



## Collaboration Instant Messaging and Presence

Revised: March 1, 2018

Cisco Unified Communications Manager IM and Presence Service provides native standards-based, dual-protocol, enterprise instant messaging (IM) and network-based presence as part of Cisco Unified Communications. This secure, scalable, and easy-to-manage service within Cisco Unified Communications Manager offers users feature-rich communications capabilities both within and external to the enterprise.

The Cisco Unified Communications Manager IM and Presence Service is one of the options for IM and Presence, which enhances the value of a Cisco Unified Communications and Collaboration system. The main presence component of the solution is the Cisco IM and Presence Service for all on-premises deployment needs, which incorporates the Extensible Communications Platform (XCP) and supports SIP/SIMPLE and Extensible Messaging and Presence Protocol (XMPP) for collecting information regarding a user's availability status and communications capabilities. The user's availability status indicates whether or not the user is actively using a particular communications device such as a phone. The user's communications capabilities indicate the types of communications that user is capable of using, such as video conferencing, web collaboration, instant messaging, or basic audio.

The IM and Presence Service is tightly integrated with Cisco and third-party compatible desktop and mobile presence and instant messaging clients, which also include Cisco Jabber SDK. It enables the clients to perform various functions such as instant messaging, presence, click-to-call, phone control, voice, video, visual voicemail, and web collaboration. The IM and Presence Service offers the flexibility of rich, open interfaces that enable implementation for IM and Cisco network-based presence, as well as IM and presence federation for a wide variety of business applications.

The aggregated user information captured by the Cisco IM and Presence Service enables Cisco Jabber, Cisco Unified Communications Manager applications, and third-party applications to increase user productivity. These applications help connect colleagues more efficiently by determining the most effective form of communication.



**Note**

The Cisco IM and Presence Service must be deployed with the equivalent version of Cisco Unified Communications Manager (Unified CM) using Cisco provided VM configuration OPTION user configuration templates on virtual servers on Cisco Unified Computing System (UCS). Cisco does not support over-subscription of VM resources between virtual servers, and system resources should be dedicated per virtual server being deployed.

This chapter explains the basic concepts of presence and instant messaging within the Cisco Unified Communications System for on-premises, cloud, and hybrid options, and it provides guidelines for how best to deploy the various components of the presence and instant messaging solution.

# What's New in This Chapter

Table 20-1 lists the topics that are new in this chapter or that have changed significantly from previous releases of this document.

**Table 20-1** *New or Changed Information Since the Previous Release of This Document*

New or Revised Topic	Described in:	Revision Date
Persistent chat	<a href="#">Persistent Chat and Compliance Logging Considerations, page 20-31</a>	March 1, 2018
Centralized IM and Presence deployments	<a href="#">Centralized IM and Presence Deployments, page 20-32</a>	March 1, 2018

## Presence

*Presence* refers to the ability and willingness of a user to communicate across a set of devices. It involves the following phases or activities:

- Publish user status  
User status changes can be published automatically by recognizing user keyboard activity, phone use, WebEx Meeting status, device connectivity to the network, and calendar status from Microsoft Exchange.
- Collect this status  
The published information is gathered from all the available sources, privacy policies are applied, and then current status is aggregated, synchronized, and stored for consumption.
- Consume the information  
Desktop applications, calendar applications, and devices can use the user status information to provide real-time updates for the end users to make better communication decisions.

