisco Jabber users cannot search for enterprise groups or see the groups that they already added to their contact lists. If a user is already logged in when you disable the feature, the group will be visible until the user logs out. When the user logs in again, the group will not be visible

Security Groups

Security Groups are a subfeature of Enterprise Groups. Cisco Jabber users can also search for, and add, security groups to their contact list. To set up this feature, administrators must configure a customized LDAP filter and apply it to the configured LDAP directory sync. Security Groups are supported with Microsoft Active Directory only.

Maximum Allowed Entries

When configuring Enterprise Groups, make sure that you configure contact list maximums that handle groups

- The maximum number of entries that are allowed in a contact list is the sum of the number of entries in the contact list and the number of entries in groups that are already added to the contact list.
- Maximum entries in contact list = (number of entries in contact list) + (number of entries in groups)
- When the Enterprise Groups feature is enabled, Cisco Jabber users can add the groups to the contact list if the number of entries in the contact list is less than the maximum allowed entries. If the maximum allowed entries is exceeded while the feature is disabled, the users are not restricted until the feature is enabled. If the user continues to be logged in after the feature is enabled, no error message is displayed. When the user logs out and logs in again, an error message is displayed that asks the users to clear the excess entries.

Enterprise Groups Prerequisites

This feature assumes that you already have an LDAP Directory sync schedule configured with the below conditions. For details on how to configure an LDAP Directory sync, see the "Import Users from LDAP Directory" chapter of the *System Configuration Guide for Cisco Unified Communications Manager*.

- The Cisco DirSync service must be activated
- The LDAP Directory sync must include both users and groups
- Regular LDAP Directory syncs, as configured with the **LDAP Directory Synchronization Schedule** must be scheduled.

Supported LDAP Directories

Only Microsoft Active Directory is supported with enterprise groups.

LDAP Directory	Enterprise Groups Support
Microsoft Active Directory	Both enterprise groups and security groups are supported.
OpenLDAP	OpenLDAP on Windows has the following support: • Only the `GroupOfNames` object class is supported • Security groups are not supported with OpenLDAP. • Minimum version is 2.4.42. • OpenLDAP on Linux is not supported.

LDAP Directory	Enterprise Groups Support
Other LDAP Directories	Not supported.

Enterprise Groups Configuration Task Flow

Complete these tasks to configure the Enterprise Groups feature.

Procedure

	Command or Action	Purpose
Step 1	Verify Group Sync from LDAP Directory, on page 235	Confirm that your LDAP Directory sync includes both users and groups.
Step 2	Enable Enterprise Groups, on page 236	Complete this task to enable Cisco Jabber users to search for enterprise groups in Microsoft Active Directory and add them to their contact lists.
Step 3	Update OpenLDAP Config File, on page 236	(OpenLDAP only) Edit the config file `slapd.conf` in the OpenLDAP directory on Windows.
Step 4	Enable Security Groups, on page 236	(Optional) If you want Cisco Jabber users to be able to search for and add security groups to their contact lists, complete this task flow.
Step 5	View User Groups, on page 239	(Optional) View enterprise groups and security groups that are synchronized with Cisco Unified Communications Manager database.

Verify Group Sync from LDAP Directory

Use this procedure to confirm that your LDAP Directory sync includes users and groups.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Server** > **LDAP** > **LDAP Directory**.

Step 2 Click **Find** and select the LDAP directory from which you are syncing enterprise groups.

Step 3 Confirm that the **Synchronize** field has **Users and Groups** selected.

Step 4 Complete any remaining fields in the LDAP Directory configuration window. For help with the fields and their settings, refer to the online help.

Step 5 Click **Save**.

Enable Enterprise Groups

Configure the system to include enterprise groups in LDAP Directory syncs.

Procedure

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

Step 2 Under **User Management Parameters**, set the **Directory Group Operations on Cisco IM and Presence** parameter to **Enabled**.

Step 3 Enter a value for the **Maximum Enterprise Group Sized to allow Presence Information** parameter. The permitted range is 1 to 200 users with a default value of 100 users.

Step 4 From the **Syncing Mode for Enterprise Groups** drop-down list configure the LDAP sync that you want to perform at regular intervals: **None**, **Differential Sync**, **Full Sync**.

Note Refer to the enterprise parameter help for additional assistance in configuring these fields.

Step 5 Click **Save**.

Update OpenLDAP Config File

If you are configuring Enterprise Groups over OpenLDAP on Windows, you must update the `slapd.conf` file in the OpenLDAP directory.

Procedure

Step 1 In the OpenLDAP file directory on Windows, browse to the `slapd.conf` file.

Step 2 Open the file in a text editor.

Step 3 Add the following text to the file:

```
moduleload memberof.la
overlay memberof
memberof-group-oc groupOfNames
memberof-member-ad member
memberof-memberof-ad memberof
memberof-refint TRUE
cachesize 160000
```

Step 4 Save the file.

Step 5 Restart the OpenLDAP directory.

Enable Security Groups

If you want to allow Cisco Jabber users to be able to add a security group to their contact list, complete these optional tasks to include security groups in an LDAP Directory sync.

Note Security group sync is supported from Microsoft Active Directory only.

Note You cannot add new configurations into an existing LDAP Directory configuration in Cisco Unified Communications Manager where the initial sync has already occurred.

Procedure

	Command or Action	Purpose
Step 1	Create Security Group Filter, on page 237	Create an LDAP filter that filters both directory groups and security groups.
Step 2	Synchronize Security Groups from LDAP Directory, on page 237	Add your new LDAP filter to an LDAP Directory sync.
Step 3	Configure Cisco Jabber for Security Groups, on page 238	Update existing service profiles to give Cisco Jabber users whom are associated to that service profile access to search and add security groups.

Create Security Group Filter

Create an LDAP filter that filters security groups.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **LDAP** > **LDAP Filter**.
Step 2 Click **Add New**.
Step 3 Enter a unique **Filter Name**. For example, `syncSecurityGroups`.
Step 4 Enter the following **Filter**: `(&(objectClass=group)(CN=*))`.
Step 5 Click **Save**.

Synchronize Security Groups from LDAP Directory

Add your Security Group filter to an LDAP Directory sync and complete a sync.

Note You cannot add new configurations into an existing LDAP Directory configuration in Cisco Unified Communications Manager if the initial LDAP sync has already occurred.

Note For detailed information on how to set up a new LDAP Directory sync, see the "Configure End Users" part of the *System Configuration Guide for Cisco Unified Communications Manager*.

Before you begin

Create Security Group Filter, on page 237

Procedure

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

Step 2 Do one of the following:

- Click Add New to create a new LDAP Directory.
- Click **Find** and select the LDAP Directory from which the security groups will be synchronized.

Step 3 From the **LDAP Custom Filter for Groups** drop-down list, select the security group filter that you created.

Step 4 Click **Save**.

Step 5 Configure any remaining fields in the **LDAP Directory Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 6 Click **Perform Full Sync Now** to synchronize immediately. Otherwise, security groups will be synchronized when the next scheduled LDAP sync occurs.

Configure Cisco Jabber for Security Groups

Update existing service profiles to allow Cisco Jabber users whom are associated to that service profile to add security groups from an LDAP directory to their contact lists.

Note For information on how to set up new service profiles and assign them to Cisco Jabber users, see the "Configure Service Profiles" chapter of the *System Configuration Guide for Cisco Unified Communications Manager*.

Before you begin

Synchronize Security Groups from LDAP Directory, on page 237

Procedure

Step 1 Complete any remaining fields in the **Service Profile Configuration** window. For help with the fields and their settings, refer to the online help.

Step 2 Click **Find** and select the service profile that your Jabber users use.

Step 3 Under **Directory Profile**, check the **Allow Jabber to Search and Add Security Groups** check box.

Step 4 Click **Save**.

Cisco Jabber users who are associated to this service profile can now search and add security groups.

Step 5 Repeat this procedure for all service profiles that your Cisco Jabber users use.

View User Groups

You can view the enterprise groups and security groups that are synchronized with the Cisco Unified Communications Manager database using the following steps.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **User Group**.
The **Find and List User Groups** window appears.

Step 2 Enter search criteria and click **Find**.
A list of user groups that match the search criteria is displayed.

Step 3 To view a list of users that belong to a user group, click on the required user group.
The **User Group Configuration** window appears.

Step 4 Enter search criteria and click **Find**.
A list of users that match the search criteria is displayed.

If you click on a user in the list, the **End User Configuration** window appears.

What to do next

(Optional) Enable Security Groups, on page 236

Enterprise Groups Deployment Models (Active Directory)

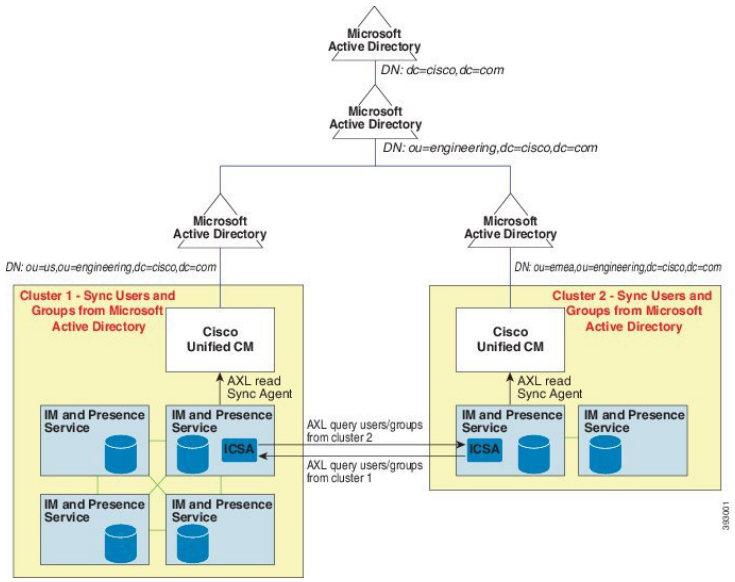
The Enterprise Groups feature offers two deployment options for Active Directory.

Important Ensure that Cluster 1 and Cluster 2 have a unique set of UserGroup, UserGroupMember, and UserGroupWatcherList records before synchronizing data through the Cisco Intercluster Sync Agent service. If both the clusters have unique sets of records, both the clusters will have a super set of all the records after synchronization.

Enterprise Groups Deployment Model 1

In this deployment model, Cluster 1 and Cluster 2 synchronize different subsets of users and groups from Microsoft Active Directory. The Cisco Intercluster Sync Agent service replicates the data from Cluster 2 into Cluster 1 to build the complete database of users and groups.

Figure 8: Enterprise Groups Deployment Model 1



Enterprise Groups Deployment Model 2

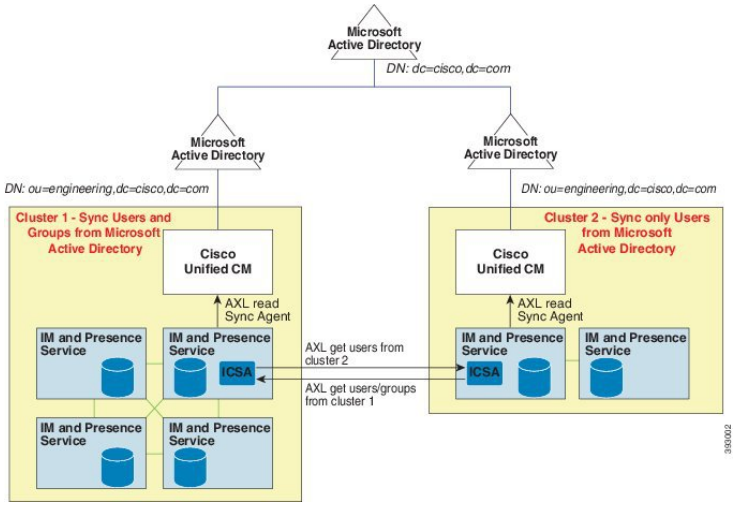
In this deployment model, Cluster 1 synchronizes all the users and groups from Microsoft Active Directory. Cluster 2 synchronizes only users from Microsoft Active Directory. The Cisco Intercluster Sync Agent service replicates groups information from Cluster 1 into Cluster 2.

Caution If you are using this deployment model, ensure that you synchronize the groups data in only one cluster. The Enterprise Groups feature will not work as expected if you fail to do so.

You can verify your configuration on the **Cisco Unified CM IM and Presence Administration** > **Presence** > **Inter-Clustering** window.

Check the status of the **Enterprise Groups LDAP Configuration** parameter in the Inter-cluster peer table. **No conflict found** means there are no misconfigurations between peers. If there are conflicts found, click the Enterprise GroupConflicts link, and click the **details** button which appears. This opens a Reporting window for a detailed report.

Figure 9: Enterprise Groups Deployment Model 2



Enterprise Groups Limitations

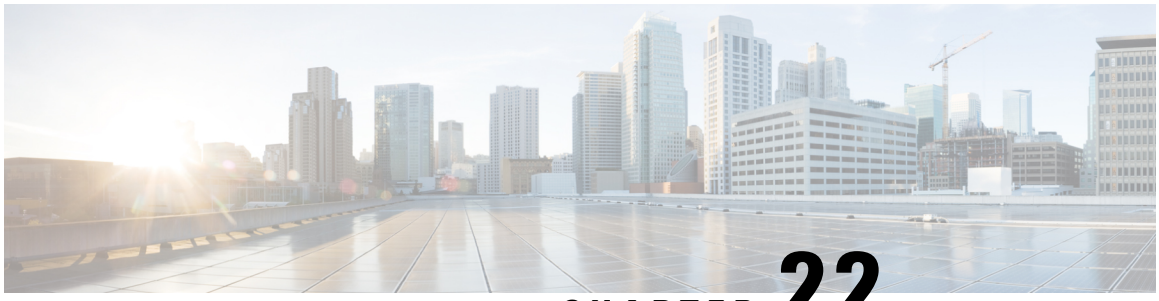
Table 26: Enterprise Groups Limitations

Limitation	Description
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.

Limitation	Description
Intercluster peering with a 10.x cluster	Enterprise Groups is supported for releases 11.0(1) and higher. If the synced group includes group members from a 10.x intercluster peer, users on the higher cluster cannot view the presence of synced members from the 10.x cluster. This is due to database updates that were introduced in 11.0(1) for the Enterprise Groups sync. These updates are not a part of the 10.x releases. To guarantee that users homed on the higher cluster can view the presence of group members homed on the 10.x cluster, users on the higher cluster should manually add the 10.x users to their contact lists. There are no presence issues for manually added users.
Multilevel grouping	Multilevel grouping is not allowed for the group sync.
Group-only synchronization	When a user group and users are present in the same search base, group-only synchronization is not allowed. Instead, the user group as well as the users are synchronized.
Maximum number of user groups	You can synchronize a maximum of 15000 user groups from Microsoft Active Directory server to the Unified Communications Manager database. Each user group can contain from 1 to 200 users. You can configure the exact amount on the **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters** window. The maximum number of user accounts in the database cannot exceed 160,000.
User group migration	If a user group is moved from one organization unit to another, you must perform a full sync on the original unit followed by a full sync on the new unit.
Local groups	Local groups are not supported. Only groups synchronized from Microsoft Active Directory are supported.
Group members not assigned to IM and Presence Service nodes	Group members that are not assigned to IM and Presence Service nodes display in the contact list with the presence bubble greyed out. However, these members are considered when calculating a maximum numbers of users allowed in the contact list.
Migration from Microsoft Office Communication Server	During migration from Microsoft Office Communication Server, the Enterprise Groups feature is not supported until users are fully migrated to the IM and Presence Service node.
LDAP synchronization	If you change the synchronization option in the **LDAP Directory Configuration window** while the synchronization is in progress, the existing synchronization remains unaffected. For example, if you change the synchronization option from **Users and Groups** to **Users Only** when the synchronization is in progress, the users and groups synchronization still continues.

Limitation	Description
Group search functionality over the Edge	Group search functionality over the Edge is offered in this release, but has not been fully tested. As a result, full support for group searches over the Edge cannot be guaranteed. Full support is expected to be offered in a future release.
Cisco Intercluster Sync Agent service periodic synchronization	If a group name or a group member name is updated in the external LDAP directory, it gets updated on the Cisco Jabber contact list only after the periodic Cisco Intercluster Sync Agent service synchronization. Typically, the Cisco Intercluster Sync Agent service synchronization occurs every 30 minutes.
Synchronization of users and user groups through different synchronization agreements in LDAP configuration	If users and user groups are synchronized into the Cisco Unified Communications Manager database as part of the same synchronization agreement, the user and group association gets updated as expected in Cisco Unified Communications Manager database after synchronization. However, if a user and user group are synchronized as part of different synchronization agreements, the user and the group may not get associated in the database after the first synchronization. The user and group association in the database depends on the sequence in which the synchronization agreements are processed. If the users are synchronized ahead of the groups, then the groups may not be available in the database for association. In such cases, you must ensure that the synchronization agreement with groups is scheduled ahead of the synchronization agreement with the users. Otherwise, after the groups synchronize into the database, the users will get associated with the groups after the next manual or periodic sync with the sync type set as Users and Groups. Users and corresponding group info will be mapped only when the agreement sync type is set as Users and Groups .
Tested OVA information for Enterprise Groups	**Tested Scenario** 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.

Limitation	Description
Export Contact List	When you export the user's contact list using **Bulk Administration** > **Contact List** > **Export Contact List**, the Contact List CSV file doesn't include the details of enterprise group they had in Jabber client.



CHAPTER 22

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 247.

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.

Note To enable branding, you must use the primary administrator account with privilege level 4 access. This is the main administrator account that is created during installation.

Note Ensure that you use only one among GUI and CLI to enable branding as well as to disable it. For example, if you enable branding using the GUI interface, you must use the GUI interface itself to disable branding. Else, it will not function properly.

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.

Note Ensure that you use only one among GUI and CLI to enable branding as well as to disable it. For example, if you enable branding using the GUI interface, you must use the GUI interface itself to disable branding. Else, it will not function properly.

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 27: 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 10: Branding Options for the Administration Login Screen

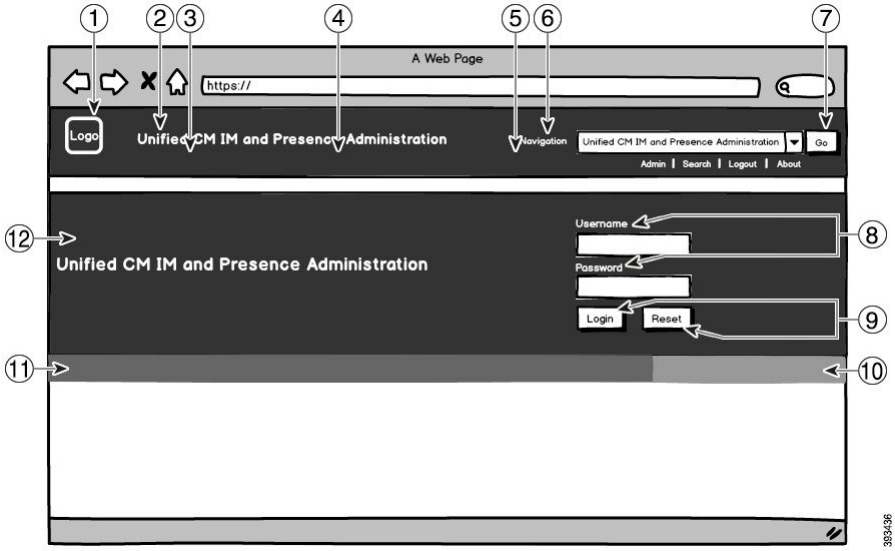
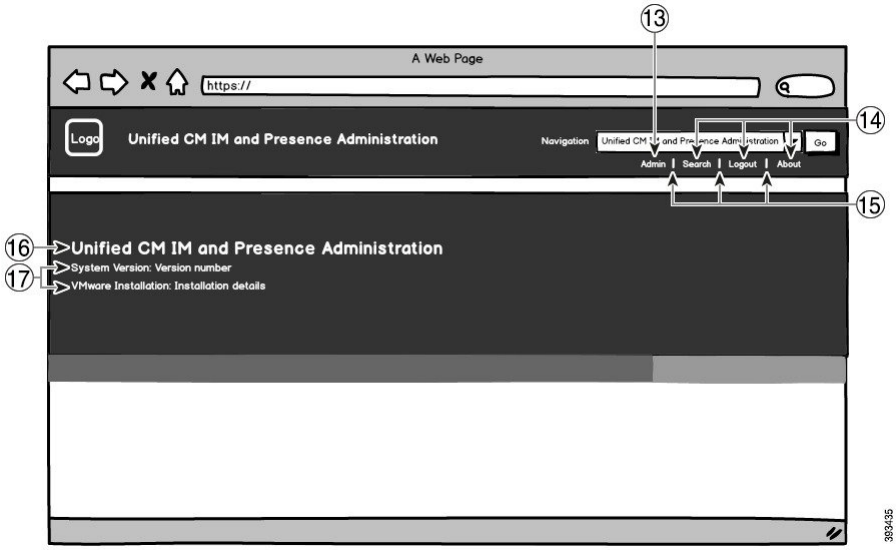


Figure 11: Branding Options for the Administration Logged In Screen



The following table describes how the callout items in the above screen captures can be customized.

Table 28: User Interface Branding Options

Item	Description	Branding Edits
Login Screen Image		

Item	Description	Branding Edits
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)
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

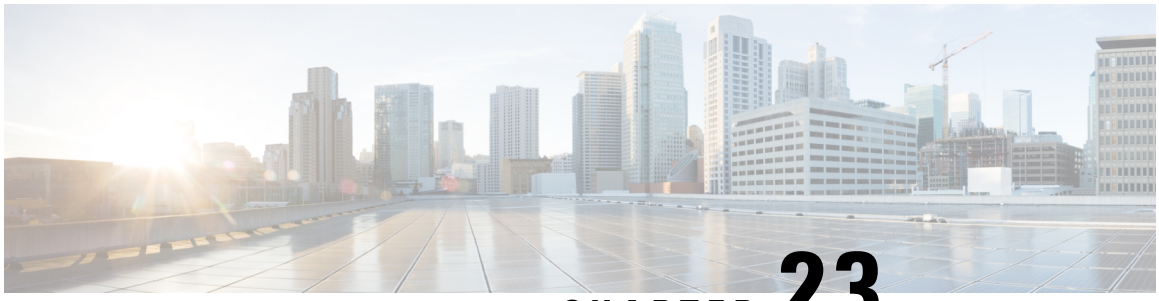
Item	Description	Branding Edits
10	Bottom background color – right	splash.hex.code.3
11	Bottom background color – left	splash.hex.code.2
12	Banner	splash.hex.code.1
Post Login Image		
13	Logged in user text (for example, the 'admin' user)	header.text.bold.color
14	Search, About, Logout links	header.link.color
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).



CHAPTER 23

Configure Advanced Features

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 29: 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**.

Calendar Integration with Microsoft Outlook

This feature allows users to incorporate their calendar and meeting status from Microsoft Outlook into their Presence status on the IM and Presence Service server. If a user is in a meeting, that status will display as a part of the user's Presence status. This feature can be configured by connecting the IM and Presence Service to an on-premises Microsoft Exchange server or to a hosted Office 365 server.

For details on how to configure calender integration with Microsoft Outlook, refer to the document *Calendar Integration with Microsoft Outlook for the IM and Presence Service* at http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html.

Federation

On IM and Presence Service, you can create federated networks from within any domain that IM and Presence Service manages. There are two main types of Federation deployments:

- Interdomain Federation—This integration enables users from within any domain that IM and Presence Service manages to exchange availability information and Instant Messaging (IM) with users in external domains. The external domain may be managed by a Microsoft, Google, IBM, or AOL server. IM and Presence Service can use a variety of protocols to communicate with the server in the external domain.
- Partitioned Intradomain Federation—With this integration, IM and Presence Service and the Microsoft server (for example, Microsoft Lync) host a common domain or set of domains. The integration allows IM and Presence Service client users and Microsoft Lync users within a single enterprise to exchange instant messaging and availability.
- SIP Open federation—Cisco IM and Presence service supports SIP open federation for Cisco Jabber clients. As an administrator, you can configure SIP open federation allowing Cisco Jabber users seamlessly federate with users from all available domains. You can configure open federation for all domains with a single static route. The static route lets Cisco Jabber federate with any external domain. More importantly, it significantly cuts down the time to configure and maintain SIP federation for individual domains.

For configuration information, see the *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager* or the *Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html.

Message Archiver

Many industries require that instant messages adhere to the same regulatory compliance guidelines as for all other business records. To comply with these regulations, your system must log and archive all business records, and the archived records must be retrievable.

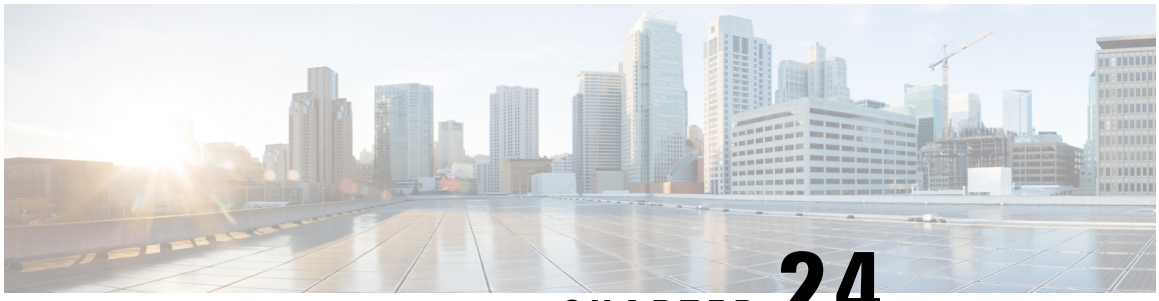
The IM and Presence Service supports instant messaging (IM) compliance by collecting data for the following IM activities in single cluster, intercluster, or federated network configurations:

- Point-to-point messages.
- Group chat - This includes ad-hoc, or temporary chat messages, and permanent chat messages.
- IM Compliance Components
- Sample Topologies and Message Flow for IM Compliance

For more information on configuring IM Compliance, see *Instant Messaging Compliance for IM and Presence Service on Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html.

