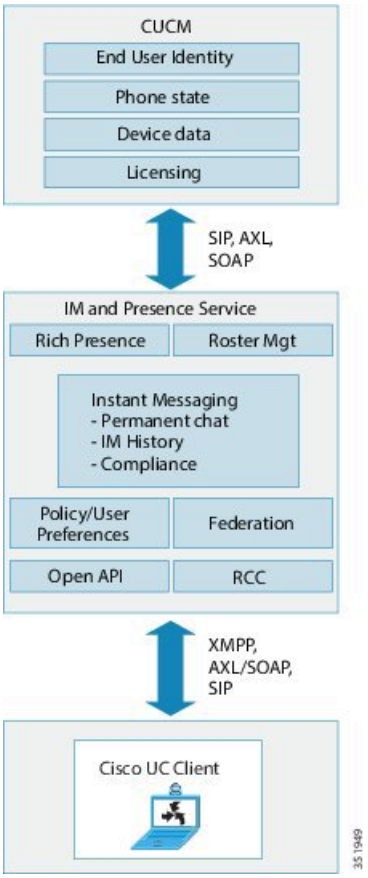
IM and Presence Service Features and Functions

IM and Presence Service Components

Main Components

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

Figure 1: IM and Presence Service Basic Deployment



SIP Interface

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

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

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

Related Topics

SIP Trunk Configuration on Cisco Unified Communications Manager
Presence Gateway Configuration Option

AXL/SOAP Interface

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

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

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

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

Related Topics

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

LDAP Interface

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

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

Related Topics

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

XMPP Interface

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

Related Topics

Configure Secure Connection Between IM and Presence Service and XMPP Clients

CTI interface

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

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

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

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

Cisco IM and Presence Data Monitor

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

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

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

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

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

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

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

- Use this CLI command:

  utils dbreplication runtimestate

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

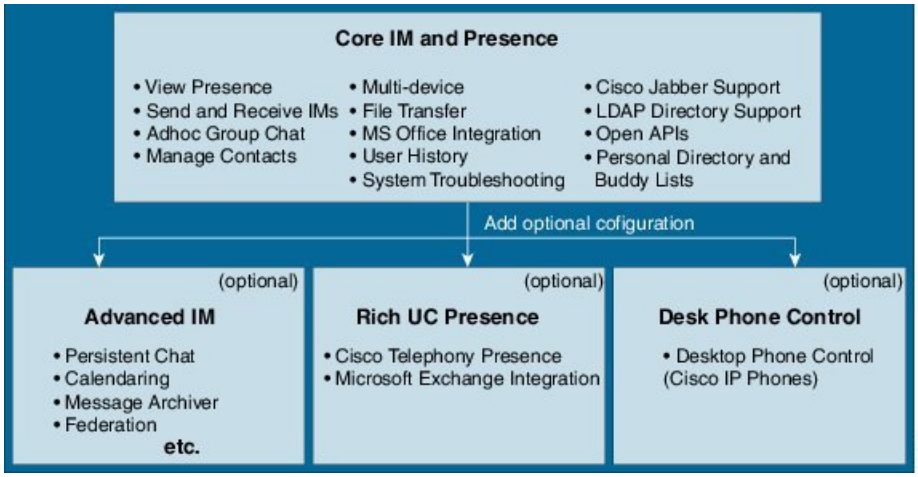
To check the status of the Cisco Sync Agent, navigate to the Cisco Unified CM IM and Presence Administration interface and select **Diagnostics** > **System Dashboard**. You will find the CUCM Publisher IP address as well as the Sync Status.

IM and Presence Service Feature Deployment Options

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

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

Figure 2: IM and Presence Service Feature Deployment Options



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

Table 1: IM and Presence Service Feature Deployment Options

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

Deployment models

IM-Only Deployment

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

Related Topics

IM-Only Deployment Workflow

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

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

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

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

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

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

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

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

Presence Redundancy Groups and High Availability

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

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

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

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

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

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

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

Clustering Over WAN

The IM and Presence Service supports Clustering over WAN deployments.

Related Topics

Clustering Over WAN for Intracluster and Intercluster Deployments

User Assignment

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

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

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

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

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

End User Management

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

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

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

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

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

Availability and Instant Messaging

Chat

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

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

Related Topics

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

IM Forking

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

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

Related Topics

Turn On or Off Offline Instant Messaging

Offline IM

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

Broadcast IM

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

Chat Rooms on IM and Presence Service

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

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

Persistent chat rooms are group chat sessions that remain in existence even when all users have left the room and do not terminate like ad hoc group chat sessions. The intent is that users will return to persistent chat

rooms over time to collaborate and share knowledge of a specific topic, search through archives of what was said on that topic (if this feature is enabled on IM and Presence Service), and then participate in the discussion of that topic in real-time. Administrators can also restrict access to persistent chat rooms so that only members of that room have access. See Configure Member Settings and IM and Presence Service Ad Hoc Group Chat Rooms Privacy Policy in the Important Notes section of the Release Notes for Cisco Unified Communications Manager and IM and Presence Service, Release 11.0(1).

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

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

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

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

Chat Room Limits

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

Table 2: Chat Room Limits for IM and Presence Service

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

File Transfer

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

Related Topics

Enable File Transfer

Important Notes About IM and Presence Service and Chat

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

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

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

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

IM Compliance

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

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

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

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

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

Presence Data Overview

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

- System Determined Presence
- Manual Presence

Manual Presence

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

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

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

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

System Determined Presence

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

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

There are four categories of System Determined Presence:

- IM Device Status

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

- Calendar Status

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

- Phone Status

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

- Third Party Application Status

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

LDAP Integrations

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

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

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

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

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

Related Topics

LDAP Directory Integration with Cisco Unified Communications Manager Task List

Third-Party Integrations

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

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

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

Third-Party Client Integration

Supported Third-Party XMPP Clients

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

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

http://developer.cisco.com/

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

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

License Requirements for Third-Party Clients

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

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

XMPP Client Integration on Cisco Unified Communications Manager

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

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

Related Topics

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

LDAP Integration for XMPP Contact Search

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

Related Topics

LDAP Directory Integration for Contact Searches on XMPP Clients

DNS Configuration for XMPP Clients

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

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

IPv6 Support

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

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

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

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

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

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

IM Address Schemes and Default Domain

The IM and Presence Service supports two IM addressing schemes:

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

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

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

IM Address Using UserID@Default_Domain

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

IM Address Using Directory URI

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

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

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

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

- Synchronize the Directory URI from the LDAP directory source.

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

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

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

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

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

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

IM Address Examples

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

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

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

IM Address Integration with Cisco Unified Communications Manager

UserID@Default_Domain Integration with Cisco Unified Communications Manager

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

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

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

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

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

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

`amckenzie@example.com@sales-example.com`. The Active Directory (AD) mapping setting that you choose is global to all users within that IM and Presence Service cluster. It is not possible to set different mappings for individual users.

Directory URI Integration with Cisco Unified Communications Manager

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

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

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

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

Multiple IM Domain Management

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

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

Security

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

For more information, see topics related to security configuration.

Single Sign-On

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

- Cisco Unified CM IM and Presence Administration
- Cisco Unified IM and Presence Serviceability
- Cisco Unified IM and Presence Reporting
- IM and Presence Disaster Recovery System

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

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

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

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