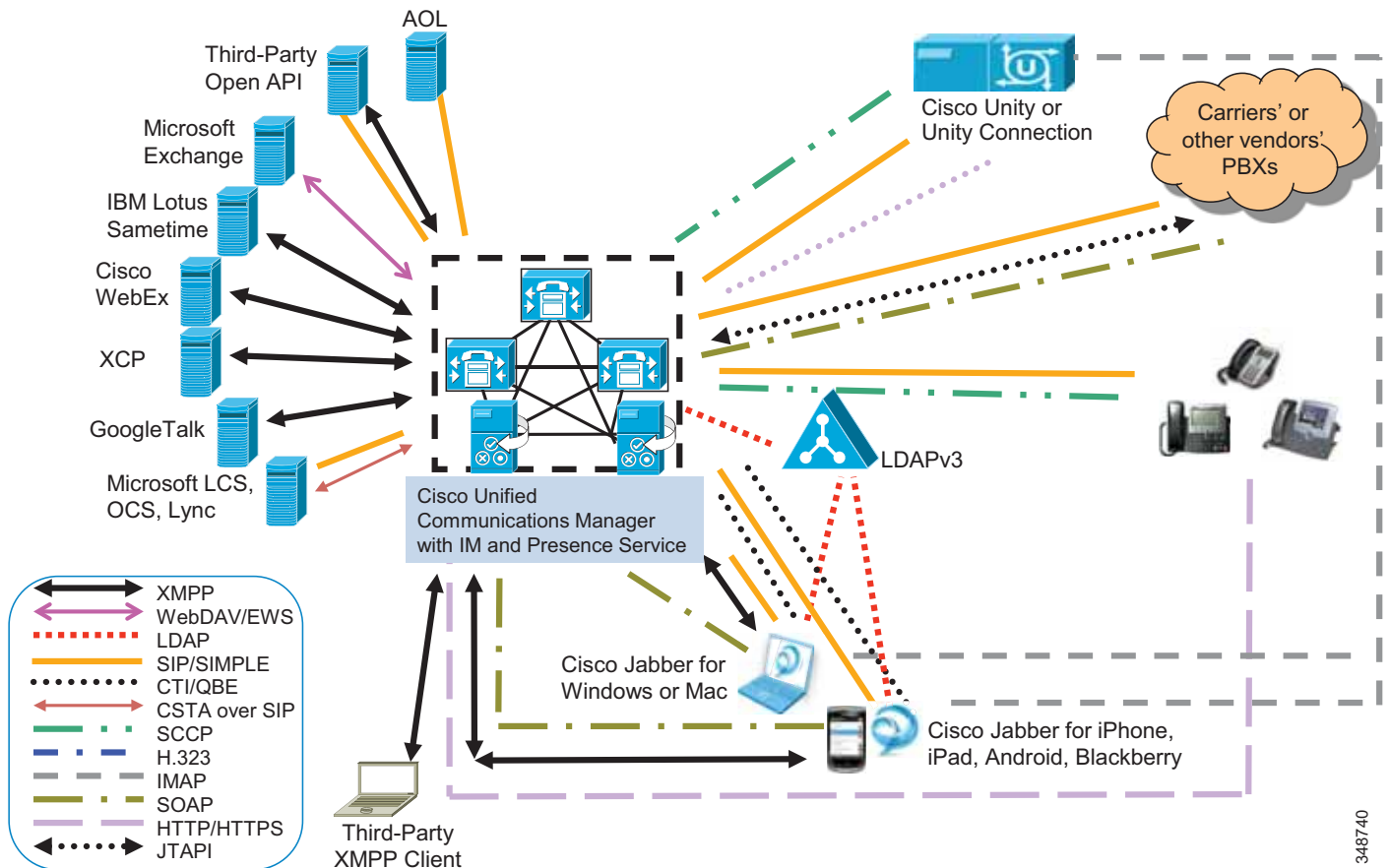
Status combines the capabilities of what the device or user can do (voice, video, instant messaging, web collaboration, and so forth) and the attributes showing the state of the device or user (available, busy, on a call, and so forth). Presence status can be derived from automatic events such as client login and telephone off-hook, or it can be derived from explicit notification events for changing status such as the user selecting Do Not Disturb from a change-status pick list.

Terminology surrounding presence refers to a watcher, presence entity (*presentity*), and presence server. The presence entity publishes its current status to the presence server by using a PUBLISH or REGISTER message for SIP/SIMPLE clients, or by using an XML Presence Stanza for XMPP clients. It can be a directory number (DN) or a SIP uniform resource identifier (URI) that resides within or outside the communications cluster. A *watcher* (device or user) requests presence status about a presence entity by sending a message to the presence server. The presence server responds to the watcher with a message containing the current status of the presence entity.