PART IV

Administer the System



CHAPTER 24

Manage Chat

Manage Chat Overview

IM and Presence Service provides you with settings you can use to manage your chat rooms and to control who has access to them. This includes the ability to:

- Create new rooms, manage members and the configurations of the rooms they create.
- Control access to persistent chat rooms so that only members of that room have access.
- Assign Administrators to a chat room.
- Invite other users to a room.
- Determine the presence status of the members displayed within the room. The presence status displayed in a room confirms the attendance of the member in a room but may not reflect their overall presence status.

IM and Presence Service also lets you manage chat node aliases. Chat node aliases make it possible for your users to search for specific chat rooms on specific nodes, and to join those chat rooms.

In addition, the IM and Presence Service also stores transcripts and makes this chat room history available to room members, including members who have just joined the chat room. You can configure how much of the existing archive you want to make available to new and old members. .

Chat Node Alias Overview

Each chat node in a system must have a unique alias. Chat node aliases are unique addresses for each chat node so that users (in any domain) can search for specific chat rooms on specific nodes, and join chat in those rooms. Chat node aliases form a part of the unique ID for each chat room that is created on that node. For example, the alias `conference-3-mycup.cisco.com` gets used to name the chat room `roomjid@conference-3-mycup.cisco.com` that is created on that node.

There are two modes for assigning chat node aliases:

- System-generated—The system automatically assigns a unique alias to each chat node. By default, the system auto-generates one alias per chat node by using the following naming convention: `conference-x-clusterid.domain`, where:
  - `conference` is a hardcoded keyword
  - `x` is the unique integer value that denotes the node ID
  - `clusterid` is the configured enterprise parameter
  - `domain` is the configured domain

  For example, the system might assign: `conference-3-mycup.cisco.com`
- Manual—You must disable system-generated aliases to be able to assign chat node aliases manually. With manually-assigned aliases, you have complete flexibility to name chat nodes using aliases that suit your specific requirements. For example, you might do this if the `congerence-x-clusterid.domain` naming convention does not suit your deployment needs.

Assigning Multiple Aliases per Node

You can associate more than one alias with each chat node on a per-node basis. Multiple aliases per node allows users to create additional chat rooms using these aliases. This functionality applies to both system-generated aliases and aliases that are created manually.

Manage Chat Prerequisites

Ensure that you have persistent chat enabled.

Manage Chat Task Flow

Procedure

	Command or Action	Purpose
Step 1	Enable Chat Room Owners to Edit Chat Room Settings, on page 259	Configure whether you want to allow chat room owners to be able to edit chat room settings. Otherwise, only administrators will be able to edit chat room settings.
Step 2	Allow Clients to Log Instant Message History, on page 260	Configure whether you want to allow users to log instant message history locally on their computer.
Step 3	Limit Persistent Chat Room Creation to Home Cluster, on page 260	Use this procedure to limit the persistent chat room creation within Cisco Jabber users home cluster.
Step 4	View External Database Text Conferencing Report, on page 261	Use this procedure to view the External Database Text Conferencing Report that lets you view details on the persistent chat rooms.

	Command or Action	Purpose
Step 5	Transfering Ownership of Persistent Chat Rooms, on page 262	Use this procedure to transfer ownership of the persistent chat rooms belonging to the home cluster to any other existing member of the chat room.
Step 6	Persistent Chat Alias Report, on page 263	Use this procedure to view the chat rooms count on the own and peer cluster aliases present in the external database.
Step 7	Edit chat room settings. Complete any of the following tasks, in any order, to update chat room settings: • Set Number of Chat Rooms, on page 263 • Configure Chat Room Member Settings, on page 263 • Configure Availability Settings, on page 265 • Configure Occupancy Settings, on page 266 • Configure Chat Message Settings, on page 266 • Configure Moderated Room Settings, on page 267 • Configure History Settings, on page 267	**Note** If you update any of the Persistent Chat settings, on Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Feature Services** to restart the Cisco XCP Text Conference Manager service.
Step 8	Reset Chat Rooms to System Defaults, on page 268	Complete this optional task if you want to reset your chat configuration to the system defaults. Be aware that ad hoc chat is enabled by default, but persistent chat is disabled by default. Completing this task would disable persistent chat.
Step 9	Manage Chat Node Aliases, on page 268	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.
Step 10	Clean External Database for Persistent Chat, on page 271	Optional. Use the External Database Cleanup Utility to configure jobs that monitor the external database and delete expired records. This will ensure that there is always enough disk space for new records.

Enable Chat Room Owners to Edit Chat Room Settings

Use this procedure if you want to allow chat room owners to be able to edit chat room settings.

Note 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.

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **Messaging** > **Group Chat and Persistent Chat**.

Step 2 Configure a value for the **Room owners can change whether or not rooms are for members only** check box.

- Checked—Chat room owners have administrative ability to edit chat room settings.
- Unchecked—Only an administrator can edit chat room settings.

Step 3 Click **Save**.

Step 4 In **Cisco Unified IM and Presence Serviceability**, choose **Tools** > **Control Center - Feature Services**.

Step 5 Restart the Cisco XCP Text Conference Manager service.

Allow Clients to Log Instant Message History

You can prevent or allow users to log instant message history locally on their computer. On the client side, the application must support this functionality; it must enforce the prevention of instant message logging

Procedure

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

Step 2 Configure the log instant message history setting as follows:

- To allow users of client applications to log instant message history on IM and Presence Service, check **Allow clients to log instant message history (on supported clients only)**.
- To prevent users of client applications from logging instant message history on IM and Presence Service, uncheck **Allow clients to log instant message history (on supported clients only)**.

Step 3 Click **Save**.

Limit Persistent Chat Room Creation to Home Cluster

Important This feature is applicable from release 14 SU1 onwards.

Use this procedure to limit the persistent chat room creation within Cisco Jabber users home cluster. This feature reduces the inter-cluster traffic and increases the system bandwidth.

The IM and Presence Service administrator manages all the chat rooms created by the users on home cluster. The maintenance activity of other clusters does not impact chat rooms created by users in home clusters.

Before you begin

Important Supported from Release 14SU1 onwards.

- Confirm that persistent chat is enabled.
- Before enabling this feature, check the **Alias Report** on **Group Chat and Persistent Chat Settings** window. For more information see, Persistent Chat Alias Report, on page 263.
- Cisco Jabber 14.1 version or higher is needed to support this feature.

Procedure

Step 1 Log in to **Cisco Unified CM IM and Presence Service Administration** on the database publisher node.
Step 2 Choose **Messaging** > **Group Chat and Persistent Chat**.
Step 3 Under **Enable Persistent Chat**, check the **Limit room creation to home cluster** check box.

What to do next

Restart the **Cisco XCP Text Conference Manager Service** on all the nodes in the home cluster.

View External Database Text Conferencing Report

Use this procedure to view the External Database Text Conferencing Report. This report lets you view details of the persistent and ad-hoc chat rooms in your deployment.

Procedure

Step 1 Log into **Cisco Unified CM IM and Presence Administration**.
Step 2 Choose **Messaging** > **Group Chat and Persistent Chat**.
Step 3 Under **Persistent Chat Database Assignment**, click the **Room Report** button.
Step 4 Use the filter tools if you want to limit the selection to rooms that meet specific criteria.
Step 5 Click **Find**.
Step 6 Select a specific chat room to view details for that room.

Note The number of records fetched from the database depends on the value selected from "Records Fetched" drop-down list.

Transfering Ownership of Persistent Chat Rooms

Important This feature is applicable from release 14 SU1 onwards.

Use this procedure for the IM and Presence Service administrators who have the access to the GUI to transfer ownership of the persistent chat rooms.

For example, John has created a persistent chat room and added a few members, later leaves the organization.

If John was the only persistent chat room owner, and the room owner capabilities are still required for the given room, the IM and Presence Service administrator can select one or more current room members as new room owners.

Consider the following while updating the **Owner ID**:

- You can change the ownership of the chat room to any chat room members belonging to the same home cluster as the previous owner.
- **Owner ID** should be a **User JID** and not a **User ID**.
- The input **Owner ID** is validated against the IM and Presence Service node database.
- Administrator cannot set the room creator's ID as the new owner ID of the chat room.

To change ownership of a chat room, perform the following steps:

Before you begin

Important Supported from Release 14SU1 onwards.

Stop the **Cisco XCP Text Conference Manager Service** on all the IM and Presence Service nodes in the home cluster before updating the **Owner ID**.

Procedure

Step 1 Log into **Cisco Unified Communications Manager IM and Presence Service Administration** on the database publisher node.

Step 2 Select **Messaging** > **Group Chat and Persistent Chat**.

Step 3 Under,**Persistent Chat Database Assignment** click the **Room Report** button.

Step 4 Use the filter tools if you want to limit the selection to rooms that meet specific criteria and click **Find**.

Step 5 (Optional) Click on a **Room JID** to view the fields of PChat rooms such as, list of owners, list of members, and date of last message. See the online help for more information and description about the fields.

Step 6 Select the check box of a **Room JID** to edit the **Owner ID** field.

Note The **Owner ID** column is editable only for the persistent chat rooms belonging to the home cluster.

Step 7 Enter the **Owner ID** in E-mail format of the chat room member whom you want to make as the new owner.

Step 8 Click **Update Owner ID**.
This updates the owner of one or more selected persistent chat rooms with the same **Owner ID**.

What to do next

Start the **Cisco XCP Text Conference Manager Service** on all the nodes in the home cluster.

Persistent Chat Alias Report

Use this procedure to view the External Database Persistent Chat alias report which lets you view the chat rooms count and the home and peer cluster aliases present in the external database.

Procedure

Step 1 Log into **Cisco Unified CM IM and Presence Service Administration** on the database publisher node.
Step 2 Choose **Messaging** > **Group Chat and Persistent Chat**.
Step 3 Under **Persistent Chat Database Assignment**, select **External Database** from the drop-down list.
Step 4 Click **Alias Report** button. Refer to the online help for field descriptions.

Configure Chat Room Settings

Set Number of Chat Rooms

Use room settings to limit the number of rooms that users can create. Limiting the number of chat rooms helps the performance of the system and allows it to scale. Limiting the number of rooms also helps to mitigate any possible service-level attacks.

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **Messaging** > **Group Chat and Persistent Chat**.
Step 2 To change the maximum number of chat rooms that are allowed, enter a value in the field for **Maximum number of rooms allowed**. The default is set to 5500.
Step 3 Click **Save**.

Configure Chat Room Member Settings

Member settings allow control over the membership in chat rooms. Such a control is useful for users to mitigate service-level attacks that can be prevented by restricting membership. Configure the member settings as required.

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **Messaging** > **Group Chat and Persistent Chat**.

Step 2 Configure the room member settings as described in Room Member Settings.

Step 3 Click **Save**.

Step 4 In **Cisco Unified IM and Presence Serviceability**, choose **Tools** > **Control Center - Feature Services**.

Step 5 Restart the Cisco XCP Text Conference Manager service.

Room Member Settings

Note Persistent chat rooms inherit their settings when you create the room. Later changes do not apply to existing rooms. Those changes only apply to rooms created after the changes take effect.

Table 30:

Field	Description
Rooms are for members only by default	Check this check box if you want rooms to be created as members-only rooms by default. Members-only rooms are accessible only by users on an allowed list configured by the room owner or administrator. The check box is unchecked by default. **Note** The allowed list contains the list of members who are allowed in the room. It is created by the owner or administrator of the members-only room.
Only moderators can invite people to members-only rooms	Check this check box if you want to configure the room so that only moderators are allowed to invite users to the room. If this check box is unchecked, members can invite other users to join the room. The check box is checked by default.
Room owners can change whether or not rooms are for members only	Check this check box if you want to configure the room so that room owners are allowed to change whether or not rooms are for members only. The check box is checked by default. **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.

Field	Description
Room owners can change whether or not only moderators can invite people to members-only rooms	Check this check box if you want to configure the room so that room owners can allow members to invite other users to the room. The check box is checked by default.
Users can add themselves to rooms as members	Check this check box if you want to configure the room so that any user can request to join the room at any time. If this check box is checked, the room has an open membership. The check box is unchecked by default.
Room owners can change whether users can add themselves to rooms as members	Check this check box if you want to configure the room so that room owners have the ability to change the setting that is listed in Step 5 at any time. The check box is unchecked by default.

Configure Availability Settings

Availability settings determine the visibility of a user within a room.

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **Messaging** > **Group Chat and Persistent Chat**.

Step 2 Configure the availability member settings as described in Availability Settings.

Step 3 Click **Save**.

Step 4 In **Cisco Unified IM and Presence Serviceablity**, choose **Tools** > **Control Center - Feature Services**.

Step 5 Restart the Cisco XCP Text Conference Manager service.

Availability Settings

Field	Description
Members and administrators who are not in a room are still visible in the room	Check this check box if you want to keep users on the room roster even if they are currently offline. The check box is checked by default. **Note** If the administrator leaves the chat room, the administrator's userid will still be visible in the chat room. The user needs to close and reopen the chat room to refresh the user's list.
Room owners can change whether members and administrators who are not in a room are still visible in the room	Check this check box if you want to allow room owners the ability to change the visibility of a member or administrator. The check box is checked by default.

Field	Description
Rooms are backwards-compatible with older clients	Check this check box if you want the service to function well with older Group Chat 1.0 clients. The check box is unchecked by default.
Room owners can change whether rooms are backwards-compatible with older clients	Check this check box if you want to allow room owners the ability to control backward compatibility of the chat rooms. The check box is unchecked by default.
Rooms are anonymous by default	Check this check box if you want the room to display the user nickname but keep the Jabber ID private. The check box is unchecked by default.
Room owners can change whether or not rooms are anonymous	Check this check box if you want to allow room owners to control the anonymity level of the user Jabber ID. The check box is unchecked by default.

Configure Occupancy Settings

Occupancy settings determine how many users can be in a chat room at a given time.

Procedure

Step 1 To change the system maximum number of users that are allowed in a room, enter a value in the field for **How many users can be in a room at one time**. The default value is set to 1000.

Note The total number of users in a room should not exceed the value that you set. The total number of users in a room includes both normal users and hidden users.

Step 2 To change the number of hidden users that are allowed in a room, enter a value in the field for **How many hidden users can be in a room at one time**. Hidden users are not visible to others, cannot send a message to the room, and do not send presence updates. Hidden users can see all messages in the room and receive presence updates from others. The default value is 1000.

Step 3 To change the default maximum number of users that are allowed in a room, enter a value in the field for **Default maximum occupancy for a room**. The default value is set to 50 and cannot be any higher than the value that is set in Step 1.

Step 4 Check **Room owners can change default maximum occupancy for a room** if you want to allow room owners to change the default maximum room occupancy. The check box is checked by default.

Step 5 Click **Save**.

Configure Chat Message Settings

Use Chat Message settings to give privileges to users based on their role. For the most part, roles exist in a visitor-to-moderator hierarchy. For example, a participant can do anything a visitor can do, and a moderator can do anything a participant can do.

The check box is checked by default.

Procedure

Step 1 From the drop-down list for **Lowest participation level a user can have to send a private message from within the room**, choose one:

- **Visitor** allows visitors, participants, and moderators to send a private message to other users in the room.This is the default setting.
- **Participant** allows participants and moderators to send a private message to other users in the room.
- **Moderator** allows only moderators to send a private message to other users in the room.

Step 2 Check **Room owners can change the lowest participation level a user can have to send a private message from within the room** if you want to allow room owners to change the minimum participation level for private messages. The check box is checked by default.

Step 3 From the drop-down list for Lowest participation level a user can have to change a room's subject, choose one:

a) **Participant** allows participants and moderators to change the room's subject. This is the default setting.
b) **Moderator** allows only moderators to change the room's subject.

Visitors are not permitted to change the room subject.

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.

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**.

Reset Chat Rooms to System Defaults

Use this procedure if you want to reset your group chat settings for both ad hoc and persistent chat rooms to the system defaults..

Note Ad hoc chat is enabled by default, but persistent chat is disabled by default. Completing this task will disable persistent chat

Procedure

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

Step 2 Click **Set to Default**.

Step 3 Click **Save**.

Chat Node Alias Management

Manage Chat Node Aliases

Complete these tasks to manage chat node aliases for your cluster. You can have the system manage aliases automatically, or you can update them yourself.

Procedure

	Command or Action	Purpose
Step 1	Assign Mode for Managing Chat Aliases , on page 269	Assign whether you want the system to manage chat node aliases or whether you want to do it manually.
Step 2	Add Chat Node Alias Manually, on page 270	Add, edit, or delete chat node aliases for your cluster.

Assign Mode for Managing Chat Aliases

Configure whether you want the system to assign chat node aliases automatically using the `conference-x-clusterid.domain` naming convention, or whether you want to assign them manually.

Before you begin

For information on chat node aliases, see Chat Node Alias Overview, on page 257.

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **Messaging** > **Group Chat and Persistent Chat**.

Step 2 Enable or disable system-generated aliases:

- If you want the system to assign chat node aliases automatically, check **System Automatically Manages Primary Group Chat Server Aliases**.

  Tip Choose **Messaging** > **Group Chat Server Alias Mapping** to verify that the system-generated alias is listed under Primary Group Chat Server Aliases.

- If you want to assign chat node aliases manually, uncheck **System Automatically Manages Primary Group Chat Server Aliases**.

What to do next

- Even if you configure a system-generated alias for a chat node, you can associate more than one alias with the node if required.
- If you are federating with external domains, you may want to inform federated parties that the aliases have changed and new aliases are available. To advertise all aliases externally, configure DNS and publish the aliases as DNS records.
- If you update any of the system-generated alias configuration, perform one of these actions: Restart the Cisco XCP Text Conference Manager.
- To add, edit, or delete a chat node alias, Add Chat Node Alias Manually, on page 270.

Add Chat Node Alias Manually

Use this procedure to manually add, edit, or delete chat node aliases. To manually manage chat node aliases, you must turn off the default setting, which uses system-generated aliases. If you turn off a system-generated alias, the existing alias (`conference-x-clusterid.domain`) reverts to a standard, editable alias listed under Conference Server Aliases. This maintains the old alias and the chat room addresses that are associated with that alias.

You can manually assign multiple aliases to chat nodes. Even if a system-generated alias already exists for a chat node, you can associate additional aliases to the node manually.

For manually-managed aliases, it is the responsibility of the administrator to manually update the alias list if the Cluster ID or domain changes. System-generated aliases will incorporate the changed values automatically.

Note Although it is not mandatory, we recommend that you always include the domain when you assign a new chat node alias to a node. Use this convention for additional aliases, newalias.domain. Choose **Cisco Unified CM IM and Presence Administration** > **Presence Settings** > **Advanced Settings** to see the domain.

Before you begin

Assign Mode for Managing Chat Aliases , on page 269

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **Messaging** > **Group Chat Server Alias Mapping**.

Step 2 Click **Find**.

The Group Chat Server Alias window displays the existing node aliases.

Step 3 To add a new alias:

a) Click **Add New**.
b) In the **Group Chat Server Alias** field, enter a new alias.
c) From the **Server Name** drop-down list box, select the server to which you want to assign the alias.
d) Click **Save**.

Step 4 To edit an existing alias:

a) Select the alias.
b) Enter your updates and click **Save**.

Step 5 To delete an alias, select the alias and click **Delete Selected**.

What to do next

- Turn on the Cisco XCP Text Conference Manager.

Chat Node Alias Troubleshooting Tips

- Every chat node alias must be unique. The system will prevent you from creating duplicate chat node aliases across the cluster.
- A chat node alias name cannot match the IM and Presence domain name.
- Delete old aliases only if you no longer need to maintain the address of chat rooms via the old alias.
- If you are federating with external domains, you may want to inform federated parties that the aliases have changed and new aliases are available. To advertise all aliases externally, configure DNS and publish the aliases as DNS records.
- If you update any of the chat node alias configuration, restart the Cisco XCP Text Conference Manager.

Clean External Database for Persistent Chat

Configure jobs that monitor the external database and delete expired records. This will ensure that there is always enough disk space for new records.

To clean database tables for Persistent Chat, make sure to select the **Text Conference (TC)** feature under **Feature Tables**.

Procedure

Step 1 Log into Cisco Unified CM IM and Presence Administration on the database publisher node.

Step 2 Choose **Messaging** > **External Server Setup** > **External DataBase Jobs**.

Step 3 Click **Clear External DB**.

Step 4 Do one of the following:

- For manual cleanup of an external database that connects to the publisher node, select **SameCup Node**.
- For manual cleanup of an external database that connects to a subscriber node, select **Other CupNode** and then select the external database details.
- If you are configuring the system to monitor and clean the external database automatically, check the **Automatic Clean-up** radio button.

Note We recommend that you run a manual cleanup prior to setting up the automatic cleanup.

Step 5 Set the **Number of Days** that you want to go back for file deletion. For example, if you enter 90, the system deletes records that are older than 90 days.

Step 6 Click **Update Schema** to create the Indexes and stored procedures for the database.

Note You need to update the schema only the first time that you run the job.

Step 7 Set the **Number of Days** that you want to go back for file deletion. For example, if you enter **90**, the system deletes records that are older than 90 days.

Step 8 In the **Feature Tables** section, select each feature for which you want to clean records:

- **Text Conference (TC)**—Select this option to clean database tables for the Persistent Chat feature.
- **Message Archiver (MA)**—Select this option to clean database tables for the Message Archiver feature.
- **Managed File Transfer (MFT)**—Select this option to clean database tables for the Managed File Transfer feature

Step 9 Click **Submit Clean-up Job**.

Note If you have the **Automatic** option enabled, and you want to disable it, click the **Disable Automatic Clean-up Job** button.

Manage Chat Interactions

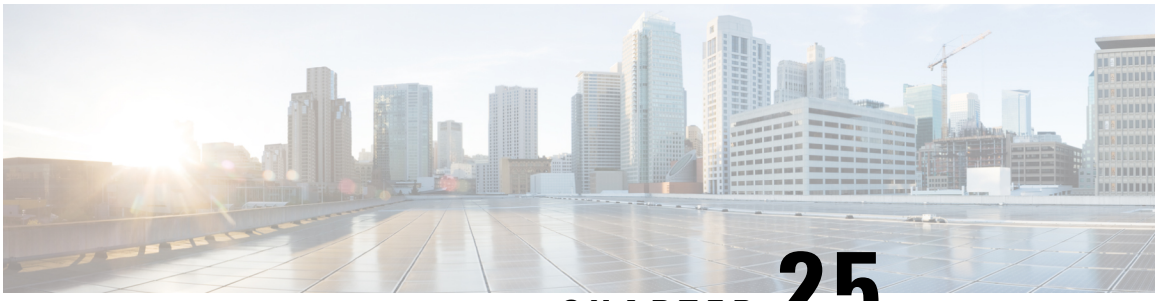
Changing chat node aliases can make the chat rooms in the database unaddressable and prevent your users from finding existing chat rooms.

Note these results before you change the constituent parts of aliases or other node dependencies:

- Cluster ID - This value is part of the fully qualified cluster name (FQDN). Changing the Cluster ID (choose System > Presence Topology: Settings) causes the FQDN to incorporate the new value and the system-managed alias to automatically change across the cluster. For manually-managed aliases, it is the responsibility of the Administrator to manually update the alias list if the Cluster ID changes.
- Domain - This value is part of the FQDN. Changing the Domain (choose Presence > Presence Settings) causes the FQDN to incorporate the new value and the system-managed alias to automatically change across the cluster. For manually-managed aliases, it is the responsibility of the Administrator to manually update the alias list if the Domain changes.
- Connection between the chat node and external database - The chat node will not start if persistent chat is enabled and you do not maintain the correct connection with the external database.
- Deletion of a chat node — If you delete a node associated with an existing alias from the Presence Topology, chat rooms created using the old alias may not be addressable unless you take further action.

We recommend that you do not change existing aliases without considering the wider implications of your changes, namely:

- Make sure that you maintain the address of old chat nodes in the database so that users can locate existing chat rooms via the old alias, if required.
- If there is federation with external domains, you may need to publish the aliases in DNS to inform theusers 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.



CHAPTER 25

Managed File Transfer Administration

Managed File Transfer Administration Overview

As the IM and Presence Service administrator , you are responsible for managing file storage and disk usage for the Managed File Transfer feature. Use this chapter to monitor the levels of file storage and disk usage and to set counters and alerts to let you know when the levels exceed your defined thresholds.

Managing External File Server and Database Server

When managing external database size, you can combine queries with shell scripting so that files get purged from the database automatically, according to your specifications. To create your queries use file transfer metadata. This includes transfer type, file type, timestamp, absolute path on the file server to the file, and other information.

When choosing how to handle file transfers within IM and group chat, consider that one-to-one IM and group chat are probably transient so transferred files may be deleted promptly. However, keep in mind that:

- IMs delivered to offline users may trigger a delayed request for a file.
- Persistent chat transfers may need to be longer lived.