## On-Premises Cisco IM and Presence Service Components

Cisco IM and Presence Service encompasses the components illustrated in Figure 20-1.

Figure 20-1 Cisco IM and Presence Service Interfaces



348740

## On-Premises Cisco IM and Presence Service User

For presence, typically a user is described in terms of the user's presence status, the number of users on the system, or the user's presence capabilities.

A user, specified in Unified CM as an *end user*, has to be associated with a line appearance. When using the IMP PUBLISH Trunk service parameter on Unified CM, you must associate the user with a line appearance. With the line appearance, the user is effectively tied to a line appearance (directory number or URI associated with a particular device), which allows for a more detailed level of granularity for aggregation of presence information. The user can be mapped to multiple line appearances, and each line appearance can have multiple users (up to 5).



### Note

For voice-only, video-only, or IM-only deployments, the IM and Presence Service in Cisco Collaboration System Release (CSR) 12.x has a cluster capacity limit of 75,000 users for Full UC Mode.

The concept of a *presence user* appears throughout this chapter; therefore, keep in mind the meaning of a user as defined for Cisco IM and Presence. By default an IM and Presence Service user is defined in a Unified Communications deployment as *user@default\_domain* (the basis for the Jabber Identifier, or JID), where *user* is what is configured manually or in the Unified CM LDAP synchronization agreement (sAMAccountName, email, employee number, telephonenumber, or UserPrincipalName) and *default\_domain* is the domain configured in the IM and Presence Service administration.

## Enhanced IM Addressing and IM Address Schemes

The Enhanced IM Addressing feature provides for additional IM Address (JID) configuration options on Unified CM IM and Presence, which provides multi-domain support.

IM Addressing Schemes:

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

The default setting of *user@default\_domain* allows for only a single domain, whereas DirectoryURI allows for greater flexibility in handling multiple domains and email addresses as the contact identifier. A user can log into Jabber with their sAMAccountName attribute, while the Jabber ID is mapped to the DirectoryURI field. The Flexible JID structure makes it independent of UID for authentication.



### Note

DirectoryURI is a global administrative setting on Unified CM. If DirectoryURI is selected for IM and Presence Service addressing, all clients in the deployment must be able to handle and support the DirectoryURI option.

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.

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

## Single Sign-On (SSO) Solutions

Cisco recommends the use of SAML SSO (Release 10.0(1) and later) as the Single Sign-On (SSO) solutions.

SAML is an open standard that enables federated authentication across all operating systems. The SAML standard enables clients to authenticate against any SAML-enabled Collaboration service regardless of the operating system (OS) of the client's platform. SAML is a set of standards that have been defined to share information about who a user is and what the user's attributes are, as well as providing a way to request authentication and grant or deny access to something. For example, two different organizations can use SAML to establish trust relations without exchanging passwords.

SAML supports the following end-user applications:

- Cisco Unified CM
- Cisco IM and Presence Service
- Cisco Unity Connection
- Cisco WebEx Connect and Messenger Cloud

SAML SSO also supports the following end-user clients:

- WebEx iOS
- WebEx Android
- WebEx Connect
- WebEx Messenger
- Jabber for Windows
- Jabber iOS
- Jabber for Android
- Jabber for Mac

For information about SAML SSO, see the section on [On-Premises Cisco IM and Presence Service SAML SSO for Jabber, page 20-40](#), or the latest version of the *SAML SSO Deployment Guide for Cisco Unified Communications Applications* available at

<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>

## IM and Presence Collaboration Clients

The Cisco Collaboration software family of Jabber clients allows users to easily access capabilities for voice and video calls, provides a contact directory with presence information for colleagues, and includes tools for instant messaging (IM), voice messaging, desktop sharing, and conferencing.

Cisco Jabber clients offer various options to choose from, as well as third-party XMPP clients and applications that can be used. Cisco Jabber clients integrate with underlying Cisco Unified Communication services through a common set of interfaces. In general, each client provides support for a specific operating system and both desktop and mobile applications.

The client-specific sections of this chapter also provide relevant deployment considerations, planning, and design guidance around integration into the Cisco Unified Communications System.

The following Collaboration clients are supported by the Cisco Unified Communications System:

- Desktop clients include:
  - Cisco Jabber for Windows
  - Virtualization Experience Media Engine (VXME) for Windows
  - Cisco Jabber for Mac
- Web platforms include:
  - Cisco Jabber Guest
  - Cisco Jabber Web SDK

- Mobile clients include:
  - Cisco Jabber for iPhone
  - Cisco Jabber for iPad
  - Cisco Jabber for Blackberry
  - Cisco Jabber for Android
  - Mobile and Tablet

Cisco Jabber desktop clients for both Macintosh and Windows provide robust and feature-rich collaboration capabilities, including standards-based IM and presence, audio and video, visual voicemail, desktop sharing, desk phone control, Microsoft Office integration, and contact management.

Cisco Jabber desktop clients can be deployed to use on-premises services in which Cisco IM and Presence and Cisco Unified Communications Manager provide client configuration, instant messaging and presence, and user and device management. Cisco Jabber for Windows and Cisco Jabber for Mac can also be deployed to use cloud-based services through integration with Cisco WebEx Messenger service.

## Multiple Device Messaging (MDM) and Logins

All Cisco Jabber clients are associated to an IM and Presence Service node when a user logs in on any of the Jabber desktop or mobile clients. The IM and Presence node to which the user is associated monitors all changes for that user such as availability, contact list, and feature-based tasks.

The IM and Presence Service node tracks all of the registered clients for every presence-enabled user, whether they are logged in from one or all of the various Jabber clients such as Cisco Jabber for iOS, Android, Windows, or Mac.

When a new IM session is initiated between users who are logged into multiple clients, the first incoming message is broadcast to all of the registered clients of the receiving user. The IM and Presence Service node then waits for the first response from one of the registered clients. The first client to respond subsequently receives the remainder of the incoming messages until the user starts responding from another registered client. The node then reroutes subsequent messages to this new client.

For example:

Johnny wishes to initiate an IM conversation with Betty. He has previously logged into Cisco Jabber for Windows and Cisco Jabber for Android. Betty has registered two clients with the central IM and Presence Service node. Johnny initiates the conversation by sending the message, "Hi Betty. Are you free?"

The IM and Presence Service node identifies that Betty has two registered clients, and it broadcasts Johnny's message to both. Betty is sitting at her desk and observes Johnny's message appearing on both her laptop and phone. She chooses to respond using her laptop and responds with the message, "I have a meeting in a few moments but I can chat briefly right now."

The IM and Presence Service node identifies that Betty has responded using Cisco Jabber for Windows, and it marks this as the client to which to route all subsequent messages in the conversation. When Johnny responds with, "This will only take a minute," this response is routed directly to Cisco Jabber for Windows. If Betty starts responding to Johnny using her phone at some point in the conversation, the IM and Presence Service node will then route subsequent messages there instead of to Cisco Jabber for Windows.

**Note**

Every client a user logs into affects the total capacity limits for users and devices on the IM and Presence and Unified CM cluster. For example, on a cluster with a 15k-user VM configuration, if every user logs into their iPhone and desktop Jabber clients, then the maximum capacity would be 7,500 presence users instead of 15,000.

## Jabber Desktop Client Modes

Cisco Jabber desktop clients can operate in one of two modes for call control:

- Softphone Mode — Using audio and video on a computer

When a Jabber desktop client is in softphone mode, it is directly registered to Unified CM as a SIP endpoint for audio and video call control functionality, and it is configured on Unified CM as device type **Client Services Framework**.

- Deskphone Control Mode — Using a Cisco IP Phone for audio (and video, if supported)

When a Jabber desktop client is in deskphone control mode, it does not register with Unified CM using SIP, but instead it uses CTI/JTAPI to initiate, monitor, and terminate calls, monitor line state, and provide call history, while controlling a Cisco IP Phone.