Note

- Do not purge files that were created during the current UTC hour.
- After the file server is assigned, you can change the name of the file server configuration, but not the file server itself.
- If managed file transfer is configured and you change settings, restarting the Cisco XCP Router service restarts the managed file transfer feature.
- If you change 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 the database, file server, or some other internal failure. The Real-Time Monitoring Tool also generates an alarm when there is a database or file server failure. This alarm is independent of whether a file transfer is occurring.

Managed File Transfer Administration Prerequisites

Configure the Managed File Transfer feature.

Managed File Transfer Administration Task Flow

Procedure

	Command or Action	Purpose
Step 1	AFT_LOG Table Example Query and Output , on page 275	The following procedure provides an example of a query that you can run on the `AFT_LOG` table and how to use the output to purge unwanted files from the file server.
Step 2	Set Service Parameter Thresholds, on page 276	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.
Step 3	Configure XCP File Transfer Manager Alarms, on page 277	Configure alarms for Managed File Transfer to let you know when defined thresholds have been reached.
Step 4	Clean External Database for Managed File Transfer, on page 279	Optional. Use the External Database Cleanup Utility to configure jobs that monitor the external database and delete expired records. This will ensure that there is always enough disk space for new records.

AFT_LOG Table Example Query and Output

The following procedure provides an example of a query that you can run on the `AFT_LOG` table and how to use the output to purge unwanted files from the file server.

This query returns records for every uploaded file after the specified date.

Note For sample SQL commands, see External Database Disk Usage, on page 275.

Procedure

Step 1 In the External Database, enter the following command:

```
SELECT file_path
FROM aft_log
WHERE method='Post' AND timestampvalue > '2014-12-18 11:58:39';
```

The command generates the following output:

```
/opt/mftFileStore/node_1/files/im/20140811/15/file_name1
/opt/mftFileStore/node_1/files/im/20140811/15/file_name2
/opt/mftFileStore/node_1/files/im/20140811/15/file_name3
/opt/mftFileStore/node_1/files/im/20140811/15/file_name4
...
/opt/mftFileStore/node_1/files/im/20140811/15/file_name99
/opt/mftFileStore/node_1/files/im/20140811/15/file_name100
```

Step 2 Write a script that uses the `rm` command and this output to purge the above files from the external file server. For sample SQL queries, see *Database Setup for IM and Presence Service on Cisco Unified Communications Manager*.

Note Files that have not been purged from the external file server can still be accessed or downloaded even if records relating to those files have been purged from the external database.

What to do next

Set Service Parameter Thresholds, on page 276

External Database Disk Usage

You must ensure that the disks or tablespaces do not become full, otherwise the managed file transfer feature may stop working. Following are sample SQL commands that you can use to purge records from the external database. For additional queries, see the *Database Setup for IM and Presence Service on Cisco Unified Communications Manager*.

Note Files that have not been purged from the external file server can still be accessed or downloaded even if records relating to those files have been purged from the external database.

Action	Sample Command

Remove all records of files that were uploaded.	`DELETE`
	`FROM aft_log`
	`WHERE method = 'Post';`

Remove records of all files that were downloaded by a specific user.	`DELETE`
	`FROM aft_log`
	`WHERE jid LIKE '<userid>@<domain>%' AND method = 'Get';`

Remove records of all files that were uploaded after a specific time.	`DELETE`
	`FROM aft_log`
	`WHERE method = 'Post' AND timestampvalue > '2014-12-18 11:58:39';`

In addition, there are counters and alarms that can help you manage database disk usage. For details, see Alarms and Counters for Managed File Transfer, on page 277.

Set Service Parameter Thresholds

Configure the Managed File Transfer service parameters to define the threshold at which an RTMT alarm is generated for the external file server disk space.

Procedure

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

Step 2 Choose the **Cisco XCP File Transfer Manager** service for the node.

Step 3 Enter values for the following service parameters.

- **External File Server Available Space Lower Threshold**— If the percentage of available space on the external file server partition is at or below this value, the XcpMFTExtFsFreeSpaceWarn alarm is raised. The default value is 10%.
- **External File Server Available Space Upper Threshold**— If the percentage of available space on the external file server partition reaches or exceeds this value, the XcpMFTExtFsFreeSpaceWarn alarm is cleared. The default value is 15%.

Note Do not configure the lower threshold value to be greater than the upper threshold value. Otherwise the Cisco XCP File Transfer Manager service will not start after you restart the Cisco XCP Router service.

Step 4 Click **Save**.

Step 5 Restart the Cisco XCP Router service:

a) From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**.
b) From the **Server** drop-down select the IM and Presence publisher and click **Go**.
c) Under **IM and Presence Services**, select **Cisco XCP Router**, and click **Restart**.

What to do next

Configure XCP File Transfer Manager Alarms, on page 277

Configure XCP File Transfer Manager Alarms

Configure alarms for Managed File Transfer to let you know when defined thresholds have been reached.

Procedure

Step 1 Sign in to **Cisco Unified IM and Presence Serviceability**.

Step 2 Choose **Alarm** > **Configuration**.

Step 3 From the **Server** drop-down, choose the server (node), and click **Go**.

Step 4 From the **Service Group** drop-down list, choose **IM and Presence Services** and click **Go**.

Step 5 From the **Service** drop-down list, choose **Cisco XCP File Transfer Manager (Active)** and click **Go**.

Step 6 Configure the preferred alarm settings. For help with the fields and tehhir settings, refer to the online help.

Step 7 Click **Save**.

What to do next

For more information on the available alarms and counters, see Alarms and Counters for Managed File Transfer, on page 277

Alarms and Counters for Managed File Transfer

With Managed File Transfers, the transferred files get delivered to users only after they are successfully archived to the external file server, and after the file metadata is logged to the external database. If an IM and Presence Service node loses its connection to the external file server or external database, IM and Presence Service does not deliver the file to the recipient.

Alarms for Managed File Transfer

To ensure that you are notified if a connection is lost, verify that the following alarms are properly configured in the Real-Time Monitoring Tool.

Note Any files that were uploaded before the connection to the external file server was lost and which were in the process of being downloaded to the recipient, fail to be downloaded. However, there is a record of the failed transfer in the external database. To identify these files, the external database fields file_size and bytes_transferred do not match.

Table 31: Alarms for Managed File Transfers

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.
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.

Counters for Managed File Transfer

To help you administer managed file transfer, you can monitor the following counters via the Real-Time Monitoring Tool. These counters are saved in the Cisco XCP MFT Counters folder.

Table 32: Counters for Managed File Transfers

Counter	Description
MFTBytesDownloadedLastTimeslice	This counter represents the number of bytes downloaded during the last reporting interval (typically 60 seconds).

Counter	Description
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).

Clean External Database for Managed File Transfer

Configure jobs that monitor the external database and delete expired records. This will ensure that there is always enough disk space for new records.

To clean database tables for Managed File Transfer, make sure to select the **Managed File Transfer (MFT)** feature under **Feature Tables**.

Procedure

Step 1 Log into Cisco Unified CM IM and Presence Administration on the database publisher node.

Step 2 Choose **Messaging** > **External Server Setup** > **External DataBase Jobs**.

Step 3 Click **Clear External DB**.

Step 4 Do one of the following:

- For manual cleanup of an external database that connects to the publisher node, select **SameCup Node**.
- For manual cleanup of an external database that connects to a subscriber node, select **Other CupNode** and then select the external database details.
- If you are configuring the system to monitor and clean the external database automatically, check the **Automatic Clean-up** radio button.

Note We recommend that you run a manual cleanup prior to setting up the automatic cleanup.

Step 5 Set the **Number of Days** that you want to go back for file deletion. For example, if you enter 90, the system deletes records that are older than 90 days.

Step 6 Click **Update Schema** to create the Indexes and stored procedures for the database.

Note You need to update the schema only the first time that you run the job.

Step 7 Set the **Number of Days** that you want to go back for file deletion. For example, if you enter **90**, the system deletes records that are older than 90 days.

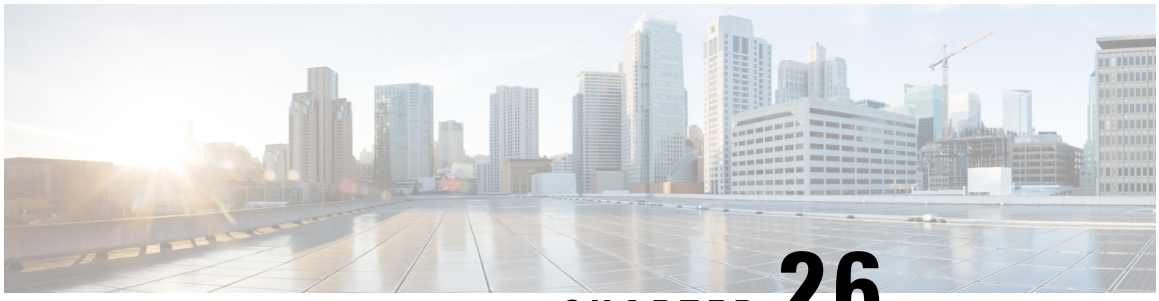
Step 8 In the **Feature Tables** section, select each feature for which you want to clean records:

- **Text Conference (TC)**—Select this option to clean database tables for the Persistent Chat feature.
- **Message Archiver (MA)**—Select this option to clean database tables for the Message Archiver feature.

- **Managed File Transfer (MFT)**—Select this option to clean database tables for the Managed File Transfer feature

Step 9 Click **Submit Clean-up Job**.

Note If you have the **Automatic** option enabled, and you want to disable it, click the **Disable Automatic Clean-up Job** button.



CHAPTER 26

Manage End Users

Manage End Users Overview

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

As part of your administrative tasks for managing end users, you may have to manage the following tasks:

- Configure a default policy for authorizing presence requests
- Configure a scheduled system check for duplicate or invalid user IDs and directory URIs
- Fix user ID and directory URI issues as they arise

For information on how to import and set up end users, see the "Configure End Users" section of the *System Configuration Guide for Cisco Unified Communications Manager*.

For information on completing bulk user contact list imports and exports, see Bulk Administration of Contact Lists, on page 365.

Presence Authorization Overview

You must assign a system authorization policy for Presence Subscription requests. The Presence Authorization Policy determines, at a system level, whether end users on the system can view other end users' presence status without requiring the authorization of the end user whose presence is requested. This setting is configured via the **Allow users to view the availability of other users without being prompted for approval** check box in the **Presence Settings** configuration window. the available settings depends partially on which protocol is being deployed:

- For SIP-based clients, you must configure the IM and Presence Service to authorize automatically all presence subscription requests or Presence will not function correctly (this is the default setting). When this option is configured, the IM and Presence Service authorizes all requests automatically with one exception: if the user whose presence is being requested has a blocked list configured in their Cisco Jabber client that includes the user making the request. In this case, the user will be prompted to approve the Presence request.

- For XMPP-based clients, you can configure whether or not you want the IM and Presence Service to prompt users to authorize presence requests from other users, or whether those presence requests should be authorized automatically.

Note The authorization system settings can be overridden by the User Policy configuration that end users can configure within their Cisco Jabber clients

User Policy Settings in Jabber

When authorizing a presence request, the IM and Presence Service also refers to the user policy that users configure within their Cisco Jabber clients. End users can add other users to a blocked list, which prevents those other users from viewing presence status without authorization, or they can add those users to an allowed list, which authorizes those users to view their presence status. These settings override the system default settings:

End users can configure the following within their Cisco Jabber clients:

- Blocked list— Users can add other users (both local and external users) to a blocked list. If any users of the blocked users view that user's presence, they will always see the availability status of the user as unavailable regardless of the true status of the user. Users can also block a whole federated domain.
- Allowed list— Users can allow other local and external users to always be able to view their availability. The user can also allow a whole external (federated) domain.
- Default policy—The default policy settings for that user. The user can set the policy to block all users, or allow all users.

Validating User IDs and Directory URIs

For single cluster deployments, duplicate user IDs and directory URIs are not an issue as it is not possible to assign duplicates within the same cluster. However, with intercluster deployments, you can unintentionally assign the same user ID or directory URI value to different users on different clusters.

The IM and Presence Service provides the following validation tools to check for duplicate user IDs and duplicate directory URIs:

- Cisco IM and Presence Data Monitor service—You can configure ongoing system checks with this service. The Cisco IM and Presence Data Monitor service checks the active directory entries for duplicate user IDs and duplicate, or empty, directory URIs for all IM and Presence Service intercluster nodes. Administrators are notified via an alarm or alert. You can use the Cisco Unified Real-Time Monitoring Tool to monitor alarms and to set up email alerts for Duplicate UserID and DuplicateDirectoryURI errors..
- System Troubleshooter—Use the System Troubleshooter if you want to run an ad hoc check the system for errors, including duplicate directory URIs and user IDs. The Troubleshooter provides details for up to 10 users only. The System Troubleshooter can be accessed from the Cisco Unified CM IM and Presence Administration interface (**Diagnostics** > **System Troubleshooter**).
- Command Line Interface—To obtain a complete and detailed report of duplicate URIs and User IDs, run the `utils users validate all` CLI command.

Manage End Users Task Flow

Procedure

	Command or Action	Purpose
Step 1	Assign a Presence Authorization Policy, on page 283	Assign a system authorization policy for Presence Subscription requests.
Step 2	Configure Data Monitor Checks for User Data, on page 284	Configure the Cisco IM and Presence Data Monitor service to run scheduled checks for duplicate directory URIs and user IDs. A system alarm or alert is raised when an issue is found.
Step 3	Validate User Data via the System Troubleshooter, on page 286	Run the system troubleshooter if you want to run an ad hoc check for system issues, including duplicate directory URIs and user IDs.
Step 4	Validate User IDs and Directory URIs via CLI, on page 287	Run a CLI command to get a detailed report of duplicate directory URIs and user IDs.
Step 5	View Presence Settings for User, on page 290	If you want to view presence settings for an IM and Presence-enabled end user, you can use the Presence Viewer to view those settings.

Assign a Presence Authorization Policy

Assign a system authorization policy for Presence Subscription requests.

Note On their Cisco Jabber client, end users can configure whether they want to allow other users to be able to view their presence status. This user policy overrides the system authorization settings.

Procedure

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

Step 2 Check or uncheck the **Allow users to view the availability of other users without being prompted for approval** check box.

- Checked—IM and Presence automatically authorizes all Presence subscription requests received within the local enterprise.
- Unchecked—IM and Presence refers all presence subscription requests to the client whose presence is requested. The user can accept or reject the request.

Note If you are deploying SIP-based clients, you must check this check box.If leave the check box unchecked, your deployment supports XMPP clients only.

Step 3 Click **Save**.

Step 4 Restart the Cisco XCP Router service.

What to do next

Proceed to configure the SIP publish trunk on IM and Presence Service.

Configure Data Monitor Checks for User Data

Complete these tasks to configure the Cisco IM and Presence Data Monitor to validate directory URIs and user IDs at scheduled intervals. Any errors are communicated via an alarm or alert with the Cisco Unified Real-Time Monitoring Tool.

Note Duplicate directory URI and duplicate user ID errors are only an issue for intercluster deployments.

Procedure

	Command or Action	Purpose
Step 1	Set Schedule for User ID and Directory URI Validation Check, on page 284	Configure the scheduled interval for the Cisco IM and Presence Data Monitor check. The service checks the active directory entries for errors, including duplicate directory URIs and user IDs.
Step 2	Set up Email Server for Email Alerts, on page 285	Optional. If you want to receive email alerts whenever the Data Monitor service finds a duplicate directory URI or user ID, you must set up an email server with the Real-Time Monitoring Tool.
Step 3	Enable Email Alerts, on page 285	Optional. Complete this procedure to enable email alerts for the DuplicateDirectoryURI and DuplicateUserid alarm. When the Cisco IM and Presence Data Monitor service returns one of these alarms, an email will be sent to the administrator.

Set Schedule for User ID and Directory URI Validation Check

Set the scheduled interval for the Cisco IM and Presence Data Monitor service. This service checks the system at scheduled intervals for data errors, including duplicate directory URIs and user IDs. The service raises an alarm or alert that can be viewed via the Real-Time Monitoring Tool whenever an error is found.

Before you begin

The Cisco IM and Presence Data Monitor network service must be running. By default, the service is running. You can confirm that the service is running from the **Control Center - Network Services** window in the Cisco Unified IM and Presence Serviceability interface.

Procedure

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

Step 2 In the **Service** drop-down, choose **Cisco IM and Presence Data Monitor**.

Step 3 In the **User Check Interval** field, enter the time interval, in minutes. You can enter an integer from 5 through 1440 (minutes). The default value is 30 minutes.

Step 4 Click **Save**.

What to do next

Optional. If you want to set up email alerting whenever a DuplicateDirectoryURI or DuplicateUserid alarm is raised, Set up Email Server for Email Alerts, on page 285

Set up Email Server for Email Alerts

It may help to have an administrator receive an email alert whenever the Data Monitor validation check finds duplicate directory URI and user ID errors. If so, use this optional procedure to set up an email server for email alerts.

Procedure

Step 1 In the Real-Time Monitoring Tool's System window, click **Alert Central**.

Step 2 Choose **System** > **Tools** > **Alert** > **Config Email Server**.

Step 3 In the **Mail Server Configuration** popup, enter the details for the mail server.

Step 4 Click **OK**.

What to do next

Enable Email Alerts, on page 285

Enable Email Alerts

Use this procedure to set up the Real-Time Monitoring Tool to email an administrator whenever a DuplicateUserID or DuplicateDirectoryURI system alert is raised.

Before you begin

Set up Email Server for Email Alerts, on page 285

Procedure

Step 1 In the Real-Time Monitoring Tool **System** area, click **Alert Central**.

Step 2 Click the **IM and Presence** tab.

Step 3 Click on the alert for which you want to add an email alert. For example, the **DuplicateDirecytoryURI** or **DuplicateUserid** system alerts.

Step 4 Choose **Tools** > **Alert** > **Config Alert Action**.

Step 5 In the **Alert Action** popup, select **Default** and click **Edit**.

Step 6 In the **Alert Action** popup, **Add** a recipient.

Step 7 In the popup window, enter the address where you want to send email alerts, and click **OK** .

Step 8 In the **Alert Action** popup, make sure that the address appears under **Recipients** and that the **Enable** check box is checked.

Step 9 Click **OK**.

Step 10 Repeat this procedure for each system alert for which you want to enable email alerting.

Validate User Data via the System Troubleshooter

Use the System Troubleshooter in the Cisco Unified CM IM and Presence Administration GUI to check your deployment for duplicate user IDs and duplicate or invalid directory URIs. The troubleshooter checks all nodes and clusters in the deployment.

Procedure

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

Step 2 Monitor the status of user IDs and Directory URIs in the **User Troubleshooter** area. The **Problem** column is populated if the system check detects any issues.

- Verify that all users have a unique User ID configured.
- Verify that all users have a Directory URI configured.
- Verify that all users have a unique Directory URI configured.
- Verify that all users have a valid Directory URI configured.
- Verify that all users have a unique Mail ID configured.

Note Duplicate mail IDs impact both Email Address for Federation and Exchange Calendar integration features.

Step 3 If an issue appears, click the **fix** link in the **Solution** column to be redirected to the **End User Configuration** window in Cisco Unified Communications Manager where you can reconfigure user settings.

Note The user ID and directory URI fields in the user profile may be mapped to the LDAP Directory. In that case, apply the fix in the LDAP Directory server.

What to do next

If any issues arise, edit the user settings in the **End User Configuration** window of Cisco Unified Communications Manager. If the user is synchronized from an LDAP directory, you will need to make your edits in the LDAP directory.

If you need a more detailed report, Validate User IDs and Directory URIs via CLI, on page 287.

Validate User IDs and Directory URIs via CLI

Use the Command Line Interface to run a detailed check of your deployment for duplicate user IDs and duplicate directory URIs.

Procedure

Step 1 Login to the Command Line Interface.

Step 2 Run one of the following commands:.

- `utils users validate all`— Checks the system for both duplicate user IDs and duplicate directory URIs.
- `utils users validate userid`— Checks the system for duplicate user IDs.
- `utils users validate uri`— Checks the system for duplicate directory URIs.

The CLI returns a report of duplicate directory URIs and/or user IDs. For a sample report, see User ID and Directory URI CLI Validation Examples, on page 287

What to do next

If any issues arise, edit the user settings in the End User Configuration window of Cisco Unified Communications Manager. If the user is synchronized from an LDAP directory, you will need to make your edits in the LDAP directory.

User ID and Directory URI CLI Validation Examples

The CLI command to validate IM and Presence Service users to identify users that have duplicate user IDs and duplicate or invalid Directory URIs is utils users validate { all | userid | uri }.

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
```

User ID and Directory URI Errors

The Cisco IM and Presence Data Monitor service checks the Active directory entries for duplicate user IDs and empty or duplicate directory URIs for all IM and Presence Service intercluster nodes. Duplicate user IDs or directory URIs are not possible within a cluster; however, it is possible to unintentionally assign the same user ID or directory URI value to users on different clusters in an intercluster deployment.

The following list displays possible errors that may be found. You can view these errors in the Real-Time Monitoring Tool, which will raise an alarm or alert for each of these:

DuplicateDirectoryURI

This alert indicates that there are multiple users within the intercluster deployment that are assigned the same directory URI value when the Directory URI IM Address scheme is configured.

DuplicateDirectoryURIWarning

This warning indicates that there are multiple users within the intercluster deployment that are assigned the same directory URI value when the `userID@Default_Domain` IM Address scheme is configured.

DuplicateUserid

This alert indicates there are duplicate user IDs assigned to one or more users on different clusters within the intercluster deployment.

InvalidDirectoryURI

This alert indicates that one or more users within the intercluster deployment are assigned an empty or invalid directory URI value when the Directory URI IM Address scheme is configured.

InvalidDirectoryURIWarning

This warning indicates that one or more users within the intercluster deployment are assigned an empty or invalid directory URI value when the `userID@Default_Domain` IM Address scheme is configured.

To gather specific information about which users have these alarm conditions, use the Command Line Interface for a complete listing. System alarms do not provide details about the affected users and the System Troubleshooter displays details for only up to 10 users. Use the Command Line Interface and validate users to gather information about which users caused an alarm. For more information, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Caution Take the appropriate action to fix duplicate user IDs and duplicate or invalid Directory URIs to avoid communications disruptions for the affected users. To modify user contact information, see the *Cisco Unified Communications Manager Administration Guide*.

Errors and Suggested Action

The following table describes 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 33: User ID and Directory URI Error Conditions and Suggested Action

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:** • `DuplicateDirectoryURI` • `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.

View Presence Settings for User

Use the Presence Viewer to get a summarized view of presence settings for an IM and Presence-enabled end user. The Presence Viewer provides information such as Presence server assignments, contacts and watchers.

Before you begin

The **Cisco AXL Web Service**, **Cisco SIP Proxy** service, and **Cisco Presence Engine** service must all be running in Cisco Unified Serviceability.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End Users**.

Step 2 Click **Find** and select the end user for whom you want to view presence settings.

Step 3 Under **Service Settings**, click **Presence Viewer for User** to open the Presence Viewer. Refer to the following table if you want to customize the view.

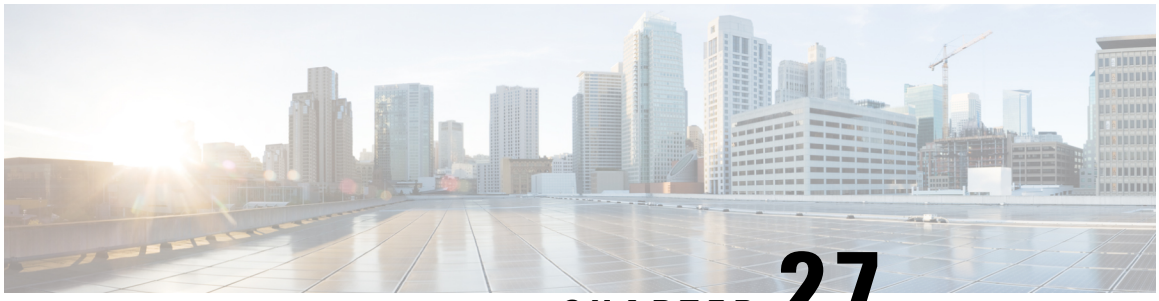
Table 34: End User Presence Viewer Fields

Presence Setting	Description
User Status	Identifies the availability state of the user, including: • Available • Away • Do Not Disturb • Unavailable • Custom

Presence Setting	Description
User ID	Identifies the selected user ID. A user photo is displayed if one is available for that user. You can click **Submit** to choose a different User ID.
View From Perspective of	Specifies a user to see the availability status from the perspective of the user. This allows you to determine how the availability status of a specified user appears to another user, known as a watcher. This functionality is useful in debugging scenarios, for example, where a user has configured privacy policies. A maximum of 128 characters is allowed.
Contacts	Displays the number of contacts in the contact list for this user. Click the arrow beside the Contacts heading in the Contacts and Watchers list area to view the availability status of a specific user contact. Click the arrow beside the group name to expand the list of contacts within that group. Contacts that are not part of a group (groupless contacts) display below the contact group list. A contact may belong to multiple groups, but will only count once against the contact list size for that user. A warning message appears if the maximum number of contacts configured for end users is exceeded. For more information about IM and Presence Service configuration and the maximum contacts setting, see the *IM and Presence Administration Online Help*.
Watchers	Displays a list of users, known as watchers, who have subscribed to see the availability status of this user in their contact list. Click the arrow beside the Watchers heading in the Contacts and Watchers list area to view the availability status of a specific watcher. Click the arrow beside the group name to expand the list of watchers within that group. A watcher may belong to multiple groups but will only count once against the watcher list size for that user. A warning message appears if the maximum number of watchers configured for end users is exceeded. For more information about IM and Presence Service configuration and the maximum watchers setting, see the *IM and Presence Administration Online Help*.
Presence Server Assignment	Identifies the IM and Presence Service server to which the user is assigned. Hyperlinks allow you to go directly to the server configuration page for details.
Enable accessible presence icons	Select this check box to enable presence accessibility icons for this end user.
Submit	Select to run the Presence Viewer. The user must be assigned to an IM and Presence node for valid presence information to be available. The AXL, Presence Engine and Proxy Service must all be running on the IM and Presence server for this action to be functional.

Presence Authorization Interactions and Restrictions

Feature	Restriction
Turning off automatic presence authorization	If you turn off automatic authorization of presence requests, IM and Presence Service still automatically authorizes subscription requests for users that are on the contact list of the other user. This applies to users in the same domain, and users in different domains (federated users). For example: • User A wishes to subscribe the view the availability status of User B. Automatic authorization is off on IM and Presence Service, and User B is not in the Allowed or Blocked list for the User A • IM and Presence Service sends the presence subscription request to the client application of User B, and the client application prompts User B to accept or reject the subscription. • User B accepts the presence subscription request, and User B is added to the contact list of User A. • User A is then automatically added to the contact list for User B without being prompted to authorize the presence subscription. This occurs even if the policy for User B blocks the external domain, or User B has "ask me" configured in the user profile.
Interdomain Federation—Presence requests received from the external domain	IM and Presence will rely solely on the user policy settings of the user whose presence status is requested. If the user has selected "ask me" in their user policy, and has not added an Allowed or Blocked list for the external contact or domain, then IM and Presence sends the Presence request to the end user to authorize.



CHAPTER 27

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 101 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 35: 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 157.

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 293 before you migrate users.

Table 36: Migration to Central Cluster Task Flow

	IM and Presence Central Cluster	Migrating Cluster	Purpose
Step 1		Export Contact Lists from Migrating Cluster, on page 296	Export user contact lists in the migrating cluster to a csv file.
Step 2		Disable High Availability in Migrating Cluster, on page 297	Disable High Availability for all Presence Redundancy Groups (subclusters) in the migrating cluster.
Step 3		Configure UC Service for IM and Presence, on page 298	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 298	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 299	Use Bulk Administration in the migrating cluster to disable IM and Presence for users.
Step 6		Enable OAuth Authentication for Central Cluster, on page 300	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 300		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 301		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 301		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 302		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 303		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 304		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 305		Start the Cisco Intercluster Sync Agent in the central cluster.
Step 14	Enable High Availability in Central Cluster, on page 306		In the central cluster, enable High Availability in all Presence Redundancy Groups.
Step 15	Delete Remaining Peers for Migrating Cluster, on page 306		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 297

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.

Note The **Presence Redundancy Group Details** page shows all the active JSM sessions, even when the high availability is disabled in the 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 298

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 298

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 299

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 Mobile and Remote Access 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 300

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.

Note The **Presence Redundancy Group Details** page shows all the active JSM sessions, even when the high availability is disabled in the cluster.

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 301

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 302

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 110.

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 303

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 304

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 305

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 306

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**:

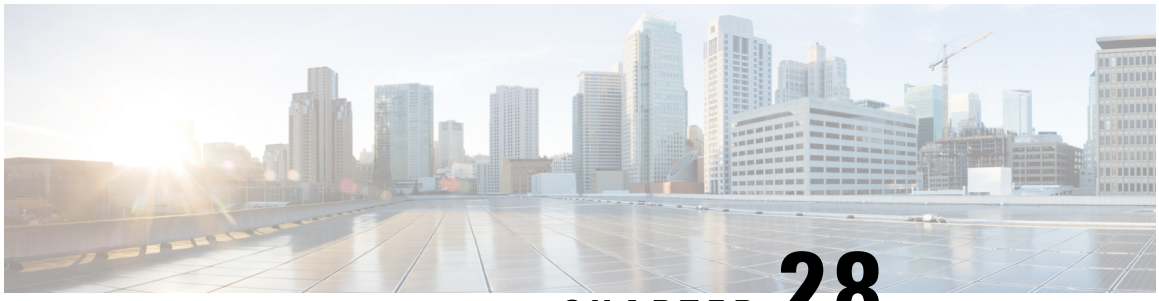
a) Log in to Unified IM and Presence Serviceability and choose **Tools** > **Control Center - Network Services**.

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 28

Migrate Users

Migrate Users Overview

This section describes how to migrate users between IM and Presence Service clusters.

Migrate Users Prerequisites

- Run full backups of both the current and destination cluster. For details, see Backup Task Flow, on page 339.
- Ensure that the users to be migrated are licensed for the IM and Presence Service or Cisco Jabber on their current home cluster only. If these users are licensed on any cluster other than the premigration cluster, they must be fully unlicensed before proceeding with the migration tasks.

Migrate Users Task Flow

Complete these tasks to migrate IM and Presence users to a new cluster.

Procedure

	Command or Action	Purpose
Step 1	Remove Stale Entries, on page 310	Before migrating users, remove all stale rosters, group entries and non-presence contract records.
Step 2	Start Essential Services for Migration, on page 312	Before migrating, confirm the following services are running: • Cisco AXL Web Service • Cisco Sync Agent

	Command or Action	Purpose
		• Cisco Intercluster Sync Agent
Step 3	Check for Intercluster Sync Errors, on page 312	Run the System Troubleshooter and confirm that there are no intercluster sync issues.
Step 4	Configure Standard Presence for Migration, on page 311	Before migrating users, configure these standard Presence settings.
Step 5	Export User Contact Lists, on page 313	Complete this procedure to export the contact lists of the migrating users from their current cluster.
Step 6	Complete one of these mini-task flows to move users to the new cluster: • Migrate Users via LDAP, on page 313 • Move Users to New Cluster Manually, on page 315 • Migrate Users via Bulk Administration, on page 317	Move users to the new cluster. You can use LDAP to provision users in the new cluster, move users manually, or use Bulk Administration to migrate users to the new cluster.
Step 7	Import Contact Lists on Home Cluster, on page 321	After you have migrated users to the new cluster, import the contact lists to restore contact data for the migrated users.
Step 8	Update Users in Old Cluster, on page 322	You may not want to remove users from the old cluster until after you confirm that everything is working fine in the new cluster. Use this procedure to use Bulk Administration's Update Users feature to remove IM and Presence functionality from the old cluster.

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)))
```

Configure Standard Presence for Migration

Before migrating users, configure these Presence settings.

Procedure

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

Step 2 Check the **Allow users to view the availability of other users without being prompted for approval** check box.

Step 3 For the **Maximum Contact List Size (per user)** setting, check the **No Limit** check box.

Step 4 For the **Maximum Watchers (per user)** setting, check the **No Limit** check box

Step 5 Click **Save**.

What to do next

Check for Intercluster Sync Errors, on page 312

Check for Intercluster Sync Errors

Before migrating, confirm that there are no intercluster sync errors.

Procedure

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Diagnostics** > **System Troubleshooter**.

Step 2 Confirm that there are no intercluster sync errors. If there are errors, fix them before proceeding.

What to do next

Start Essential Services for Migration, on page 312

Start Essential Services for Migration

In Cisco Unified IM and Presence Serviceability, confirm that the following essential services for the migration are running:

- Cisco AXL Web Service
- Cisco Sync Agent
- Cisco Intercluster Sync Agent

Procedure

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

Step 2 From the **Server** drop-down select your IM and Presence node and click **Go**.

Step 3 Under **Database and Admin Services**, confirm that the **Cisco AXL Web Service** is Started. If the service is not running (the default setting is not running), select the service and click **Start**.

Step 4 Choose **Tools** > **Control Center - Network Services**.

Step 5 From the **Server** drop-down select your IM and Presence node and click **Go**.

Step 6 Under **IM and Presence Services**, confirm that both the **Cisco Sync Agent** and **Cisco Intercluster Sync Agent** services are running. If they are not running, **Start** them.

What to do next

Export User Contact Lists, on page 313

Export User Contact Lists

Complete this procedure to export the contact lists of the migrating users from their current cluster.

Procedure

Step 1 Export the contact lists of the migrating users from the current home cluster.

a) In **Cisco Unified CM IM and Presence Administration**, choose **Bulk Administration** > **Contact List** > **Export**.
b) Choose **All unassigned users in the cluster** and click **Find**.
c) Review the results and use the **AND/OR** filter to filter the search results as required.
d) When the list is complete, click **Next**.
e) Choose a filename for the exported contact list data.
f) Optionally update the Job Description.
g) Click **Run Now** or schedule the job to run later.

Step 2 Monitor the status of the contact list export job.

a) In **Cisco Unified CM IM and Presence Administration**, choose **Bulk Administration** > **Job Scheduler**.
b) Click **Find** to list all BAT jobs.
c) Find your contact list export job and when it is reported as completed, choose the job.
d) Choose the CSV File Name link to view the contents of the contact list export file. A time stamp is appended to the filename.
e) From the **Job Results** section, choose the log file to see a summary of what was uploaded. The log file includes the start and end time and result summary for the job.

Step 3 Download the contact list export file and store it for use later when the user migration is complete.

a) In **Cisco Unified CM IM and Presence Administration**, choose **Bulk Administration** > **Upload/Download Files**.
b) Click **Find**.
c) Choose the contact list export file and click **Download Selected**.
d) Save the CSV file locally for upload later in the procedure.

What to do next

Go to one of the following task flows to assign users in the new cluster:

- Migrate Users via LDAP, on page 313
- Move Users to New Cluster Manually, on page 315

Migrate Users via LDAP

Complete these tasks if your users are synced with an LDAP Directory and you want to migrate to a new cluster.

Note You must add your LDAP Directory configuration into the new cluster. This includes any service profiles, user profiles, and feature group templates. Make sure that your feature group template configuration has the **Enable Users for Unified CM IM and Presence** check box checked.

Procedure

	Command or Action	Purpose
Step 1	Update External LDAP Directory, on page 314	You may need to update your external LDAP directory if your deployment uses a separate LDAP structure for each cluster and where users are synchronized only to their home cluster.
Step 2	Configure LDAP in New Cluster, on page 315	If LDAP is enabled on Cisco Unified Communications Manager, import users to your new cluster by synchronizing your new cluster with the updated LDAP directory.

What to do next

Import Contact Lists on Home Cluster, on page 321

Update External LDAP Directory

You may need to update your external LDAP directory if your deployment uses a separate LDAP structure for each cluster and where users are synchronized only to their home cluster.

Note You do not need to move the users if the deployment uses a flat LDAP structure, that is, all users are synchronized to all Cisco Unified Communications Manager and IM and Presence Service clusters where users are licensed to only one cluster.

Note Depending on how you have your LDAP Directory sync configured in the old and new cluster, moving your users within the external LDAP Directory may automatically migrate those users to the new IM and Presence Service cluster when the next sync occurs.

Procedure

Step 1 Update users in your external LDAP directory.

Step 2 After you move the users, delete the LDAP entries from the old LDAP cluster.

What to do next

Configure LDAP in New Cluster, on page 315

Configure LDAP in New Cluster

Before you begin

Provision the LDAP directory in your new cluster. If your LDAP directory sync includes universal line and device templates, and feature group templates, you must configure these templates in your new cluster. Make sure that your feature group template has the following options checked:

- Home Cluster
- Enable Users for Unified CM IM and Presence

For details on how to configure an LDAP directory sync, refer to the "Configure End Users" section of the *System Configuration Guide for Cisco Unified Communications Manager*.

Procedure

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

Step 2 Click **Find** and select the LDAP Directory that you've configured

Step 3 Click **Perform Full Sync Now**.

What to do next

Import Contact Lists on Home Cluster, on page 321

Move Users to New Cluster Manually

Complete these tasks to move a user to the new cluster manually.

Note If you have a large number of users, you may want to use the Bulk Administration Tool in Cisco Unified Communications Manager to update a large number of users via a csv file. For details, see the *Bulk Administration Guide for Cisco Unified Communications Manager*.

Procedure

	Command or Action	Purpose
Step 1	Disable IM and Presence For User Manually, on page 316	Disable a migrating user for IM and Presence Service and Cisco Jabber on their current home cluster.
Step 2	Import Users Manually, on page 316	If LDAP synchronization is not configured in the new cluster, provision users manually to

	Command or Action	Purpose
		your new Cisco Unified Communications Manager cluster.
Step 3	Enable Users for IM and Presence Service on New Cluster, on page 317	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.

What to do next

Import Contact Lists on Home Cluster, on page 321

Disable IM and Presence For User Manually

The following procedure describes how to disable a migrating user for IM and Presence Service and Cisco Jabber on their current home cluster.

Note If you are migrating a large number of users at once, you may want to use the Bulk Administration Tool in Cisco Unified Communications Manager. For details, see the *Bulk Administration Guide for Cisco Unified Communications Manager*.

Before you begin

Export User Contact Lists, on page 313

Procedure

Step 1 In **Cisco Unified CM Administration**, choose **> User Management** > **End User**.

Step 2 Use the filters to find the user that you want to disable for IM and Presence Service.

Step 3 In the **End User Configuration** screen, uncheck **Enable User for Unified CM IM and Presence**.

Step 4 Click **Save**.

What to do next

Import Users Manually, on page 316

Import Users Manually

If LDAP synchronization is not configured in the new cluster, import users manually to your new Cisco Unified Communications Manager cluster.

For details, see Configure User Settings, on page 67.

What to do next

Enable Users for IM and Presence Service on New Cluster, on page 317

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 In **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 *Administration Guide for Cisco Unified Communications Manager* for more information.

What to do next

Import Contact Lists on Home Cluster, on page 321

Migrate Users via Bulk Administration

Move the users to a new cluster via the Bulk Administration Tool (for example, migrating from cluster 1 to cluster 2).

Before you begin

The **Cisco Bulk Provisioning Service** must be running in both clusters.

Note If the number of users to be moved from source to destination in IM and Presence cluster are less than 100 then, do not start or stop Cisco Intercluster Sync Agent service.

If you are moving 100 to 1,000 users from any source / destination cluster perform the below steps by stopping Intercluster Sync Agent service on both source and destination clusters.

If the number of users to be moved are more than 1000, For example, if we have to move 16K users then first move 8K users by following below steps and stop the Intercluster Sync Agent service while moving users in chunks of 1K users. Later move the next 8K in a balanced and serial sequence in chunks of 1K users.

On the IM and Presence cluster where the users are being moved from source:

Step 1 On the associated subscriber node of the IM and Presence publisher's Presence Redundancy Group (PRG) pair stop Intercluster Sync Agent service.

Step 2 On the publisher node of the publisher IM and Presence Presence Redundancy Group pair stop Intercluster Sync Agent service.

On the IM and Presence cluster where the users are being moved from destination:

Step 3 On the secondary node of the publisher Presence Redundancy Group pair stop Intercluster Sync Agent service.

Step 4 On the publisher node of the publisher Presence Redundancy Group pair stop Intercluster Sync Agent service.

Note No other cluster nodes require Intercluster Sync Agent service to be stopped.

Step 5 Peform the steps mentioned in Migrate Users via Bulk Administration.

Step 6 Start the Intercluster Sync Agent service on the IM and Presence publisher and subscriber nodes on both destination and source clusters.

Step 7 It can take up to 30 minutes for all other clusters to complete their sync with the destination cluster.

Procedure

	Command or Action	Purpose
Step 1	Export Users to CSV File, on page 318	In the original cluster (cluster 1) export the migrating users to a CSV file.
Step 2	Download CSV Export File, on page 319	Download the CSV export file.
Step 3	Upload CSV Export File to New Cluster, on page 319	Upload the CSV file to the destination cluster (cluster 2).
Step 4	Configure User Template, on page 320	In the destination cluster, configure a User Template with the user settings.
Step 5	Import Users to New Cluster, on page 320	Use the Insert Users menu in Bulk Administration to import users from the CSV file.
Step 6	Verify User Migration via Bulk Administration, on page 321	Verify the user migration via bulk administration.

Export Users to CSV File

In the original cluster, use the Bulk Administration Tool to export the users whom you want to migrate to a CSV file.

Note: After the job runs, you can go to the Job Scheduler to check the status of the job and confirm that the file was created. If you selected Run Later, you can use the Job Scheduler to set the time for the job to run.

Procedure

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

Step 2 Use the **Filter** tools to search for and select the users whom you want to migrate and click **Find**.

Step 3 Click **Next**.

Step 4 Enter a **File Name** for the file.
The tool appends the `.txt` extension to the end of your file. For example, `<csvfilename>.txt`.

Step 5 From the **File Format** drop-down, select the format of the export file.

Step 6 To run the job right away, select **Run Immediately** and click **Submit**.

What to do next

After the job runs, you can go to the **Job Scheduler** to check the status of the job and confirm that the file was created. If you selected **Run Later**, you can use the Job Scheduler to set the time for the job to run.

Once you have confirmed that the file was created, Download CSV Export File, on page 319.

Download CSV Export File

Once you have confirmed that the export file was created, download the file.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Bulk Administration** > **Upload/Download Files**.

Step 2 Click **Find**.

Step 3 Select the file that was created and click **Download Selected**.

Step 4 Download the file.

What to do next

Upload CSV Export File to New Cluster, on page 319

Upload CSV Export File to New Cluster

In the destination cluster (cluster 2), upload the csv file that you exported from cluster 1.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Bulk Administration** > **Upload/Download Files**.

Step 2 Click **Add New**.

Step 3 Click **Choose File**. Browse and select the export file from the other system.

Step 4 From the **Target** drop-down, select the Bulk Administration menu that you want to use to import the file contents. For example, **Users** or **Phones and Users**.

Step 5 From the **Transaction Type** drop-down, select the submenu that you want to use to import the file contents. For example, **Insert Users** or **Insert Phones/Users**.

Step 6 Click **Save**

What to do next

Configure User Template, on page 320

Configure User Template

In the destination cluster, configure a user template with the settings that you want to apply to imported users.

Procedure

Step 1 From Cisco Unified CM Administration choose **Bulk Administration** > **Users** > **User Templates**.

Step 2 Do either of the following:

- Click **Find** and select an existing template.
- Click **Add New** to create a new template.

Step 3 Configure the user settings that you want to apply to your imported users. For example, make sure that the following fields are checked

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

Step 4 If you want users to be enabled for calendar integration with Microsoft Outlook, check the **Include meeting information in Presence check box**.

Step 5 Configure any remaining fields.

Step 6 Click **Save**.

What to do next

Import Users to New Cluster, on page 320

Import Users to New Cluster

Use Bulk Administration's Insert Users menu to import the exported users into the new Cluster.

Procedure

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

Step 2 From **File Name**, select the file that was exported from the other system.

Step 3 From the **User Template Name**, select the user template that you just created.

Step 4 Check the **File created with Export Users** check box.

Step 5 Check **Run Immediately** and click **Submit**.

What to do next

Import Contact Lists on Home Cluster, on page 321

Verify User Migration via Bulk Administration

After migrating users via Bulk Administration and starting Cisco Intercluster Sync Agent Services on the source and destination clusters, it is necessary to verify that other clusters than source and destination clusters received notifications that user move has been occurred.

It can take up to 30 minutes for all other clusters to complete their sync with the destination cluster. While you wait, you can open a terminal session to sample (5) IMP publishers in parallel that are not part of the change (source or destination) to monitor the CiscoSyslogs.

Procedure

Step 1 Run the below command to observe if the sample IMP publisher node has already completed its sync after migrating users via Bulk Administration and starting Cisco Intercluster Sync Agent Services on the source and destination clusters. Notify the timestamp for this moment. In the following example syntax, the destination cluster name is dst-name. Replace this with your destination cluster name.

```
admin:file search activelog syslog/CiscoSyslog ".*InterClusterSyncAgentStatus:.*dst-name.*"
```

Step 2 If the time stamp in the ICSA status is not more recent than the timestamp recorded, then use the following command for up to 30 minutes for a successful sync:

```
admin:file tail activelog syslog/CiscoSyslog regexp
".*InterClusterSyncAgentStatus:.*dst-name.*"
```

If you see an ICSA failed sync status alarm on the selected sample cluster/node, wait for 5-10 minutes for a successful sync status alarm. ICSA will retry every 5 minutes. If you do not have a successful sync alarm or have consistent sync failures, please open a TAC case.

At this point you have verified the 5 remote sample clusters if the current time is 30 minutes later than timestamp recorded after migrating users via Bulk Administration and starting Cisco Intercluster Sync Agent Services on source and destination clusters. You can now proceed to the next move process or if there no other moves, you are finished.

Import Contact Lists on Home Cluster

After you have migrated users to the new cluster, import the contact lists to restore contact data for the migrated users.

Procedure

Step 1 Upload the previously exported contact list CSV file.

a) In **Cisco Unified CM IM and Presence Administration** , choose **Bulk Administration** > **Upload/Download Files**.
b) Click **Add New**.
c) Click **Browse** to locate and choose the contact list CSV file.
d) Choose **Contact Lists** as the Target.
e) Choose **Import Users' Contacts - Custom File** as the Transaction Type.
f) Optionally check **Overwrite File if it exists**.

g) Click **Save** to upload the file.
h) Click **Save** to upload the file.

Step 2 Run the import contact list job.

a) In **Cisco Unified CM IM and Presence Administration**, choose **Bulk Administration** > **Contact List** > **Update**.
b) Choose the CSV file you uploaded in Step 1.
c) Optionally update the Job Description.
d) To run the job now, click **Run Immediately**. Click **Run Later** to schedule the update for a later time.
e) Click **Submit**.

Step 3 Monitor the contact list import status

a) In **Cisco Unified CM IM and Presence Administration**, choose **Bulk Administration** > **Contact List** > **Job Scheduler**.
b) Click **Find** to list all BAT jobs.
c) Choose the job ID of the contact list import job when its status is reported as complete.
d) To view the contents of the contact list file, choose the file listed at **CSV File Name**.
e) Click the **Log File Name** link to open the log.

The begin time and end time of the job is listed and a result summary is also displayed.

Update Users in Old Cluster

You may not want to remove users from the old cluster until after you confirm that everything is working fine in the new cluster. Use this procedure to use Bulk Administration's Update Users feature to remove IM and Presence functionality from the old cluster.

Procedure

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

Step 2 Use the Filter tools to search for the migrating users. For example, you can search for all users whom meet this condition: **Has IM and Presence Enabled**.

Step 3 Click **Next**

Step 4 For each of the following two fields, check the far left box and leave the adjacent box on the right unchecked. The left box indicates that you want to update the field and the right box indicates the new setting: unchecked.

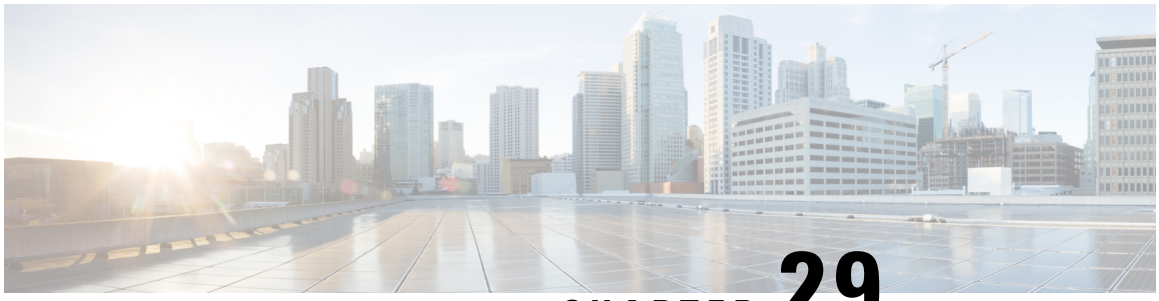
- **Home Cluster**
- **Enable User for Unified CM IM and Presence**

Step 5 Under **Job Information**, select **Run Immediately**.

Step 6 Click **Submit**.

What to do next

Once you are confident that the migration worked, and that all users are configured properly in the new cluster, you can delete migrated users in the old cluster.



CHAPTER 29

Manage Locales

Manage Locales Overview

You can configure Cisco Unified Communications Manager and IM and Presence Service to support multiple languages. There is no limit to the number of supported languages you can install.

Cisco provides locale-specific versions of the Cisco Unified Communications Manager Locale Installer and the IM and Presence Service Locale Installer on www.cisco.com. Installed by the system administrator, the locale installer allows the user to view/receive the chosen translated text or tones, if applicable, when a user works with supported interfaces.

After you upgrade Cisco Unified Communications Manager or the IM & Presence Service, you must reinstall all the locales. Install the latest version of the locales that match the major.minor version number of your Cisco Unified Communications Manager node or IM and Presence Service node.

Install locales after you have installed Cisco Unified Communications Manager on every node in the cluster and have set up the database. If you want to install specific locales on IM and Presence Service nodes, you must first install the Cisco Unified Communications Manager locale file for the same country on the Cisco Unified Communications Manager cluster.

Use the information in the following sections to install locales on Cisco Unified Communications Manager nodes and on IM and Presence Service nodes after you complete the software upgrade.

User Locales

User locale files contain language information for a specific language and country. They provide translated text and voice prompts, if available, for phone displays, user applications, and user web pages in the locale that the user chooses. These files use the following naming convention:

- cm-locale-language-country-version.cop (Cisco Unified Communications Manager)
- ps-locale-language_country-version.cop (IM and Presence Service)

If your system requires user locales only, install them after you have installed the CUCM locale.

Network Locales

Network locale files provide country-specific files for various network items, including phone tones, annunciators, and gateway tones. The combined network locale file uses the following naming convention:

- cm-locale-combinednetworklocale-version.cop (Cisco Unified Communications Manager)

Cisco may combine multiple network locales in a single locale installer.

Note Cisco Unified Communications Manager and IM and Presence Service on Cisco-approved, customer-provided servers can support multiple locales. Installing multiple locale installers ensures that the user can choose from a multitude of locales.

You can install locale files from either a local or a remote source by using the same process for installing software upgrades. You can install more than one locale file on each node in the cluster. Changes do not take effect until you reboot every node in the cluster. Cisco strongly recommends that you do not reboot the nodes until you have installed all locales on all nodes in the cluster. Minimize call-processing interruptions by rebooting the nodes after regular business hours.

Manage Locales Prerequisites

Locale Installation Considerations

- Install all of the Cisco Unified Communications Manager and IM and Presence Service cluster nodes and set up the database before you install locales.
- If you want to install specific locales on IM and Presence Service nodes, you must first install the Cisco Unified Communications Manager locale file for the same country on the Cisco Unified Communications Manager cluster.
- You can install more than one locale file on each node in the cluster. To activate the new locale, you must restart each node in the cluster after installation.
- You can install locale files from either a local or a remote source by using the same process for installing software upgrades. See the *Upgrade Guide for Cisco Unified Communications Manager* for more information about upgrading from a local or a remote source.

Install Locale Installer on IM and Presence Service

- Install the Locale Installer on Cisco Unified Communications Manager before you install locales for IM and Presence Service. If you want to use a locale other than English, you must install the appropriate language installers on both Cisco Unified Communications Manager and on IM and Presence Service.
- If your IM and Presence Service cluster has more than one node, make sure that the locale installer is installed on every node in the cluster (install on the IM and Presence database publisher node before the subscriber nodes).

- User locales should not be set until all appropriate locale installers are loaded on both systems. Users may experience problems if they inadvertently set their user locale after the locale installer is loaded on Cisco Unified Communications Manager but before the locale installer is loaded on IM and Presence Service. If issues are reported, we recommend that you notify each user to sign into the Cisco Unified Communications Self Care Portal and change their locale from the current setting to English and then back again to the appropriate language. You can also use the BAT tool to synchronize user locales to the appropriate language.

Procedure

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 Locales Reference

See the following table for a description of the messages that can occur during Locale Installer activation. If an error occurs, you can view the messages in the installation log.

Table 37: Locale Installer Messages and Descriptions

Message	Description
[LOCALE] File not found: <language>_<country>_user_locale.csv, the user locale has not been added to the database.	This error occurs when the system cannot locate the CSV file, which contains user locale information to add to the database, which indicates an error with the build process.
[LOCALE] File not found: <country>_network_locale.csv, the network locale has not been added to the database.	This error occurs when the system cannot locate the CSV file, which contains network locale information to add to the database This indicates an error with the build process.
[LOCALE] CSV file installer installdb is not present or not executable	You must ensure that an application called installdb is present. It reads information that a CSV file contains and applies it correctly to the target database. If this application is not found, it did not get installed with the Cisco Unified Communications application (very unlikely), has been deleted (more likely), or the node does not have a Cisco Unified Communications application, such as Cisco Unified Communications Manager or IM and Presence Service, installed (most likely). Installation of the locale will terminate because locales will not work without the correct records in the database.
[LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maDialogs_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maMessages_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maGlobalUI_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt.Checksum.	These errors could occur when the system fails to create a checksum file, which an absent Java executable, `/usr/local/thirdparty/java/j2sdk/jre/bin/java`, an absent or damaged Java archive file, `/usr/local/cm/jar/cmutil.jar`, or an absent or damaged Java class, `com.cisco.ccm.util.Zipper`, causes. Even if these errors occur, the locale will continue to work correctly, with the exception of Cisco Unified Communications Manager Assistant, which can not detect a change in localized Cisco Unified Communications Manager Assistant files.
[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.

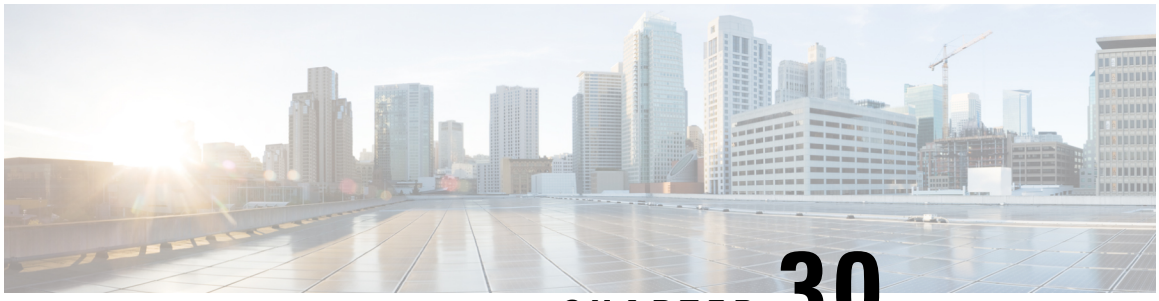
Message	Description
[LOCALE] Could not locate <locale-installer-file-name>	The system will not migrate this locale during an upgrade. The downloaded locale installer file no longer resides in the download location. The platform may have moved or deleted it. This is noncritical error indicates that after 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.
[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 38: 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 30

Manage the Server

Manage the Server Overview

This chapter contains information on how to edit server details for a deployed system. This includes assigning a new node to a cluster, removing a node from a cluster, viewing the presence status and changing server address details.

Changing the Server Address

If you have an up and running system, and you need to make any of the following changes to the server addressing, refer to the procedures in the document *Changing the IP Address and Hostname for Cisco Unified Communications Manager and the IM and Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

This applies to the following types of address changes:

- Changing the server IP Address
- Changing the server hostname
- Changing the node name (for example, if you are using an IP address to define the node name and you want to use a hostname instead).
- Changing the default domain for the IM and Presence Service

Delete IM and Presence Node From Cluster

Follow this procedure if you need to safely remove an IM and Presence Service node from its presence redundancy group and cluster.

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

Procedure

Step 1 On the **Cisco Unified CM Administration > System > Presence Redundancy Groups** page, disable High Availability if it is enabled.

Step 2 On the **Cisco Unified CM Administration > User Management > Assign Presence Users** page, unassign or move all the users off the node that you want to remove.

Step 3 To remove the node from its presence redundancy group, choose **Not-Selected** from the Presence Server drop down list on the presence redundancy group's **Presence Redundancy Group Configuration** page. Select **OK** when a warning dialog box indicates that services in the presence redundancy group will be restarted as a result of unassigning the node.

Note You cannot delete the publisher node directly from a presence redundancy group. To delete a publisher node, first unassign users from the publisher node and delete the presence redundancy group completely.

However, you can add the deleted IM and Presence node back into the cluster. For more information on how to add the deleted nodes, see Add Deleted Server Back in to Cluster, on page 332. In this scenario, the **DefaultCUPSubcluster** is created automatically when the deleted publisher node is added back to the server in the **System > Server** screen in the Cisco Unified CM Administration console.

Step 4 In Cisco Unified CM Administration, delete the unassigned node from the **System** > **Server**. Click **OK** when a warning dialog box indicates that this action cannot be undone.

Step 5 Shut down the host VM or server for the node you have unassigned.

Step 6 Restart the **Cisco XCP Router** on all nodes.

Add Deleted Server Back in to Cluster

If you delete a subsequent node (subscriber) from Cisco Unified Communications Manager Administration and you want to add it back to the cluster, perform the following procedure.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, add the server by choosing **System** > **Server**.

Step 2 After you add the subsequent node to Cisco Unified Communications Manager Administration, perform an installation on the server by using the disk that Cisco provided in the software kit for your version.

Tip Make sure that the version that you install matches the version that runs on the publisher node. If the version that is running on the publisher does not match your installation file, choose the Upgrade During Install option during the installation process. For details, see the *Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service*.

Step 3 After you install Cisco UnifiedCM, configure the subsequent node, as described in the installation documentation that supports your version of Cisco UnifiedCM.

Step 4 Access the Cisco Unified Reporting, RTMT, or the CLI to verify that database replication is occurring between existing nodes; if necessary, repair database replication between the nodes.

Add Node to Cluster Before Install

Use Cisco Unified Communications Manager Administration to add a new node to a cluster before installing the node. The server type you select when adding the node must match the server type you install.

You must configure a new node on the first node using Cisco Unified Communications Manager Administration before you install the new node. To install a node on a cluster, see the *Cisco Unified Communications Manager Installation Guide*.

For Cisco Unified Communications Manager Video/Voice servers, the first server you add during an initial installation of the Cisco Unified Communications Manager software is designated the publisher node. All subsequent server installations or additions are designated as subscriber nodes. The first Cisco Unified Communications Manager IM and Presence node you add to the cluster is designated the IM and Presence Service database publisher node.

Note You cannot use Cisco Unified Communications Manager Administration to change the server type after the server has been added. You must delete the existing server instance, and then add the new server again and choose the correct server type setting.

Procedure

Step 1 Select **System** > **Server**.

The **Find and List Servers** window displays.

Step 2 Click **Add New**.

The **Server Configuration - Add a Server** window displays.

Step 3 From the **Server Type** drop-down list box, choose the server type that you want to add, and then click **Next**.

- CUCM Video/Voice
- CUCM IM and Presence

Step 4 In the **Server Configuration** window, enter the appropriate server settings.

For server configuration field descriptions, see Server Settings.

Step 5 Click **Save**.

View Presence Server Status

Use Cisco Unified Communications Manager Administration to view the status of critical services and self-diagnostic test results for the IM and Presence Service node.

Procedure

Step 1 Select **System** > **Server**.

The **Find and List Servers** window appears.

Step 2 Select the server search parameters, and then click **Find**.

Matching records appear.

Step 3 Select the IM and Presence server that is listed in the **Find and List Servers** window.

The **Server Configuration** window appears.

Step 4 Click on the Presence Server Status link in the IM and Presence Server Information section of the **Server Configuration** window.

The **Node Details** window for the server appears.

Restarting Services with High Availability

If you make any system configuration changes, or system upgrades, that require you to disable High Availability and then restart either the Cisco XCP router, Cisco Presence Engine, or the server itself, you must allow sufficient time for Cisco Jabber sessions to be recreated before you enable High Availability. Otherwise, Presence won't work for Jabber clients whose sessions aren't created.

Make sure to follow this process:

Procedure

Step 1 Before you make any changes, check the **Presence Topology** window in Cisco Unified CM IM and Presence Administration window (**System** > **Presence Topology**). Take a record of the number of assigned users to each node in each Presence Redundancy Group.

Step 2 Disable High Availability in each Presence Redundancy Group and wait at least two minutes for the new HA settings to synchronize.

Step 3 Do whichever of the following is required for your update:

- Restart the Cisco XCP Router
- Restart the Cisco Presence Engine
- Restart the server

Step 4 After the restart, monitor the number of active sessions on all nodes.

Step 5 For each node, run the `show perf query counter "Cisco Presence Engine" ActiveJsmSessions` CLI command on each node to confirm the number of active sessions on each node. The number of active sessions should match the number that you recorded in step 1 for assigned users. It should take no more than 15 minutes for all sessions to resume.

Step 6 Once all of your sessions are created, you can enable High Availability within the Presence Redundancy Group.

Note If 30 minutes passes and the active sessions haven't yet been created, restart the Cisco Presence Engine. If that doesn't work, there is a larger system issue for you to fix.

Note It is not recommended to do back-to-back restarts of the Cisco XCP Router and/or Cisco Presence Engine. However, if you do need to do a restart: restart the first service, wait for all of the JSM sessions to be recreated. After all of the JSM sessions are created, then do the second restart.

Hostname Configuration

The following table lists the locations where you can configure a host name for the Unified Communications Manager server, the allowed number of characters for the host name, and the recommended first and last characters for the host name. Be aware that, if you do not configure the host name correctly, some components in Unified Communications Manager, such as the operating system, database, installation, and so on, may not work as expected.

Table 39: Host Name Configuration in Cisco Unified Communications Manager

Host Name Location	Allowed Configuration	Allowed Number of Characters	Recommended First Character for Host Name	Recommended Last Character for Host Name
Host Name/ IP Address field **System** > **Server** in Cisco Unified Communications Manager Administration	You can add or change the host name for a server in the cluster.	2-63	alphabetic	alphanumeric
Hostname field Cisco Unified Communications Manager installation wizard	You can add the host name for a server in the cluster.	1-63	alphabetic	alphanumeric
Hostname field **Settings** > **IP** > **Ethernet** in Cisco Unified Communications Operating System	You can change, not add, the host name for a server in the cluster.	1-63	alphabetic	alphanumeric

Host Name Location	Allowed Configuration	Allowed Number of Characters	Recommended First Character for Host Name	Recommended Last Character for Host Name
set network hostname hostname Command Line Interface	You can change, not add, the host name for a server in the cluster.	1-63	alphabetic	alphanumeric

Tip The host name must follow the rules for ARPANET host names. Between the first and last character of the host name, you can enter alphanumeric characters and hyphens.

Before you configure the host name in any location, review the following information:

- The Host Name/IP Address field in the Server Configuration window, which supports device-to-server, application-to-server, and server-to-server communication, allows you to enter an IPv4 address in dotted decimal format or a host name.

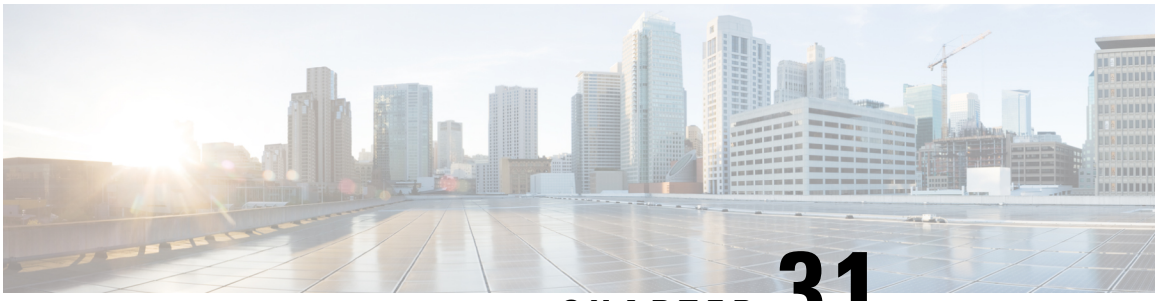
  After you install the Unified Communications Manager publisher node, the host name for the publisher automatically displays in this field. Before you install a Unified Communications Manager subscriber node, enter either the IP address or the host name for the subscriber node in this field on the Unified Communications Manager publisher node.

  In this field, configure a host name only if Unified Communications Manager can access the DNS server to resolve host names to IP addresses; make sure that you configure the Cisco Unified Communications Manager name and address information on the DNS server.

Tip In addition to configuring Unified Communications Manager information on the DNS server, you enter DNS information during the Cisco Unified Communications Manager installation.

- During the installation of the Unified Communications Manager publisher node, you enter the host name, which is mandatory, and IP address of the publisher node to configure network information; that is, if you want to use static networking.

  During the installation of a Unified Communications Manager subscriber node, you enter the hostname and IP address of the Unified Communications Manager publisher node, so that Unified Communications Manager can verify network connectivity and publisher-subscriber validation. Additionally, you must enter the host name and the IP address for the subscriber node. When the Unified Communications Manager installation prompts you for the host name of the subscriber server, enter the value that displays in the Server Configuration window in Cisco Unified Communications Manager Administration; that is, if you configured a host name for the subscriber server in the Host Name/IP Address field.



CHAPTER 31

Backup the System

Backup Overview

Cisco recommends performing regular backups. You can use the Disaster Recovery System (DRS) to do a full data backup for all servers in a cluster. You can set up automatic backups or invoke a backup at any time.

The Disaster Recovery System performs a cluster-level backup, which means that it collects backups for all servers in a Cisco Unified Communications Manager cluster to a central location and archives the backup data to physical storage device. Backup files are encrypted and can be opened only by the system software.

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

When you perform a system data restoration, you can choose which nodes in the cluster you want to restore.

The Disaster Recovery System includes the following capabilities:

- A user interface for performing backup and restore tasks.
- A distributed system architecture for performing backup functions.
- Scheduled backups or manual (user-invoked) backups.
- It archives backups to a remote sftp server.

The table displays the features and components that the Disaster Recovery System can back up and restore. For each feature that you choose, the system backs up all its components automatically.

Table 40: Cisco Unified CM Features and Components

Feature	Components
CCM - Unified Communications Manager	Unified Communications Manager database
	Platform
	Serviceability
	Music On Hold (MOH)
	Cisco Emergency Responder
	Bulk Tool (BAT)
	Preference
	Phone device files (TFTP)
	syslogagt (SNMP syslog agent)
	cdpagent (SNMP cdp agent)
	tct (trace collection tool)
	Call Detail Records (CDRs)
	CDR Reporting and Analysis (CAR)

Table 41: IM and Presence Features and Components

Feature	Components
IM and Presence Service	IM and Presence database
	syslogagt (SNMP syslog agent)
	cdpagent (SNMP cdp agent)
	Platform
	Reporter (Serviceability Reporter)
	CUP SIP Proxy
	XCP
	CLM
	Bulk Tool (BAT)
	Preference
	tct (trace collection tool)

Backup Prerequisites

- Make sure that you meet the version requirements:
  - All Cisco Unified Communications Manager cluster nodes must be running the same version of the Cisco Unified Communications Manager application.
  - All IM and Presence Service cluster nodes must be running the same version of the IM and Presence Service application.
  - The software version saved in the backup file must match the version that is running on the cluster nodes.

  The entire version string must match. For example, if the IM and Presence database publisher node is at version 11.5.1.10000-1, then all IM and Presence subscriber nodes must be 11.5.1.10000-1, and the backup file must also be must be 11.5.1.10000-1. If you try to restore the system from a backup file that does not match the current version, the restore will fail. Ensure that you backup the system whenever you upgrade the software version so that the version saved in the backup file matches the version that is running on the cluster nodes.
- Be aware the DRS encryption depends on the cluster security password. When running the backup, DRS generates a random password for encryption and then encrypts the random password with the cluster security password. If the cluster security password ever gets changed between the backup and this restore, you will need to know what the password was at the time of the backup in order to use that backup file to restore your system or take a backup immediately after the security password change/reset.
- If you want to back up to a remote device, make sure that you have an SFTP server set up. For more information on the available SFTP servers, see SFTP Servers for Remote Backups , on page 345

Backup Task Flow

Complete these tasks to configure and run a backup. Do not perform any OS Administration tasks while a backup is running. This is because Disaster Recovery System blocks all OS Administration requests by locking platform API. However, Disaster Recovery System does not block most CLI commands, because only the CLI-based upgrade commands use the Platform API locking package.

Procedure

	Command or Action	Purpose
Step 1	Configure Backup Devices, on page 340	Specify the devices on which to back up data.
Step 2	Estimate Size of Backup File, on page 341	Estimate size of backup file created on the SFTP device.
Step 3	Choose one of the following options: • Configure a Scheduled Backup, on page 341 • Start a Manual Backup, on page 343	Create a backup schedule to back up data on a schedule. Optionally, run a manual backup.

	Command or Action	Purpose
Step 4	View Current Backup Status, on page 343	Optional. Check the Status of the Backup. While a backup is running, you can check the status of the current backup job.
Step 5	View Backup History, on page 344	Optional. View Backup History

Configure Backup Devices

You can configure up to 10 backup devices. Perform the following steps to configure the location where you want to store backup files.

Before you begin

- Ensure you have write access to the directory path in the SFTP server to store the backup file.
- Ensure that the username, password, server name, and directory path are valid as the DRS Master Agent validates the configuration of the backup device.

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

Procedure

Step 1 From Disaster Recovery System, select **Backup** > **Backup Device**.

Step 2 In the **Backup Device List** window, do either of the following:

- To configure a new device, click **Add New**.
- To edit an existing backup device, enter the search criteria, click Find, and **Edit Selected**.
- To delete a backup device, select it in the **Backup Device** list and click **Delete Selected**.

You cannot delete a backup device that is configured as the backup device in a backup schedule.

Step 3 Enter a backup name in the **Backup Device Name** field.

The backup device name contains only alphanumeric characters, spaces (), dashes (-) and underscores (_). Do not use any other characters.

Step 4 In the **Select Destination** area, under **Network Directory** perform the following:

- In the **Host name/IP Address** field, enter the hostname or IP address for the network server.
- In the **Path name** field, enter the directory path where you want to store the backup file.
- In the **User name** field, enter a valid username.
- In the **Password** field, enter a valid password.
- From the **Number of backups to store on Network Directory** drop-down list, choose the required number of backups.

Step 5 Click **Save**.

What to do next

Estimate Size of Backup File, on page 341

Estimate Size of Backup File

Cisco Unified Communications Manager will estimate the size of the backup tar, only if a backup history exists for one or more selected features.

The calculated size is not an exact value but an estimated size of the backup tar. Size is calculated based on the actual backup size of a previous successful backup and may vary if the configuration changed since the last backup.

You can use this procedure only when the previous backups exist and not when you back up the system for the first time.

Follow this procedure to estimate the size of the backup tar that is saved to a SFTP device.

Procedure

Step 1 From the Disaster Recovery System, select **Backup** > **Manual Backup**.

Step 2 In the **Select Features** area, select the features to back up.

Step 3 Click **Estimate Size** to view the estimated size of backup for the selected features.

What to do next

Perform one of the following procedures to backup your system:

- Configure a Scheduled Backup, on page 341
- Start a Manual Backup, on page 343

Configure a Scheduled Backup

You can create up to 10 backup schedules. Each backup schedule has its own set of properties, including a schedule for automatic backups, the set of features to back up, and a storage location.

Be aware that your backup .tar files are encrypted by a randomly generated password. This password is then encrypted by using the cluster security password and gets saved along with the backup .tar files. You must remember this security password or take a backup immediately after the security password change or reset.

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

Before you begin

Configure Backup Devices, on page 340

Procedure

Step 1 From the Disaster Recovery System, choose **Backup Scheduler**.

Step 2 In the **Schedule List** window, do one of the following steps to add a new schedule or edit an existing schedule.

- To create a new schedule, click **Add New**.
- To configure an existing schedule, click the name in the Schedule List column.

Step 3 In the **scheduler** window, enter a schedule name in the **Schedule Name** field.

Note You cannot change the name of the default schedule.

Step 4 Select the backup device in the **Select Backup Device** area.

Step 5 Select the features to back up in the **Select Features** area. You must choose at least one feature.

Step 6 Choose the date and time when you want the backup to begin in the **Start Backup at** area.

Step 7 Choose the frequency at which you want the backup to occur in the **Frequency** area. The frequency can be set to Once Daily, Weekly, and Monthly. If you choose **Weekly**, you can also choose the days of the week when the backup will occur.

Tip To set the backup frequency to **Weekly**, occurring Tuesday through Saturday, click **Set Default**.

Step 8 To update these settings, click **Save**.

Step 9 Choose one of the following options:

- To enable the selected schedules, click **Enable Selected Schedules**.
- To disable the selected schedules, click **Disable Selected Schedules**.
- To delete the selected schedules, click **Delete Selected**.

Step 10 To enable the schedule, click **Enable Schedule**.

The next backup occurs automatically at the time that you set.

Note Ensure that all servers in the cluster are running the same version of Cisco Unified Communications Manager or Cisco IM and Presence Service and are reachable through the network. Servers that are not reachable at the time of the scheduled backup will not get backed up.

What to do next

Perform the following procedures:

- Estimate Size of Backup File, on page 341
- (Optional) View Current Backup Status, on page 343

Start a Manual Backup

Before you begin

- Ensure that you use a network device as the storage location for the backup files. Virtualized deployments of Unified Communications Manager do not support the use of tape drives to store backup files.
- Ensure that all cluster nodes have the same installed version of Cisco Unified Communications Manager or IM and Presence Service.
- The backup process can fail due to non availability of space on a remote server or due to interruptions in the network connectivity. You need to start a fresh backup after addressing the issues that caused the backup to fail.
- Ensure that there are no network interruptions.
- Configure Backup Devices, on page 340
- Estimate Size of Backup File, on page 341
- Make sure that you have a record of the cluster security password. If the cluster security password changes after you complete this backup, you will need to know the password or you will not be able to use the backup file to restore your system.

Note While a backup is running, you cannot perform any tasks in Cisco Unified OS Administration or Cisco Unified IM and Presence OS Administration because Disaster Recovery System locks the platform API to block all requests. However, Disaster Recovery System does not block most CLI commands because only the CLI-based upgrade commands use the Platform API locking package.

Procedure

Step 1 From the Disaster Recovery System, select **Backup** > **Manual Backup**.

Step 2 In the **Manual Backup** window, select a backup device from the **Backup Device Name** area.

Step 3 Choose a feature from the **Select Features** area.

Step 4 Click **Start Backup.**

What to do next

(Optional) View Current Backup Status, on page 343

View Current Backup Status

Perform the following steps to check the status of the current backup job.

Caution Be aware that if the backup to the remote server is not completed within 20 hours, the backup session times out and you must begin a fresh backup.

Procedure

Step 1 From the Disaster Recovery System, select **Backup** > **Current Status**.

Step 2 To view the backup log file, click the log filename link.

Step 3 To cancel the current backup, click **Cancel Backup**.

Note The backup cancels after the current component completes its backup operation.

What to do next

View Backup History, on page 344

View Backup History

Perform the following steps to view the backup history.

Procedure

Step 1 From the Disaster Recovery System, select **Backup** > **History**.

Step 2 From the **Backup History** window, you can view the backups that you have performed, including filename, backup device, completion date, result, version, features that are backed up, and failed features.

Note The **Backup History** window displays only the last 20 backup jobs.

Backup Interactions and Restrictions

• Backup Restrictions , on page 345

Backup Restrictions

The following restrictions apply to backups:

Table 42: Backup Restrictions

Restriction	Description
Cluster Security Password	We recommend that you run a backup whenever you change the cluster security password. Backup encryption uses the cluster security password to encrypt data on the backup file. If you edit the cluster security password after a backup file is created, you will not be able to use that backup file to restore data unless you remember the old password.
Certificate Management	The Disaster Recovery System (DRS) uses an SSL-based communication between the Master Agent and the Local Agent for authentication and encryption of data between the Cisco Unified Communications Manager cluster nodes. DRS makes use of the IPsec certificates for its Public/Private Key encryption. Be aware that if you delete the IPSEC truststore(hostname.pem) file from the Certificate Management pages, then DRS will not work as expected. If you delete the IPSEC-trust file manually, you must ensure that you upload the IPSEC certificate to the IPSEC-trust. For more details, see the "Certificate management" section in the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

SFTP Servers for Remote Backups

To back up data to a remote device on the network, you must have an SFTP server that is configured. For internal testing, Cisco uses the SFTP Server on Cisco Prime Collaboration Deployment (PCD) which is provided by Cisco, and which is supported by Cisco TAC. Refer to the following table for a summary of the SFTP server options:

Use the information in the following table to determine which SFTP server solution to use in your system.

Table 43: SFTP Server Information

SFTP Server	Information
SFTP Server on Cisco Prime Collaboration Deployment	This server is the only SFTP server that is provided and tested by Cisco, and fully supported by Cisco TAC. Version compatibility depends on your version of Unified Communications Manager and Cisco Prime Collaboration Deployment. See the Cisco Prime Collaboration Deployment Administration Guide before you upgrade its version (SFTP) or Unified Communications Manager to ensure that the versions are compatible.

SFTP Server	Information
SFTP Server from a Technology Partner	These servers are third party provided and third party tested. Version compatibility depends on the third party test. See the Technology Partner page if you upgrade their SFTP product and/or upgrade Unified Communications Manager for which versions are compatible: https://marketplace.cisco.com
SFTP Server from another Third Party	These servers are third party provided and are not officially supported by Cisco TAC. Version compatibility is on a best effort basis to establish compatible SFTP versions and Unified Communications Manager versions. **Note** These products have not been tested by Cisco and we cannot guarantee functionality. Cisco TAC does not support these products. For a fully tested and supported SFTP solution, use Cisco Prime Collaboration Deployment or a Technology Partner.

Cipher Support

For Unified Communications Manager 11.5, Unified Communications Manager advertises the following CBC and CTR ciphers for SFTP connections:

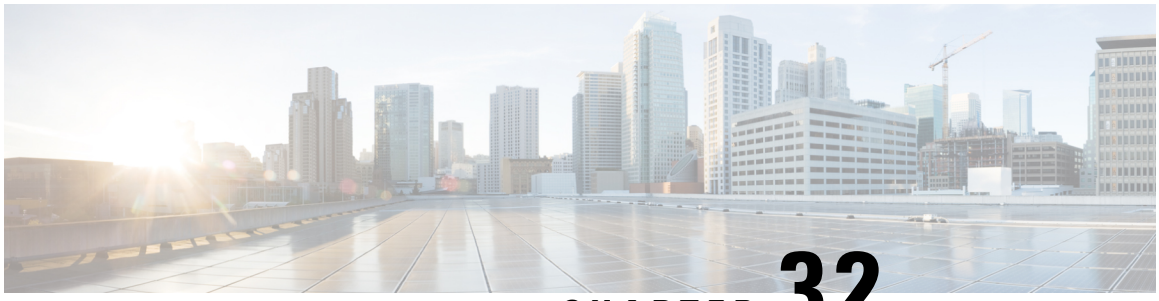
- aes128-cbc
- 3des-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr

Note Make sure that the backup SFTP Server supports one of these ciphers to communicate with Unified Communications Manager.

From Unified Communications Manager 12.0 release onwards, CBC ciphers are not supported. Unified Communications Manager supports and advertises only the following CTR ciphers:

- aes256-ctr
- aes128-ctr
- aes192-ctr

Note Make sure that the backup SFTP Server supports one of these CTR ciphers to communicate with Unified Communications Manager.



CHAPTER 32

Restore the System

Restore Overview

The Disaster Recovery System (DRS) provides a wizard to walk you through the process of restoring your system.

The backup files are encrypted and only the DRS system can open them to restore the data. The Disaster Recovery System includes the following capabilities:

- A user interface for performing restore tasks.
- A distributed system architecture for performing restore functions.

Master Agent

The system automatically starts the Master Agent service on each node of the cluster, but the Master Agent is functional only on the publisher node. The Master Agents on the subscriber nodes do not perform any functions.

Local Agents

The server has a Local Agent to perform backup and restore functions.

Each node in a Cisco Unified Communications Manager cluster, including the node that contains the Master Agent, must have its own Local Agent to perform backup and restore functions.

Note By default, a Local Agent automatically gets started on each node of the cluster, including IM and Presence nodes.

Restore Prerequisites

- Make sure that you meet the version requirements:
  - All Cisco Unified Communications Manager cluster nodes must be running the same version of the Cisco Unified Communications Manager application.
  - All IM and Presence Service cluster nodes must be running the same version of the IM and Presence Service application.
  - The version saved in the backup file must match the version that is running on the cluster nodes.

  The entire version string must match. For example, if the IM and Presence database publisher node is at version 11.5.1.10000-1, then all IM and Presence subscriber nodes must be 11.5.1.10000-1, and the backup file must also be must be 11.5.1.10000-1. If you try to restore the system from a backup file that does not match the current version, the restore will fail.
- Make sure that the IP address, hostname, DNS configuration and deployment type for the server matches the IP address, hostname, DNS configuration and deployment type that are stored on the backup file.
- If you have changed the cluster security password since the backup was run, make sure that you have a record of the old password, or the restore will fail.
- If IPsec policy is enabled in a cluster, ensure to disable it before starting the restore operation.

Re-enable SAML SSO after Restore

Important This section is applicable for Release 12.5(1)SU7 only.

After restoring the system using DRS, SAML SSO can be disabled on any of the nodes in the cluster intermittently. To re-enable SAML SSO on the affected nodes, you must perform the following:

1. From Cisco Unified CM Administration, choose **System** > **SAML Single Sign On**.
2. Click **Fix All Disabled Servers**.

   The **SAML Single Sign-On Configuration** window appears; click **Next**.
3. Click **Run SSO Test**.
4. After you see the **"SSO Test Succeeded!"** message, close the browser window; click **Finish**.

Note Cisco Tomcat restarts during SAML SSO re-enabling process. It will not have any impact on the nodes where SAML SSO is already enabled.

Restore Task Flow

During the restore process, do not perform any tasks with Cisco Unified Communications Manager OS Administration or Cisco Unified IM and Presence OS Administration.

Procedure

	Command or Action	Purpose
Step 1	Restore the First Node Only, on page 349	(Optional) Use this procedure only to restore the first publisher node in the cluster.
Step 2	Restore Subsequent Cluster Node, on page 351	(Optional) Use this procedure to restore the subscriber nodes in a cluster.
Step 3	Restore Cluster in One Step After Publisher Rebuilds, on page 352	(Optional) Follow this procedure to restore the entire cluster in one step if the publisher has already been rebuilt.
Step 4	Restore Entire Cluster, on page 354	(Optional) Use this procedure to restore all nodes in the cluster, including the publisher node. If a major hard drive failure or upgrade occurs, or in the event of a hard drive migration, you may need to rebuild all nodes in the cluster.
Step 5	Restore Node Or Cluster to Last Known Good Configuration, on page 355	(Optional) Use this procedure only if you are restoring a node to a last known good configuration. Do not use this after a hard drive failure or other hardware failure.
Step 6	Restart a Node, on page 355	Use this procedure to restart a node.
Step 7	Check Restore Job Status, on page 356	(Optional) Use this procedure to check the restore job status.
Step 8	View Restore History, on page 357	(Optional) Use this procedure to view the restore history.

Restore the First Node Only

If you are restoring the first node after a rebuild, you must configure the backup device.

This procedure is applicable to the Cisco Unified Communications Manager First Node, also known as the publisher node. The other Cisco Unified Communications Manager nodes and all the IM and Presence Service nodes are considered as secondary nodes or subscribers.

Before you begin

If there is an IM and Presence Service node in the cluster, ensure that it is running and accessible when you restore the first node. This is required so that a valid backup file can be found during the procedure.

Procedure

Step 1 From the Disaster Recovery System, choose **Restore** > **Restore Wizard**.

Step 2 In the **Restore Wizard Step 1** window, **Select Backup Device** area, select the appropriate backup device to restore.

Step 3 Click **Next**.

Step 4 In the **Restore Wizard Step 2** window, select the backup file you want to restore.

Note The backup filename indicates the date and time that the system created the backup file.

Step 5 Click **Next**.

Step 6 In the **Restore Wizard Step 3** window, click **Next**.

Step 7 Choose the features that you want to restore.

Note The features that you have selected for backup will be displayed.

Step 8 Click **Next**. The Restore Wizard Step 4 window displays.

Step 9 Select the Perform file integrity check using the SHA1 Message Digest checkbox if you want to run a file integrity check.

Note The file integrity check is optional and is only needed in the case of SFTP backups.

Be aware that the file integrity check process consumes a significant amount of CPU and network bandwidth, which slows down the restore process.

We can use SHA-1 for message digest verification in FIPS mode as well. SHA-1 is allowed for all non-digital signature uses in the hash functions applications like HMAC and Random Bit Generation that are not used for digital signatures. For instance, SHA-1 can still be used to compute a checksum. Only for signature generation and verification, we can't use SHA-1.

Step 10 Select the node to restore.

Step 11 Click **Restore** to restore the data.

Step 12 Click **Next**.

Step 13 When you are prompted to select the nodes to restore, choose only the first node (the publisher).

Caution Do not select the subsequent (subscriber) nodes in this condition as this will result in failure of the restore attempt.

Step 14 (Optional) From the **Select Server Name** drop-down list, select the subscriber node from which you want to restore the publisher database. Ensure that the subscriber node that you chose is in-service and connected to the cluster.
The Disaster Recovery System restores all non database information from the backup file and pulls the latest database from the chosen subscriber node.

Note This option appears only if the backup file that you selected includes the CCMDB database component. Initially, only the publisher node is fully restored, but when you perform Step 14 and restart the subsequent cluster nodes, the Disaster Recovery System performs database replication and fully synchronizes all cluster node databases. This ensures that all cluster nodes are using current data.

Step 15 Click **Restore**.

Step 16 Your data is restored on the publisher node. Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore.

Note Restoring the first node restores the whole Cisco Unified Communications Manager database to the cluster. This may take up to several hours based on number of nodes and size of database that is being restored. Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore.

Step 17 When the **Percentage Complete** field on the **Restore Status** window, shows 100%, restart the server. Restart of all the nodes in the cluster is required in case of restoring only to the first node. Ensure that you restart the first node before you restart the subsequent nodes. For information about how to restart the server, see the What to Do Next section.

Note If you are restoring a Cisco Unified Communications Manager node only, the Cisco Unified Communications Manager and IM and Presence Service cluster must be restarted.

If you are restoring an IM and Presence Service Publisher node only, the IM and Presence Service cluster must be restarted.

What to do next

- (Optional) To view the status of the restore, see Check Restore Job Status, on page 356
- To restart a node, see Restart a Node, on page 355

Restore Subsequent Cluster Node

This procedure is applicable to the Cisco Unified Communications Manager subscriber (subsequent) nodes only. The first Cisco Unified Communications Manager node installed is the publisher node. All other Cisco Unified Communications Manager nodes, and all IM and Presence Service nodes are subscriber nodes.

Follow this procedure to restore one or more Cisco Unified Communications Manager subscriber nodes in the cluster.

Before you begin

Before you perform a restore operation, ensure that the hostname, IP address, DNS configuration, and deployment type of the restore matches the hostname, IP address, DNS configuration, and deployment type of the backup file that you want to restore. Disaster Recovery System does not restore across different hostnames, IP addresses, DNS configurations and deployment types.

Ensure that the software version that is installed on the server matches the version of the backup file that you want to restore. Disaster Recovery System supports only matching software versions for restore operations. If you are restoring the subsequent nodes after a rebuild, you must configure the backup device.

Procedure

Step 1 From the Disaster Recovery System, select **Restore** > **Restore Wizard**.

Step 2 In the **Restore Wizard Step 1** window, **Select Backup Device** area, choose the backup device from which to restore.

Step 3 Click **Next**.

Step 4 In the **Restore Wizard Step 2** window, select the backup file that you want to restore.

Step 5 Click **Next**.

Step 6 In the **Restore Wizard Step 3** window, select the features that you want to restore.

Note Only the features that were backed up to the file that you chose display.

Step 7 Click **Next**. The Restore Wizard Step 4 window displays.

Step 8 In the **Restore Wizard Step 4** window, when you are prompted to choose the nodes to restore, select only the subsequent nodes.

Step 9 Click **Restore**.

Step 10 Your data is restored on the subsequent nodes. For more information about how to view the status of the restore, see the What to Do Next section.

Note During the restore process, do not perform any tasks with Cisco Unified Communications Manager Administration or User Options.

Step 11 When the **Percentage Complete** field on the **Restore Status** window shows 100%, restart the secondary servers you just restored. Restart of all the nodes in the cluster is required in case of restoring only to the first node. Ensure that you restart the first node before you restart the subsequent nodes. For information about how to restart the server, see the What to Do Next section.

Note If the IM and Presence Service first node is restored. Ensure to restart the IM and Presence Service first node before you restart the IM and Presence Service subsequent nodes.

What to do next

- (Optional) To view the status of the restore, see Check Restore Job Status, on page 356
- To restart a node, see Restart a Node, on page 355

Restore Cluster in One Step After Publisher Rebuilds

Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore. Follow this procedure to restore the entire cluster in one step if the publisher has already been rebuilt or freshly installed.

Procedure

Step 1 From the Disaster Recovery System, select **Restore** > **Restore Wizard**.

Step 2 In the **Restore Wizard Step 1** window **Select Backup Device** area, choose the backup device from which to restore.

Step 3 Click **Next**.

Step 4 In the **Restore Wizard Step 2** window, select the backup file that you want to restore.

The backup filename indicates the date and time that the system created the backup file.

Choose only the backup file of the cluster from which you want to restore the entire cluster.

Step 5 Click **Next**.

Step 6 In the **Restore Wizard Step 3** window, select the features that you want to restore.

The screen displays only those features that were saved to the backup file.

Step 7 Click **Next**.

Step 8 In the **Restore Wizard Step 4** window, click **One-Step Restore**.

This option appears on **Restore Wizard Step 4** window only if the backup file selected for restore is the backup file of the cluster and the features chosen for restore includes the feature(s) that is registered with both publisher and subscriber nodes. For more information, see Restore the First Node Only, on page 349 and Restore Subsequent Cluster Node, on page 351.

Note If a status message indicates that *Publisher has failed to become cluster aware. Cannot start one-step restore*, you need to restore the publisher node and then the subscriber node. See the Related topics for more information.

This option allows the publisher to become cluster aware and will take five minutes to do so. Once you click on this option, a status message displays as “Please wait for 5 minutes until Publisher becomes cluster aware and do not start any backup or restore activity in this time period”.

After the delay, if the publisher becomes cluster aware, a status message displays as “Publisher has become cluster aware. Please select the servers and click on Restore to start the restore of entire cluster”.

After the delay, if the publisher has not become cluster aware, a status message displays as "Publisher has failed to become cluster aware. Cannot start one-step restore. Please go ahead and do a normal two-step restore." To restore the whole cluster in two-step (publisher and then subscriber), perform the steps mentioned in Restore the First Node Only, on page 349 and Restore Subsequent Cluster Node, on page 351.

Step 9 When you are prompted to choose the nodes to restore, choose all the nodes in the cluster.

The Disaster Recovery System restores the Cisco Unified Communications Manager database (CCMDB) on subsequent nodes automatically when you restore a first node. This may take up to several hours based on number of nodes and size of that database that is being restored.

Step 10 Click **Restore**.
Your data is restored on all the nodes of the cluster.

Step 11 When the **Percentage Complete** field on the **Restore Status window** shows 100%, restart the server. Restart of all the nodes in the cluster is required in case of restoring only to the first node. Ensure that you restart the first node before you restart the subsequent nodes. For information about how to restart the server, see the What to Do Next section.

What to do next

- (Optional) To view the status of the restore, see Check Restore Job Status, on page 356

- To restart a node, see Restart a Node, on page 355

Restore Entire Cluster

If a major hard drive failure or upgrade occurs, or in the event of a hard drive migration, you have to rebuild all nodes in the cluster. Follow these steps to restore an entire cluster.

If you are doing most other types of hardware upgrades, such as replacing a network card or adding memory, you do not need to perform this procedure.

Procedure

Step 1 From Disaster Recovery System, select **Restore** > **Restore Wizard**.

Step 2 In the **Select Backup Device** area, select the appropriate backup device to restore.

Step 3 Click **Next**.

Step 4 In the **Restore Wizard Step 2** window, select the backup file you want to restore.

Note The backup filename indicates the date and time that the system created the backup file.

Step 5 Click **Next**.

Step 6 In the **Restore Wizard Step 3** window, click **Next**.

Step 7 In the **Restore Wizard Step 4** window, select all the nodes when prompted to choose restore nodes.

Step 8 Click **Restore** to restore the data.

The Disaster Recovery System restores the Cisco Unified Communications Manager database (CCMDB) on subsequent nodes automatically when you restore a first node. This may take up to several hours based on number of nodes and size of that database.

Data is restored on the all the nodes.

Note During the restore process, do not perform any tasks with Cisco Unified Communications Manager Administration or User Options.

Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore.

Step 9 Restart the server once the restoration process is completed. See the What to Do Next section for more information about how to restart the server.

Note Make sure that you restart the first node before you restart the subsequent nodes.

After the first node has restarted and is running the restored version of Cisco Unified Communications Manager, restart the subsequent nodes.

Step 10 Replication will be setup automatically after cluster reboot. Check the Replication Status value on all nodes by using the “utils dbreplication runtimestate” CLI command as described in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*. The value on each node should equal 2.

Note Database replication on the subsequent nodes may take enough time to complete after the subsequent node restarts, depending on the size of the cluster.

Tip If replication does not set up properly, use the "utils dbreplication rebuild" CLI command as described in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

What to do next

- (Optional) To view the status of the restore, see Check Restore Job Status, on page 356
- To restart a node, see Restart a Node, on page 355

Restore Node Or Cluster to Last Known Good Configuration

Follow this procedure to restore node or cluster to last known good configuration.

Before you begin

- Ensure that the restore file contains the hostname, IP address, DNS configuration, and deployment type that is configured in the backup file.
- Ensure that the Cisco Unified Communications Manager version installed on the server matches the version of the backup file that you want to restore.
- Ensure this procedure is used only to restore node to a last known good configuration.

Procedure

Step 1 From the Disaster Recovery System, choose **Restore** > **Restore Wizard**.

Step 2 In the **Select Backup Device** area, select the appropriate backup device to restore.

Step 3 Click **Next**.

Step 4 In the **Restore Wizard Step 2** window, select the backup file you want to restore.

Note The backup filename indicates the date and time that the system created the backup file.

Step 5 Click **Next**.

Step 6 In the **Restore Wizard Step 3** window, click **Next**.

Step 7 Select the appropriate node, when prompted to choose restore nodes.
Data is restored on the chosen nodes.

Step 8 Restart all nodes in the cluster. Restart the first Cisco Unified Communications Manager node before restarting the subsequent Cisco Unified Communications Manager nodes. If the cluster also has Cisco IM and Presence nodes, restart the first Cisco IM and Presence node before restarting the subsequent IM and Presence nodes. See the What to Do Next section for more information.

Restart a Node

You must restart a node after you restore data.

If you are restoring a publisher node (first node), you must restart the publisher node first. Restart subscriber nodes only after the publisher node has restarted and is successfully running the restored version of the software.

Note Do not restart IM and Presence subscriber nodes if the CUCM publisher node is offline. In such cases, the node services will fail to start because the subscriber node is unable to connect to the CUCM publisher.

Caution This procedure causes the system to restart and become temporarily out of service.

Perform this procedure on every node in the cluster that you need to restart.

Procedure

Step 1 From Cisco Unified OS Administration, select **Settings** > **Version**.

Step 2 To restart the node, click **Restart**.

Step 3 Replication will be setup automatically after cluster reboot. Check the Replication Status value on all nodes by using the **utils dbreplication runtimestate** CLI command. The value on each node should be equal 2. See Cisco Unified Communications (CallManager) Command References for more information about CLI commands.

If replication does not set up properly, use the **utils dbreplication reset** CLI command as described in the *Command Line Reference Guide for Cisco Unified Communications Solutions*.

Note Database replication on the subsequent nodes may take several hours to complete after the subsequent nodes restart, depending on the size of the cluster.

What to do next

(Optional) To view the status of the restore, see Check Restore Job Status, on page 356.

Check Restore Job Status

Follow this procedure to check the restore job status.

Procedure

Step 1 From the Disaster Recovery System, select **Restore** > **Current Status**.

Step 2 In the **Restore Status** window, click the log filename link to view the restore status.

View Restore History

Perform the following steps to view the restore history.

Procedure

Step 1 From Disaster Recovery System, choose **Restore** > **History**.

Step 2 From the **Restore History** window, you can view the restores that you have performed, including filename, backup device, completion date, result, version, features that were restored, and failed features.

The **Restore History** window displays only the last 20 restore jobs.

Data Authentication

Trace Files

The following trace file locations are used during troubleshooting or while collecting the logs.

Trace files for the Master Agent, the GUI, each Local Agent, and the JSch library get written to the following locations:

- For the Master Agent, find the trace file at platform/drf/trace/drfMA0*
- For each Local Agent, find the trace file at platform/drf/trace/drfLA0*
- For the GUI, find the trace file at platform/drf/trace/drfConfLib0*
- For the JSch, find the trace file at platform/drf/trace/drfJSch*

For more information, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html.

Command Line Interface

The Disaster Recovery System also provides command line access to a subset of backup and restore functions, as shown in the following table. For more information on these commands and on using the command line interface, see the *Command Line Interface Reference Guide* for Cisco Unified Communications Solutions at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html.

Table 44: Disaster Recovery System Command Line Interface

Command	Description
utils disaster_recovery estimate_tar_size	Displays estimated size of backup tar from SFTP/Local device and requires one parameter for feature list

Command	Description
utils disaster_recovery backup	Starts a manual backup by using the features that are configured in the Disaster Recovery System interface
utils disaster_recovery jschLogs	Enables or disables JSch library logging
utils disaster_recovery restore	Starts a restore and requires parameters for backup location, filename, features, and nodes to restore
utils disaster_recovery status	Displays the status of ongoing backup or restore job
utils disaster_recovery show_backupfiles	Displays existing backup files
utils disaster_recovery cancel_backup	Cancels an ongoing backup job
utils disaster_recovery show_registration	Displays the currently configured registration
utils disaster_recovery device add	Adds the network device
utils disaster_recovery device delete	Deletes the device
utils disaster_recovery device list	Lists all the devices
utils disaster_recovery schedule add	Adds a schedule
utils disaster_recovery schedule delete	Deletes a schedule
utils disaster_recovery schedule disable	Disables a schedule
utils disaster_recovery schedule enable	Enables a schedule
utils disaster_recovery schedule list	Lists all the schedules
utils disaster_recovery backup	Starts a manual backup by using the features that are configured in the Disaster Recovery System interface.
utils disaster_recovery restore	Starts a restore and requires parameters for backup location, filename, features, and nodes to restore.
utils disaster_recovery status	Displays the status of ongoing backup or restore job.
utils disaster_recovery show_backupfiles	Displays existing backup files.

Command	Description
utils disaster_recovery cancel_backup	Cancels an ongoing backup job.
utils disaster_recovery show_registration	Displays the currently configured registration.

Alarms and Messages

Alarms and Messages

The Disaster Recovery System issues alarms for various errors that could occur during a backup or restore procedure. The following table provides a list of Cisco Disaster Recovery System alarms.

Table 45: Disaster Recovery System Alarms and Messages

Alarm Name	Description	Explanation
DRFBackupDeviceError	DRF backup process has problems accessing device.	DRS backup process encoun while it was accessing devic
DRFBackupFailure	Cisco DRF Backup process failed.	DRS backup process encoun
DRFBackupInProgress	New backup cannot start while another backup is still running	DRS cannot start new backup backup is still running.
DRFInternalProcessFailure	DRF internal process encountered an error.	DRS internal process encoun
DRFLA2MAFailure	DRF Local Agent cannot connect to Master Agent.	DRS Local Agent cannot con Agent.
DRFLocalAgentStartFailure	DRF Local Agent does not start.	DRS Local Agent might be c
DRFMA2LAFailure	DRF Master Agent does not connect to Local Agent.	DRS Master Agent cannot co Agent.
DRFMABackupComponentFailure	DRF cannot back up at least one component.	DRS requested a component data; however, an error occur backup process, and the comp get backed up.
DRFMABackupNodeDisconnect	The node that is being backed up disconnected from the Master Agent prior to being fully backed up.	While the DRS Master Agen a backup operation on a Cisc Communications Manager n disconnected before the back completed.

Alarm Name	Description	Explanation
DRFMARestoreComponentFailure	DRF cannot restore at least one component.	DRS requested a component to r data; however, an error occurred restore process, and the compone get restored.
DRFMARestoreNodeDisconnect	The node that is being restored disconnected from the Master Agent prior to being fully restored.	While the DRS Master Agent wa a restore operation on a Cisco U Communications Manager node, disconnected before the restore c completed.
DRFMasterAgentStartFailure	DRF Master Agent did not start.	DRS Master Agent might be dov
DRFNoRegisteredComponent	No registered components are available, so backup failed.	DRS backup failed because no r components are available.
DRFNoRegisteredFeature	No feature got selected for backup.	No feature got selected for backu
DRFRestoreDeviceError	DRF restore process has problems accessing device.	DRS restore process cannot read device.
DRFRestoreFailure	DRF restore process failed.	DRS restore process encountere
DRFSftpFailure	DRF SFTP operation has errors.	Errors exist in DRS SFTP opera
DRFSecurityViolation	DRF system detected a malicious pattern that could result in a security violation.	The DRF Network Message con malicious pattern that could resu security violation like code injec directory traversal. DRF Networl has been blocked.
DRFTruststoreMissing	The IPsec truststore is missing on the node.	The IPsec truststore is missing or DRF Local Agent cannot connect Agent.
DRFUnknownClient	DRF Master Agent on the Pub received a Client connection request from an unknown server outside the cluster. The request has been rejected.	The DRF Master Agent on the Pu a Client connection request from unknown server outside the clus request has been rejected.
DRFBackupCompleted	DRF backup completed successfully.	DRF backup completed successf
DRFRestoreCompleted	DRF restore completed successfully.	DRF restore completed successf
DRFNoBackupTaken	DRF did not find a valid backup of the current system.	DRF did not find a valid backup current system after an Upgrade/ or Fresh Install.
DRFComponentRegistered	DRF successfully registered the requested component.	DRF successfully registered the component.
DRFRegistrationFailure	DRF Registration operation failed.	DRF Registration operation faile component due to some internal

Alarm Name	Description	Explanation
DRFComponentDeRegistered	DRF successfully deregistered the requested component.	DRF successfully deregistered component.
DRFDeRegistrationFailure	DRF deregistration request for a component failed.	DRF deregistration request fo failed.
DRFFailure	DRF Backup or Restore process has failed.	DRF Backup or Restore proc encountered errors.
DRFRestoreInternalError	DRF Restore operation has encountered an error. Restore cancelled internally.	DRF Restore operation has e error. Restore cancelled inter
DRFLogDirAccessFailure	DRF could not access the log directory.	DRF could not access the log
DRFDeRegisteredServer	DRF automatically de-registered all the components for the server.	The server may have been di from the Unified Communicat cluster.
DRFSchedulerDisabled	DRF Scheduler is disabled because no configured features are available for backup.	DRF Scheduler is disabled b configured features are availa
DRFSchedulerUpdated	DRF Scheduled backup configuration is updated automatically due to feature de-registration.	DRF Scheduled backup conf updated automatically due to de-registration

Restore Interactions and Restrictions

Restore Restrictions

The following restrictions apply to using Disaster Recovery System to restore Cisco Unified Communications Manager or IM and Presence Service

Table 46: Restore Restrictions

Restriction	Description
Export Restricted	You can restore the DRS backup from a restricted version only to a restricted version and the backup from an unrestricted version can be restored only to an unrestricted version. Note that if you upgrade to the U.S. export unrestricted version of Cisco Unified Communications Manager, you will not be able to later upgrade to or be able to perform a fresh install of the U.S. export restricted version of this software

Restriction	Description
Platform Migrations	You cannot use the Disaster Recovery System to migrate data between platforms (for example, from Windows to Linux or from Linux to Windows). A restore must run on the same product version as the backup. For information on data migration from a Windows-based platform to a Linux-based platform, see the *Data Migration Assistant User Guide*.
HW Replacement and Migrations	When you perform a DRS restore to migrate data to a new server, you must assign the new server the identical IP address and hostname that the old server used. Additionally, if DNS was configured when the backup was taken, then the same DNS configuration must be present prior to performing a restore. For more information about replacing a server, refer to the *Replacing a Single Server or Cluster for Cisco Unified Communications Manager guide*. In addition, you must run the Certificate Trust List (CTL) client after a hardware replacement. You must run the CTL client if you do not restore the subsequent node (subscriber) servers. In other cases, DRS backs up the certificates that you need. For more information, see the "Installing the CTL Client" and "Configuring the CTL Client " procedures in the *Cisco Unified Communications Manager Security Guide*.
Extension Mobility Cross Cluster	Extension Mobility Cross Cluster users who are logged in to a remote cluster at backup shall remain logged in after restore.

Note DRS backup/restore is a high CPU-oriented process. Smart Licence Manager is one of the components that are backed-up and restored. During this process Smart License Manger service is restarted. You can expect high resource utilization so recommended to schedule the process during maintenance period.

After successfully restoring the Cisco Unified Communications server components, register the Cisco Unified Communications Manager with Cisco Smart Software Manager or Cisco Smart Software Manager satellite. If the product is already registered before taking the backup, then reregister the product for updating the license information.

For more information on how to register the product with Cisco Smart Software Manager or Cisco Smart Software Manager satellite, see the *System Configuration Guide for Cisco Unified Communications Manager* for your release.

Troubleshooting

DRS Restore to Smaller Virtual Machine Fails

Problem

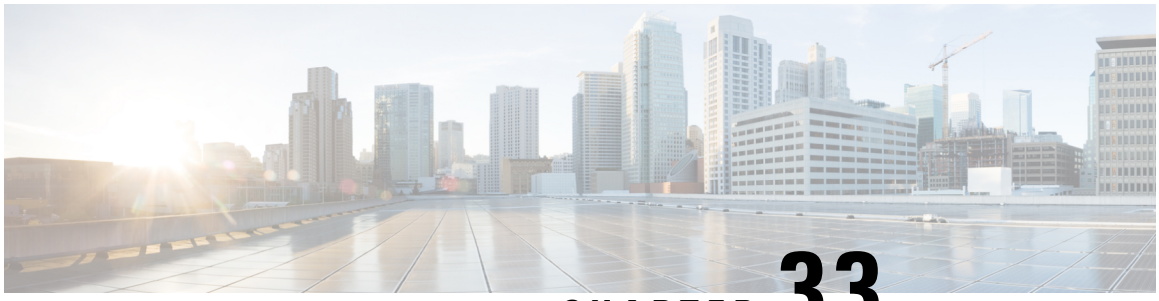
A database restore may fail if you restore an IM and Presence Service node to a VM with smaller disks.

Cause

This failure occurs when you migrate from a larger disk size to a smaller disk size.

Solution

Deploy a VM for the restore from an OVA template that has 2 virtual disks.



CHAPTER 33

Bulk Administration of Contact Lists

Bulk Administration Overview

With the IM and Presence Service Bulk Administration Tool, you can perform bulk transactions on many IM and Presence Service users, including:

- Rename User Contact IDs for use in the Microsoft migration process.
- Export the contact lists, non-presence contact lists, and location details of users who belong to a particular node or presence redundancy group, to a CSV data file.

Note Non-presence contacts are contacts who do not have an IM address and can only be exported using this procedure.

- You can import user contacts lists, non-presence contact lists, and user location migration details you had exported to another node or presence redundancy group in a different cluster. Prepopulate contact lists for new users or add to existing contact lists.
- These features facilitate the migration of users between clusters.

Bulk Administration Prerequisites

Before importing your user contact lists:

1. Provision the users on Cisco Unified Communications Manager.
2. Ensure that the users are licensed on Cisco Unified Communications Manager for the IM and Presence Service.

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.

Bulk Administration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Bulk Rename User Contact IDs, on page 366	Upload the CSV file and rename the contact IDs for a list of users.
Step 2	Bulk Export User Contact Lists and Non-Presence Contact Lists, on page 367	Use this procedure to export your users' contact lists to a CSV file. You can then use Bulk Administration to move user contact lists to another node or cluster.
Step 3	Bulk Export User Location Details , on page 368	Use this procedure to export user location details to a CSV file. You can then use Bulk Administration to move user location details lists to another node or cluster.
Step 4	Carry out these tasks to import your user contact lists into IM and Presence Service: • Verify Maximum Contact List Size, on page 371 • Upload Input File, on page 372 • Create New Bulk Administration Job, on page 376 • Check Results of Bulk Administration Job, on page 377	

Bulk Rename User Contact IDs

Caution Bulk rename of contact IDs is used in the migration of users from a Microsoft server (for example Lync) to IM and Presence Service Service. See the Partitioned Intradomain Federation Guide on Cisco.com for detailed instructions on how this tool should be used as part of the user migration process. Using this tool in any other circumstances is not supported.

Upload the CSV file and rename the contact IDs for a list of users.

Procedure

Step 1 Upload the CSV file with the list of contact IDs that you want to rename in all contact lists:

a) Go to the IM and Presence Service database publisher node.
b) In **Cisco Unified CM IM and Presence Administration**, choose **Bulk Administration** > **Upload/Download Files.**.
c) Click **Add New**.
d) Click **Browse** to locate and choose the CSV file. For more on the input file, see Bulk Rename User Contact IDs File Details, on page 367.
e) Choose **Contacts** as the Target.
f) Choose **Rename Contacts – Custom File** as the Transaction Type.
g) Click **Save** to upload the file.

Step 2 In **Cisco Unified CM IM and Presence Administration** on the publisher node, choose **Bulk Administration** > **Contact List** > **Rename Contacts**.

Step 3 In the **File Name** field, choose the file that you uploaded.

Step 4 Choose one of the following actions:

- Click **Run Immediately** to execute the Bulk Administration job immediately.
- Click **Run Later** to schedule a time to execute the Bulk Administration job. For more information about scheduling jobs in the Bulk Administration Tool, see the Online Help in Cisco Unified CM IM and Presence Administration.

Step 5 Click **Submit**.

If you chose to run the job immediately, the job runs after you click Submit.

What to do next

Bulk Export User Contact Lists and Non-Presence Contact Lists, on page 367

Bulk Rename User Contact IDs File Details

The file that you upload before you can run this job must be a CSV file with the following format:

<Contact ID>, <New Contact ID>

where <Contact ID> is the existing contact ID and <New Contact ID> is the new format of the contact ID.

<Contact ID> is the user's IM address as it appears on the **Presence Topology User Assignment window**.

The following is a sample CSV file with one entry:

```
Contact ID, New Contact ID
john.smith@example.com, jsmith@example.com
```

Bulk Export User Contact Lists and Non-Presence Contact Lists

Use this procedure to export your users' contact lists to a CSV file. You can then use Bulk Administration to move user contact lists to another node or cluster.

- Contact Lists—This list consists of IM and Presence contacts. Contacts whom do not have an IM address will not be exported (you must export a non-presence contact list).
- Non-presence Contact Lists—This list consists of contacts whom do not have an IM address.

Procedure

Step 1 From Cisco Unified CM IM and Presence Administration, do either of the following:

- To export Contact Lists, choose **Bulk Administration** > **Contact List** > **Export Contact List**
- To export Non-presence Contact Lists, choose **Bulk Administration** > **Non-presence Contact List** > **Export Non-presence Contact List** and skip the next step.

Step 2 Contact Lists only. Select the users for whom you will export contact lists:

a) Under **Export Contact List Options**, choose the category of users for whom you will export contact lists. The default is to export contact lists for all users.
b) Click **Find** to bring up the list of users and then click **Next**.

Step 3 In the **File Name** field, enter a name for the CSV file.

Step 4 Under **Job Information**, configure when you want to run this job:

- **Run Immediately**—Check this button to export contact lists right away.
- **Run Later**—Check this button if you want to schedule a time for the job. With this option, you will need to use the Job Scheduler page at **Bulk Administration** > **Job Scheduler** to schedule a time for this job to run.

Step 5 Click **Submit**.
If you choose **Run Immediately**, the export job runs right away.

Step 6 After the export file is created, download the exported file:

a) From Cisco Unified CM IM and Presence Administration, choose **Bulk Administration** > **Upload/Download Files**.
b) Click **Find** and select the export file.
c) Click **Download Selected** and download the file to a location you can access.

Bulk Export User Location Details

Use this procedure to export user location details to a CSV file. You can then use Bulk Administration to move user location details to another node or cluster.

Procedure

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Bulk Administration** > **User Location Migration** > **Export User Location Details**.

Step 2 Under, **User Location Details Export**, in the **File Name** field, enter a name for the CSV file.

Step 3 Under **Job Information**, configure when you want to run this job:

- **Run Immediately**—Check this button to export user location details immediately.

- **Run Later**—Check this button if you want to schedule a time for the job. With this option, you will need to use the **Job Scheduler** page in **Bulk Administration** > **Job Scheduler** to schedule a time for this job to run.

Step 4 Click **Submit**.
If you choose **Run Immediately**, the export job is executed immediately.

Step 5 After the export file is created, download the exported file:

a) From Cisco Unified CM IM and Presence Administration, choose **Bulk Administration** > **Upload/Download Files**.
b) Click **Find** and select the export file.
c) Click **Download Selected** and download the file to a location you can access.

File Details for Export Contact Lists

The following is a sample CSV file entry:

```
userA,example.com,userB,example.com,buddyB,General,0
```

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>,<State>
```

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.
State	The state of the rosters, the roster database stores it in decimal format.

File Details for Export Non-Presence Contact Lists

The non-presence user contact lists are exported to a CSV file with the following format:

```
<User JID>,<Contact JID>,<Group Name>,<Content Type>,<Version>,<Info>
```

The following table describes the parameters in the export file:

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 textmime 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.

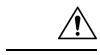
The following is a sample CSV file entry:

```
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
```

File Details for Export User Location Details

The user location details are exported to a CSV file with the following format:

```
<User JID>,<Access Type>,<Create Time>,<Item ID>,<Resource ID>,<Message Text>
```



Caution We recommend that you do not manually modify the exported CSV file, due to the size of the file itself and the risk of corrupting the user location information.

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.
Access Type	The Access Type defines the access type of the user. The values for access type are as follows: • W: white list • R: roster groups • O: open **Note** Use 'W' for Jabber.
Create Time	The Create Time shows the date and time the item was created or updated.
Item ID	The Item ID identifies a particular record for a user.
Resource ID	The Resource ID is the Jabber Instance ID.
Message Text	The Message Text is the location information of the user.

The following is a sample CSV file entry:

```
userA@example.com,W,2021-01-22
10:11:18.000001,7d0ec34c-458f-4fd2-9d15-58accac4af00,jabber_7151,

<geoloc
xmlns='http://jabber.org/protocol/geoloc'><description>newlocation104</description><street>104</street><mobile>0</mobile><enable>1</enable></geoloc>
```

Bulk Import Of User Contact Lists

Verify Maximum Contact List Size

Check the Maximum Contact List Size and Maximum Watchers settings on IM and Presence Service. The system default value is 200 for Maximum Contact List Size and 200 for Maximum Watchers.

Cisco recommends that you set the Maximum Contact List Size and Maximum Watchers settings to Unlimited while importing user contact lists. Even though o exceed the maximum contact list size without losing data when importing contact lists using BAT, this step ensures that each migrated user contact list is fully imported. After all users have migrated, you can reset the Maximum Contact List Size and Maximum Watchers settings to the preferred values.

You only need to check the maximum contact list size on those clusters that contain users for whom you wish to import contacts. When you change Presence settings, the changes are applied to all nodes in the cluster; therefore you only need to change these settings on the IM and Presence database publisher node within the cluster.

What to do next

Upload Input File, on page 372

Upload Input File

The following procedure describes how to upload the CSV input file using BAT for contact lists and non-presence contact lists.

Before you begin

Verify Maximum Contact List Size, on page 371

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **Bulk Administration** > **Upload/Download Files**.

Step 2 Click **Add New**.

Step 3 Click **Browse** to locate and choose the CSV file.

Step 4 For the Target setting:

- If you want to upload an input file for contact lists, choose **Contact Lists**. For more on user contact list input files, see File Details for Import Contact Lists, on page 372.
- If you want to upload an input file for non-presence contact lists, choose **Non-presence Contact Lists**. For more on non-presence user contact list input files, see File Details for Import Non-Presence Contact Lists, on page 374.
- If you want to upload an input file for user location migration details, choose **User Location Migration**. For more on user location details input files, see File Details for Import User Location Details, on page 375.

Step 5 For the Transaction Type: Choose as the Transaction Type.

- If you want to upload an input file for contact lists, choose **Import Users' Contacts – Custom File**
- If you want to upload an input file for non-presence contact lists, choose **Import Users' Non Presence Contacts**
- If you want to upload an input file for user location migration details, choose **Import User Location Details**

Step 6 Click **Save** to upload the file.

What to do next

Create New Bulk Administration Job, on page 376

File Details for Import Contact Lists

The input file must be a CSV file in the following format:

```
<User ID>,<User Domain>,<Contact ID>,<Contact Domain>,<Nickname>,<Group Name>,<State>
```

The following is a sample CSV file entry:

```
userA,example.com,userB,example.com,buddyB,General,0
```

The following table describes the parameters in the input file.

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. • JSM session will not be created for User ID containing the following characters: º ª ² ¼ ¾ - ³ µ ¹ ½ ß ´ ¸ , – Æ
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.

Parameter	Description
Contact ID	This is a mandatory parameter. The user ID of the contact list entry. It can have a maximum of 132 characters.
Contact Domain	This is a mandatory parameter. The Presence domain of the contact list entry. The following restrictions apply to the format of the domain name: • Length must be less than or equal to 128 characters • Contains only numbers, upper- and lowercase letters, and hyphens (-) • Must not start or end with hyphen (-) • Length of label must be less than or equal to 63 characters • Top-level domain must be characters only and have at least two characters
Nickname	The nickname of the contact list entry. It can have a maximum of 255 characters.
Group Name	Group Name 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.
State	The state of the rosters, the roster database stores it in decimal format.

File Details for Import Non-Presence Contact Lists

The input file must be a CSV file in the following format:

```
<User JID>,<Contact JID>,<Group Name>,<Content Type>,<Version>,<Info>
```

The following is a sample CSV file entry:

```
user2@cisco.com,ce463d44-02c3-4975-a37f-d4553e3f17e1,group01,text/directory,3,BEGIN:VCARD
ADR;TYPE=WORK:ADR\;WORK:\;\;123 Dublin rd\,\;Oranmore\;Galway\;\;Ireland
EMAIL;TYPE=X-CUSTOM1;X LABEL=Custom:testuser01@test.com N: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:

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 textmime 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.

File Details for Import User Location Details

The input file must be a CSV file in the following format:

```
<User JID>,<Access Type>,<Item ID>,<Create Time>,<Resource ID>,<Message Text>
```

The following is a sample CSV file entry:

```
userA@example.com,W,7d0ec34c-458f-4fd2-9d15-58accac4af00,2021-01-22
10:11:18.000001,jabber_7151,
```

```
<geoloc
xmlns='http://jabber.org/protocol/geoloc'><description>newlocation104</description><street>104</street><mobile>0</mobile><enable>1</enable></geoloc>
```

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 user location information.

The following table describes the parameters in the input file for user location migration:

Parameter	Description
User JID	This is a mandatory parameter. The User JID is the IM address of the user. It can have a maximum 255 characters.
Access Type	This is a mandatory parameter.The Access Type defines the access type of the user. It can have a maximum of 128 characters. The values for access type are as follows: • W: white list • R: roster groups • O: open **Note** Use 'W' for Jabber.

Parameter	Description
Item ID	This is a mandatory parameter. The Item ID identifies a particular record for a user. The value of Item ID should be 'Ignore' or an alphanumeric value. The user ID of the contact list entry. It can have a maximum of 50 characters.
Create Time	This is a mandatory parameter. The Create Time shows the date and time the item was created or updated. It can have a maximum of 26 characters.
Resource ID	This is a mandatory parameter. The Resource ID is the Jabber Instance ID. It can have a maximun of 1023 characters.
Message Text	This is a mandatory parameter. The Message Text is the location information of the user. It can have a maximum of 30000 characters.

Create New Bulk Administration Job

Create a new bulk administration job for contact lists and non-presence contact lists.

Before you begin

Upload Input File, on page 372

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**:

- If you want to create a new bulk administration job for contact lists, choose **Bulk Administration** > **Contact List** > **Update**
- If you want to create a new bulk administration job for contact lists, choose **Bulk Administration** > **Contact Non-presence List** > **Import Non-presence Contact List**.
- If you want to create a new bulk administration job for user location migration, choose **Bulk Administration** > **User Location Migration** > **Import User Location Details**.

Step 2 From the File Name drop-down list, choose the file to import.

Step 3 In the Job Description field, enter a description for this Bulk Administration job.

Step 4 Choose one of the following:

- Click **Run Immediately** to execute the Bulk Administration job immediately.
- Click **Run Later** to schedule a time to execute the Bulk Administration job. For more information about scheduling jobs in BAT, see the Online Help in Cisco Unified CM IM and Presence Administration.

Step 5 Click **Submit**. If you chose to run the job immediately, the job runs after you click Submit.

What to do next

Check Results of Bulk Administration Job, on page 377

Check Results of Bulk Administration Job

When the Bulk Administration job is complete, the IM and Presence Service BAT tool writes the results of the contact list import job to a log file. The log file contains the following information:

- The number of contacts that were successfully imported.
- The number of internal server errors that were encountered while trying to import the contacts.
- The number of contacts that were not imported (ignored). The log file lists a reason for each ignored contact at the end of the log file. The following are the reasons for not importing a contact:
  - Invalid format - invalid row format, for example, a required field is missing or empty
  - Invalid contact domain - the contact domain is in an invalid format. See topics related to bulk import of user contact lists for the valid format of the contact domain
  - Cannot add self as a contact - you cannot import a contact for a user if the contact is the user
  - User's contact list is over limit - the user has reached the maximum contact list size and no more contacts can be imported for that user
  - User is not assigned to local node - the user is not assigned to the local node
- The number of contacts in the CSV file that were unprocessed due to an error that caused the BAT job to finish early. This error rarely occurs.

Complete the following procedure to access this log file.

Before you begin

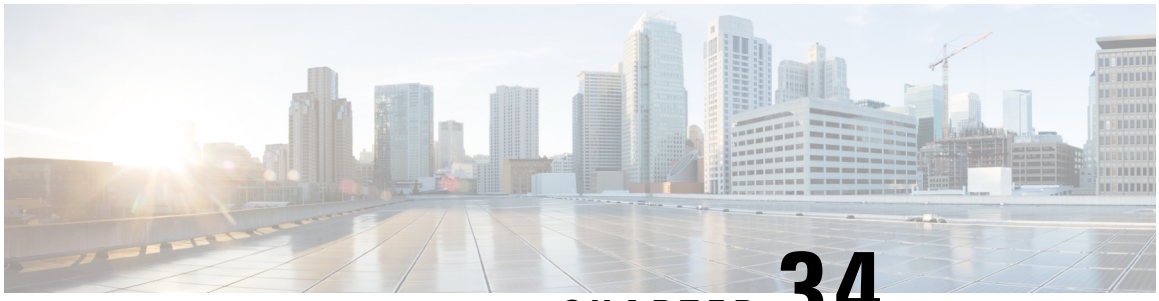
Create New Bulk Administration Job, on page 376

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **Bulk Administration** > **Job Scheduler**.

Step 2 Click **Find** and choose the job ID of the contact list import job.

Step 3 Click the **Log File Name** link to open the log.



CHAPTER 34

Troubleshoot the System

Troubleshooting Overview

Use the procedures in this chapter to troubleshoot issues with your IM and Presence deployment. With your IM and Presence Service deployment, you can:

- Use the Command Line Interface (CLI) to build trace logs that you can use to check to resolve issues.
- Run diagnostics, to check for issues with your system.
- Run the system troubleshooter to confirm the health of your system.
- Troubleshoot duplicate directory URI issues.

Run the System Troubleshooter

Run the troubleshooter to diagnose issues with your IM and Presence Service deployment. The troubleshooter checks automatically for a wide range of issues with your deployment including:

- System Issues
- Sync Agent Issues
- Presence Engine Issues
- SIP Proxy Issues
- Calendaring Issues
- Inter-clustering Issues
- Topology Issues
- Cisco Jabber Redundancy Assignments

- External Database entries
- Third-Party Compliance Server
- Third-Party LDAP Connection
- LDAP Connection
- XCP Staus
- User Configuration

Procedure

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Diagnostics** > **System Troubleshooter**. The troubleshooter runs a series of automated checks against your system. The results display in the **System Configuration Troubleshooter** window.

Step 2 Resolve any issues that the troubleshooter highlights.

Run Diagnostics

When administering an up and running system, you may encounter problems which affect the normal running of the system. You can use the IM and Presence Service Diagnostic tools to help determine the root causes of these problems.

Use this procedure to access the Diagnostic tools on IM and Presence Service.

These tools can be accessed in **Cisco Unified CM IM and Presence Administration** by clicking **Diagnostics** and choosing from one of these options:

Procedure

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

Step 2 Click the Diagnostic tool you want to use from the drop-down list.

See Diagnostic Tools Overview for more on the purpose of these tools.

Diagnostic Tools Overview

Diagnostic Tool	Purpose
System Dashboard	Use the System Dashboard to acquire a snapshot of the state of your IM and Presence Service system including a summary data view of these system components - number of devices, number of users, per-user data such as contacts, and primary extension.
System Configuration Troubleshooter	Use the System Configuration Troubleshooter to diagnose IM and Presence Service configuration issues after your initial configuration or whenever you make configuration changes. The Troubleshooter performs a set of tests on both the IM and Presence Service cluster and on the Cisco Unified Communications Manager cluster to validate the IM and Presence Service configuration. After the Troubleshooter finishes testing, it reports one of three possible states for each test: • Test Passed • Test Failed • Test Warning, which indicates a possible configuration issue For each test that fails or that results in a warning, the Troubleshooter provides a description of the problem and a possible solution. For any test failures or test warnings, click the fix link in the solution column to go to the Cisco Unified Communications Manager IM and Presence Administration window where the Troubleshooter found the problem. Correct any configuration errors that you find and rerun the Troubleshooter.

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 47: 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 384 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 384 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 384 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 384 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 384 for CLI commands to build logs and output locations.

Issues with...	View Traces for These Services	Additional Instructions
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 384 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 384 for CLI commands to build logs and output locations. Perform trace on each IM and Presence node on which XMPP Federation is enabled
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 384 for CLI commands to build logs and output locations.
Calendaring Traces	Cisco Presence Engine	See Common Traces via CLI, on page 384 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 384 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 384 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 388.

Table 48: 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 49: 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
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 384 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 384.

Table 50: 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

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
```

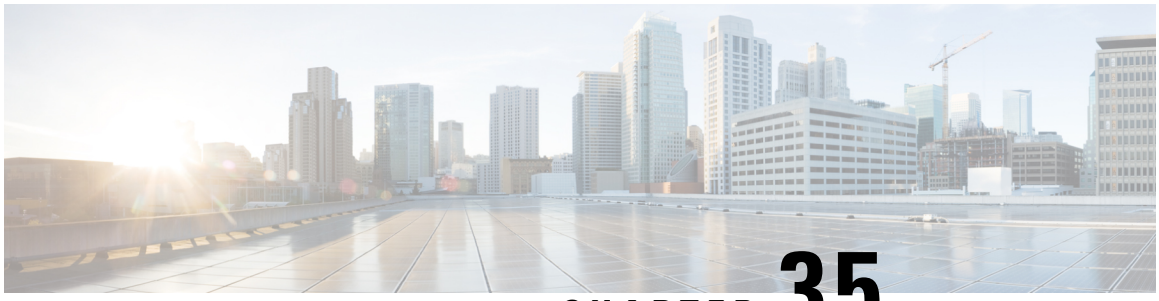
2. If the same user is assigned to two different clusters, then unassign the user from one of the clusters.
3. If different users on different clusters have the same Directory URI value assigned to them, then rename the Directory URI value for one of the users to ensure there is no longer any duplication.
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.

PART V

Reference Information



CHAPTER 35

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 51: Intracluster Ports Between Cisco Unified Communications Manager Servers

From (Sender)	To (Listener)	Destination Port	Purpose
Endpoint	Unified Communications Manager	514 / UDP	System logging se
Endpoint	Unified Communications Manager	514 / UDP	System logging se
Unified Communications Manager	Unified Communications Manager	443 / TCP	This port is used f communication be subscriber and pul COP file installati subscriber node.
Unified Communications Manager	RTMT	1090, 1099 / TCP	Cisco AMC Servi performance mon collection, logging
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1500, 1501 / TCP	Database connecti TCP is the second connection)

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1510 / TCP	CAR IDS DB. CAR I listens on waiting for c requests from the clie
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1511 / TCP	CAR IDS DB. An alte used to bring up a sec instance of CAR IDS upgrade.
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1515 / TCP	Database replication l nodes during installat
Cisco Extended Functions (QRT)	Unified Communications Manager (DB)	2552 / TCP	Allows subscribers to Cisco Unified Commu Manager database cha notification
Unified Communications Manager	Unified Communications Manager	2551 / TCP	Intracluster communi between Cisco Exten Services for Active/B determination
Unified Communications Manager (RIS)	Unified Communications Manager (RIS)	2555 / TCP	Real-time Information (RIS) database server
Unified Communications Manager (RTMT/AMC/SOAP)	Unified Communications Manager (RIS)	2556 / TCP	Real-time Information (RIS) database client 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 S monitor for Real Tim Monitoring Service.
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5002/TCP	This port is used by S monitor for Performa Monitor Service.
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5003/TCP	This port is used by S monitor for Control C Service.
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5004/TCP	This port is used by S monitor for Log Colle Service.
Standard CCM Admin Users / Admin	Unified Communications Manager	5005 / TCP	This port is used by S CDROnDemand2 ser

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5007 / TCP	SOAP monitor
Unified Communications Manager (RTMT)	Unified Communications Manager (TCTS)	Ephemeral / TCP	Cisco Trace Colle Service (TCTS) -- service for RTMT Log Central (TLC
Unified Communications Manager (Tomcat)	Unified Communications Manager (TCTS)	7000, 7001, 7002 / TCP	This port is used f communication be Trace Collection T and Cisco Trace C servlet.
Unified Communications Manager	Certificate Manager	7070 / TCP	Certificate Manag
Unified Communications Manager (DB)	Unified Communications Manager (CDLM)	8001 / TCP	Client database ch notification
Unified Communications Manager (SDL)	Unified Communications Manager (SDL)	8002 / TCP	Intracluster comm service
Unified Communications Manager (SDL)	Unified Communications Manager (SDL)	8003 / TCP	Intracluster comm service (to CTI)
Unified Communications Manager	CMI Manager	8004 / TCP	Intracluster comm between Cisco Un Communications CMI Manager
Unified Communications Manager (Tomcat)	Unified Communications Manager (Tomcat)	8005 / TCP	Internal listening Tomcat shutdown
Unified Communications Manager (Tomcat)	Unified Communications Manager (Tomcat)	8080 / TCP	Communication be used for diagnosti
Gateway	Unified Communications Manager	8090	HTTP Port for co between CuCM a (Cayuga interfae) Recording feature
Unified Communications Manager	Gateway		
Unified Communications Manager (IPSec)	Unified Communications Manager (IPSec)	8500 / TCP and UDP	Intracluster replic system data by IP Manager
Unified Communications Manager (RIS)	Unified Communications Manager (RIS)	8888 - 8889 / TCP	RIS Service Mana request and reply
Location Bandwidth Manager (LBM)	Location Bandwidth Manager (LBM)	9004 / TCP	Intracluster comm between LBMs

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager [Dialed Number Analyzer (DNA) initializing server]	JNIWrapper server	30000 / TCP	Dialed Number Analy (DNA) Port used by the serv handles DNA initializ JNIWrapper function to requests that the D service sends.
Unified Communications Manager Publisher	Unified Communications Manager Subscriber	22 / TCP	Cisco SFTP service. open this port when i new subscriber.
Unified Communications Manager	Unified Communications Manager	8443 / TCP	Allows access to Cont - Feature and Networ between nodes.

Common Service Ports

Table 52: 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, Call Detail Record)	SFTP server	22 / TCP	Send the backup data to SFTP server. (DRS Local Agent) Send the Call Detail Record data to SFTP server.

From (Sender)	To (Listener)	Destination Port	Purpose
Endpoint	Unified Communications ManagerDNS Server)	Ephemeral / UDP	Cisco Unified Communications Manager acting as a DNS server or DNS client **Note** Cisco recommends that Cisco Unified Communications Manager not act as a DNS server and that all IP telephony applications and endpoints use static IP addresses instead of hostnames.
Unified Communications Manager	DNS 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.)
Endpoint or Gateway	Unified Communications Manager	69, 6969, then Ephemeral / UDP	TFTP service to phones and gateways

From (Sender)	To (Listener)	Destination Port	Purpose
Endpoint or Gateway	Unified Communications Manager	6970 / TCP	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	built-in 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
Unified Communications Manager	Unified Communications Manager	6666 / UDP	Netdump server
Centralized TFTP	Alternate TFTP	6970 / TCP	Centralized TFTP File Locator Service
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

From (Sender)	To (Listener)	Destination Port	Purpose
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.
Unified Communications Manager	Unified Communications Manager	9966	Used by Cisco push notification service to communicate between the nodes in the cluster when firewall is enabled.
Unified Communications Manager	Unified Communications Manager	9560	Used by Local Push Notification Service (LPNS).
--	--	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 53: 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 54: 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 P (HTTP)
Browser	Unified Communications Manager	443, 8443 / TCP	Hypertext Transport P over SSL (HTTPS)
Browser	Unified Communications Manager	9463 / TCP	Hypertext Transport P over SSL (HTTPS) al TLS1.3 with v6.
Browser or CLI	Unified Communications Manager	2355, 2356 / TCP	Log audit events from and Web applications
Unified Communications Manager	Cisco License Manager	5555 / TCP	Cisco License Manag for license requests o

Web Requests From Cisco Unified Communications Manager to Phone

Table 55: 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 Transp (HTTP)

Signaling, Media, and Other Communication Between Phones and Cisco Unified Communications Manager

Table 56: Signaling, Media, and Other Communication Between Phones and Cisco Unified Communications Manager

From (Sender)	To (Listener)	Destination Port	Purpose
Phone	DNS server	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)

From (Sender)	To (Listener)	Destination Port	Purpose
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
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, and so on. 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	Phones use this port number to use the Headset Management feature.
iPhone/iPad (Webex App)	Unified Communications Manager	9560/Secure WebSocket	Webex App uses this port number for the LPNS feature.

From (Sender)	To (Listener)	Destination Port	Purpose
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 57: 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 E (GRE), Encapsula Payload (ESP), A Header (AH). The numbers carry enc traffic. They do no port as indicated i heading.
Unified Communications Manager	Gateway		
Gateway	Unified Communications Manager	500 / UDP	Internet Key Exch for IP Security pro establishment
Unified Communications Manager	Gateway		
Gateway	Unified Communications Manager (TFTP)	69, then Ephemeral / UDP	Trivial File Transf (TFTP)
Unified Communications Manager with Cisco Intercompany Media Engine (CIME) trunk	CIME ASA	1024-65535 / TCP	Port mapping serv in the CIME off-p deployment mode
Gatekeeper	Unified Communications Manager	1719 / UDP	Gatekeeper (H.22

From (Sender)	To (Listener)	Destination Port	Purpose
Gateway	Unified Communications Manager	1720 / TCP	H.225 signaling servi H.323 gateways and I Trunk (ICT)
Unified Communications Manager	Gateway		
Gateway	Unified Communications Manager	Ephemeral / TCP	H.225 signaling servi gatekeeper-controlled
Unified Communications Manager	Gateway		
Gateway	Unified Communications Manager	Ephemeral / TCP	H.245 signaling servi establishing voice, vi data **Note** The H.24 used by t system d the type gateway. For IOS g the H.24 range is 11000 to
Unified Communications Manager	Gateway		
Gateway	Unified Communications Manager	2000 / TCP	Skinny Client Contro (SCCP)
Gateway	Unified Communications Manager	2001 / TCP	Upgrade port for 6608 with Cisco Unified Communications Ma deployments
Gateway	Unified Communications Manager	2002 / TCP	Upgrade port for 6624 with Cisco Unified Communications Ma deployments
Gateway	Unified Communications Manager	2427 / UDP	Media Gateway Cont Protocol (MGCP) ga control
Gateway	Unified Communications Manager	2428 / TCP	Media Gateway Cont Protocol (MGCP) ba

From (Sender)	To (Listener)	Destination Port	Purpose
--	--	4000 - 4005 / TCP	These ports are us Real-Time Transp (RTP) and Real-T Control Protocol for audio, video a channel when Cis Communications not have ports for
Gateway	Unified Communications Manager	5060 / TCP and UDP	Session Initiation gateway and Inter (ICT)
Unified Communications Manager	Gateway		
Gateway	Unified Communications Manager	5061 / TCP	Secure Session In Protocol (SIPS) g Intercluster Trunk
Unified Communications Manager	Gateway		
Gateway	Unified Communications Manager	16384 - 32767 / UDP	Real-Time Protoc Secure Real-Time (SRTP) **Note** Cisco Comm Mana 2457 altho devic full r
Unified Communications Manager	Gateway		

Communication Between Applications and Cisco Unified Communications Manager

Table 58: 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 L provider listening Cisco Unified Co Manager
Cisco Unified Communications App	Unified Communications Manager	2748 / TCP	CTI application s

From (Sender)	To (Listener)	Destination Port	Purpose
Cisco Unified Communications App	Unified Communications Manager	2749 / TCP	TLS connection betw applications (JTAPI/T CTIManager
Cisco Unified Communications App	Unified Communications Manager	2789 / TCP	JTAPI application ser
Unified Communications Manager Assistant Console	Unified Communications Manager	2912 / TCP	Cisco Unified Commu Manager Assistant se (formerly IPMA)
Unified Communications Manager Attendant Console	Unified Communications Manager	1103 -1129 / TCP	Cisco Unified Commu Manager Attendant C (AC) JAVA RMI Reg server
Unified Communications Manager Attendant Console	Unified Communications Manager	1101 / TCP	RMI server sends RM messages to clients o ports.
Unified Communications Manager Attendant Console	Unified Communications Manager	1102 / TCP	Attendant Console (A server bind port -- RM sends RMI messages ports.
Unified Communications Manager Attendant Console	Unified Communications Manager	3223 / UDP	Cisco Unified Commu Manager Attendant C (AC) server line state receives ping and reg message from, and se states to, the attendan server.
Unified Communications Manager Attendant Console	Unified Communications Manager	3224 / UDP	Cisco Unified Commu Manager Attendant C (AC) clients register AC server for line an state information.
Unified Communications ManagerAttendant Console	Unified Communications Manager	4321 / UDP	Cisco Unified Commu Manager Attendant C (AC) clients register server for call control
Unified Communications Manager with SAF/CCD	IOS Router running SAF image	5050 / TCP	Multi-Service IOS Ro running EIGRP/SAF

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 use communicate to t Intercompany Me server.
Cisco Unified Communications App	Unified Communications Manager	8443 / TCP	AXL / SOAP API programmatic rea writes to the Cisc Communications database that thir as billing or telep management appl

Communication Between CTL Client and Firewalls

Table 59: Communication Between CTL Client and Firewalls

From (Sender)	To (Listener)	Destination Port	Purpose
CTL Client	TLS Proxy Server	2444 / TCP	Certificate Trust L provider listening ASA firewall

Communication Between Cisco Smart Licensing Service and Cisco Smart Software Manager

Cisco Smart Licensing Service in Unified Communications Manager sets up direct communication with Cisco Smart Software Manager through Call Home.

Table 60: Communication Between Cisco Smart Licensing Service and Cisco Smart Software Manager

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager (Cisco Smart Licensing Service)	Cisco Smart Software Manager (CSSM)	443 / HTTPS	Smart Licensing Service sends the license usage to CSSM to check whether Unified CM is a complaint or not.

Special Ports on HP Servers

Table 61: Special Ports on HP Servers

From (Sender)	To (Listener)	Destination Port	Purpose
Endpoint	HP SIM	2301 / TCP	HTTP port to HP age
Endpoint	HP SIM	2381 / TCP	HTTPS port to HP ag
Endpoint	Compaq Management Agent	25375, 25376, 25393 / UDP	COMPAQ Managem extension (cmaX)
Endpoint	HP SIM	50000 - 50004 / TCP	HTTPS port to HP SI

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

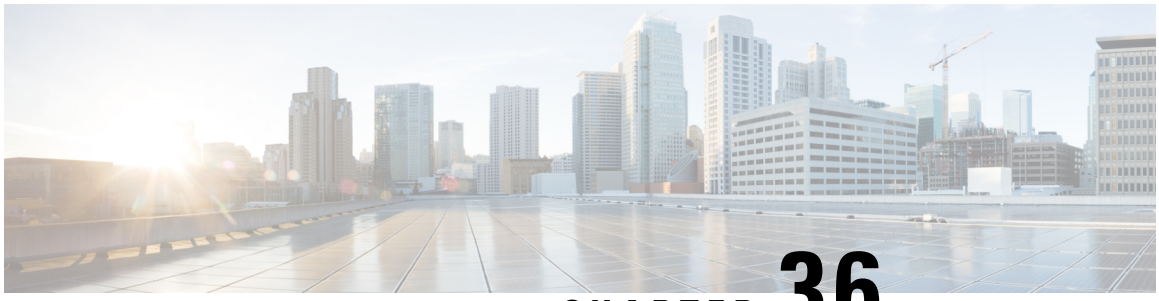
http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e30.html

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 36

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 62: 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 63: 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 64: 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 65: 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
Browser	IM and Presence	HTTPS	TCP	9463	Ephemeral	Hypertext Transport Protocol over SSL(HTTPS) allows only TLS1.3 with v6.

Table 66: 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 67: 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 68: 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 69: 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 70: 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 71: 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 72: 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 73: 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

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
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
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 74: 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 KeyManagement Protocol

Table 75: 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 76: 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 77: 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 78: 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 79: 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 80: 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 81: 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 82: 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 83: 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 84: IM and Presence Service Ports - External Database Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence	PostgreSQL database	TCP	TCP	5432[1]	Ephemeral	PostgreSQL database listening port
IM and Presence	Oracle database	TCP	TCP	1521	Ephemeral	Oracle database listening port
IM and Presenc	MSSQL database	TCP	TCP	1433	Ephemeral	MSSQL database listening port

[1] This is the default port, however you can configure the PostgreSQL database to listen on any port.

Table 85: 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 86: 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 87: 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 88: 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 89: 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.

Table 90: IM and Presence Service Ports - ICMP Requests

From (Sender)	To (Listener)	Destination Port	Purpose
Endpoint/IM and Presence	IM and Presence	7	Internet Control M Protocol (ICMP) number carries ec traffic. It does not port as indicated i heading.
IM and Presence	Endpoint/IM and Presence		

Table 91: Ports used for IM and Presence - Cisco Unified CM communication and IM and Presence Publisher - Subscriber communication

From (Sender)	To (Listener)	Transport Protocol	Destination / Listener	Source / Sender	Remarks
Cisco Unified Communications Manager	IM and Presence Publisher	TCP	1500	Bi-directional	Internal ID port for Database clients. Localhost traffic only.
Cisco Unified Communications Manager	IM and Presence Publisher	TCP	8443	Bi-directional	Provides access to Web administration.
Cisco Unified Communications Manager	IM and Presence Publisher	TCP	1090	Bi-directional	AMC RMI Object port. Cisco AMC Service for RTMT performance monitors, data collection, logging, and alerting.
Cisco Unified Communications Manager	IM and Presence Publisher	TCP	2555	Bi-directional	Bi-directional Real-time Information Services (RIS) database server. Connects to other RISDC services in the cluster to provide clusterwide real-time information.
Cisco Unified Communications Manager	IM and Presence Publisher	TCP	8500	Bi-directional	Internal port - cluster manager port used by the ipsec_mgr daemon for cluster replication of platform data (hosts) certificates.
Cisco Unified Communications Manager	IM and Presence Publisher	TCP	8600	Bi-directional	Config Agent heartbeat port
Cisco Unified Communications Manager	IM and Presence Publisher	UDP	123	Bi-directional	Network Time Protocol(NTP) used for time synchronization.

From (Sender)	To (Listener)	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence Publisher	IM and Presence Subscriber	UDP	50000	Bi-directional	Internal port. Localhost traffic only. LiveBus messaging port. TheIM and PresenceService uses this port for cluster communication.
IM and Presence Publisher	IM and Presence Subscriber	UDP	21999	Bi-directional	The port that Cisco Server Recovery Manager uses to communicate with its peer.
IM and Presence Publisher	Cisco Unified Communications Manager	TCP	4040	Bi-directional	DRF Master Agent server port that accepts connections from Local Agent, GUI, and CLI.
IM and Presence Publisher	Cisco Unified Communications Manager	TCP	8001	Bi-directional	Used while configuring persistent chat.
IM and Presence Publisher	Cisco Unified Communications Manager	TCP	6379	Bi-directional	Used while configuring managed file transfer (MFT).
IM and Presence Publisher	IM and Presence Subscriber	TCP	7	Bi-directional	Used while configuring external database (MSSQL).
IM and Presence Publisher	IM and Presence Subscriber	TCP	20075	Bi-directional	The port that Cisco Server Recovery Manager uses to provide admin RPC requests.
IM and Presence Publisher	IM and Presence Subscriber	TCP	8600	Bi-directional	Config Agent heartbeat port
IM and Presence Subscriber	IM and Presence Publisher	TCP	9005	Bi-directional	Cisco SIP Registration Datastore dual node presence redundancy group replication.
IM and Presence Subscriber	IM and Presence Publisher	TCP	9003	Bi-directional	Cisco Presence Datastore dual node presence redundancy group replication.
IM and Presence Subscriber	IM and Presence Publisher	TCP	20075	Bi-directional	The port that Cisco Server Recovery Manager uses to provide admin RPC requests.

From (Sender)	To (Listener)	Transport Protocol	Destination / Listener	Source / Sender	Remarks
IM and Presence Subscriber	IM and Presence Publisher	TCP	9004	Bi-directional	Cisco Login Datastore dual node presence redundancy group replication.
Cisco Unified Communications Manager	IM and Presence Publisher	TCP	5070	Bi-directional	Used on a call configuration
IM and Presence Publisher	IM and Presence Subscriber	TCP	44000	Bi-directional	Used on a call configuration

Table 92: On-a-call_Presence

From (Sender)	To (Listener)	Source Port	Destination Port	Protocol	Remarks
Cisco Unified Communications Manager	IM and Presence Publisher	[37240 – 61000]	5070	TCP	
IM and Presence Publisher	XMPP client (Jabber)	5222	64846	TCP	Client Access Port
IM and Presence Publisher	XMPP client (Jabber)	5222	56361	TCP	Client Access Port

Table 93: MS-SQL DB Configuration

From (Sender)	To (Listener)	Source Port	Destination Port	Protocol
IM and Presence Publisher	Database	[37240 – 61000]	7	TCP

Table 94: MS-SQL Persistent Chat Configuration

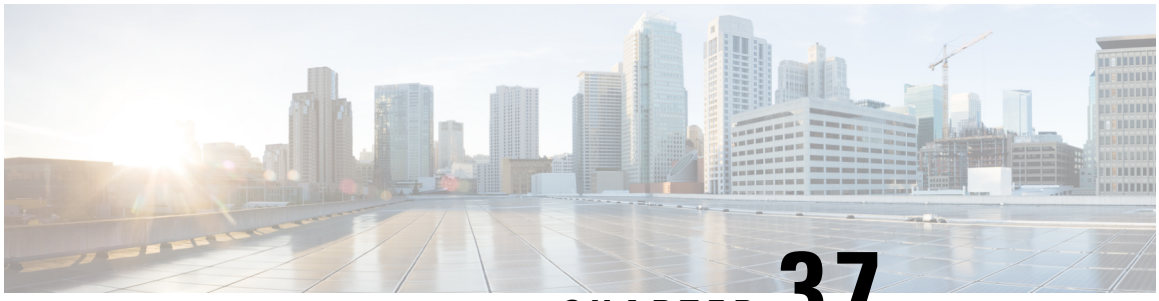
From (Sender)	To (Listener)	Source Port	Destination Port	Protocol
IM and Presence Publisher	Database	37240 – 61000	1433	TCP

Table 95: Managed File Transfer (MFT) Configuration

From (Sender)	To (Listener)	Source Port	Destination Port	Protocol
IM and Presence Publisher	External File Server	37240 – 61000	7	TCP

From (Sender)	To (Listener)	Source Port	Destination Port	Protocol
IM and Presence Publisher	External File Server	37240 – 61000	22	TCP
IM and Presence Publisher	External File Server	37240 – 61000	5432	TCP
IM and Presence Publisher	Database	54288 - 54292	5432	TCP

See the *Cisco Unified Serviceability Administration Guide* for information about SNMP.



CHAPTER 37

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 96: 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 97: 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 98: 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 99: 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 100: 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 101: 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 102: 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

Attention To achieve maximum client login throughput on a 5000 user system, Cisco recommends a minimum of 2.6GHz CPU clock speed.

Table 103: 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	154
500	120	287
1000	120	453
1500	120	620
2000	120	787
2500	120	953
3000	120	1120
3500	120	1287
4000	120	1453
4500	120	1620
5000	120	1787

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 104: 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

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
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
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 2.6GHz CPU clock speed.

Table 105: 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	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

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
4500	120	870
5000	120	953
6000	120	1120
7000	120	1287
8000	120	1453
9000	120	1620
10000	120	1787
11000	120	1953
12000	120	2120
13000	120	2287
14000	120	2453
15000	120	2620

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 106: 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

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
4000	120	564
4500	120	620
5000	120	676
6000	120	787
7000	120	898
7500	120	953
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 2.6GHz CPU clock speed.

Table 107: Login rates for active /standby profiles: 16 users 80% CPU

Expected number of Active Users	Lower Retry Limit	Upper Retry Limit
100	120	133
500	120	183
1000	120	245
1500	120	308
2000	120	370
2500	120	433
3000	120	495
3500	120	558
4000	120	620

Expected number of Active Users	Lower Retry Limit	Upper Retry Limit
4500	120	683
5000	120	745
6000	120	870
7000	120	995
8000	120	1058
9000	120	1120
10000	120	1245
11000	120	1370
12000	120	1495
13000	120	1620
14000	120	1870
15000	120	1995
16000	120	2120
17000	120	2245
18000	120	2370
19000	120	2495
20000	120	2620
21000	120	2745
22000	120	2870
23000	120	2995
24000	120	3120
25000	120	3245

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

Configurations that Require a Restart	Restart this Service
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
Message Settings Configuration (Messaging > Settings) Editing the Enable instant message Suppress offline instant messaging	Cisco XCP Router
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