### Cisco Jabber for Mobile Clients

Cisco provides collaboration clients for the following mobile devices: Android, BlackBerry, and Apple iOS devices such as iPhone and iPad. For more information on Cisco Jabber for mobile devices, see the chapter on [Mobile Collaboration, page 21-1](#).

### Cisco UC Integration™ for Microsoft Lync

Cisco UC Integration™ for Microsoft Lync allows for integrated Cisco Unified Communications services with Microsoft Lync and Microsoft Office Communications Server (OCS) R2, while delivering a consistent user experience. The solution extends the presence and instant-messaging capabilities of Microsoft Lync by providing access to a broad set of Cisco Unified Communications services, including standards-based audio and video, unified messaging, web conferencing, deskphone control, and telephony presence.

### Third-Party XMPP Clients and Applications

Cisco IM and Presence, with support for SIP/SIMPLE and Extensible Messaging and Presence Protocol (XMPP), provides support of third-party clients and applications to communicate presence and instant messaging updates between multiple clients. Third-party XMPP clients allow for enhanced interoperability across various desktop operating systems. In addition, web-based applications can obtain presence updates, instant messaging, and roster updates using the HTTP interface with SOAP, REST, or BOSH (based on the Cisco AJAX XMPP Library API). For additional information on the third-party open interfaces, see the section on [Third-Party Presence Server Integration, page 20-62](#).

## SAML Single Sign On

Single Sign-On allows Cisco Jabber users to securely access all Jabber services without being prompted to log into each of them separately. The Cisco Jabber application uses authentication performed by the corporate Identity Provider. The Identity Provider can control the authentication experience for Cisco



Jabber users – for example, by prompting users for their enterprise username and password once when the Cisco Jabber application is first run and by specifying the length of time a user is authorized to use Cisco Jabber services.

The Cisco Jabber application uses the Security Assertion Markup Language (SAML), which is an XML-based open standard data format that enables access to a defined set of Cisco services transparently after verifying credentials with an Identity Provider. SAML Single Sign-On can be enabled for Cisco WebEx Messenger Services, Cisco Unified Communications Manager, and Cisco Unity Connection. SSO is deployed for use with Cisco Jabber clients using service discovery.

SAMLv2 SSO supports the following deployment models:

- On-premises deployment models
  - IM and Presence and Unified CM
  - IM and Presence, Unified CM, and Unity Connection (SSO)
  - IM and Presence, Unified CM, Unity Connection (SSO), and Cisco Mobile Workspace Solution (SSO or not)
- Hybrid deployment models
  - WebEx Messenger (SSO) and Unified CM
  - WebEx Messenger (SSO), Unified CM, and Unity Connection
  - WebEx Messenger (SSO), Unified CM, Unity Connection, and WebEx Meeting Center

## Cisco Unified CM User Data Service (UDS)

UDS is an umbrella of service APIs provided by Unified CM. UDS provides a contact source API that can be used by Jabber over Cisco Expressway mobile and remote access for the contact source. The UDS contact source uses the Unified CM end user table information to provide a contact lookup service.

Beginning with Cisco Unified CM 11.5, the UDS-to-LDAP Proxy feature can also be used for contact searches. When enabled, contact searches are still handled by UDS but are proxied to the corporate LDAP directory, with UDS relaying results back to the Jabber client. This enables Jabber clients to search a corporate directory that exceeds the maximum number of users supported within Unified CM.

The UDS contact service is always used for remote Jabber clients connected over Expressway mobile and remote access, and it is an optional contact service for clients on the corporate network. You can populate the UDS contact source data by using the Unified CM web interface (by creating end users), by using the LDAP sync function to Active Directory or other supported LDAP source, or by using the UDS-to-LDAP Proxy function.

UDS does not support the same attribute list as LDAP contact sources. Rather, UDS supports the following attributes:

[username, firstname, lastname, middlename, nickname, phone number, homenummer, mobilenumber, email,directory URI, msURI, title,department, manager]

UDS does not provide the same level of predictive search or Ambiguous Name Resolution (ANR) provided by LDAP contact sources. UDS searches against firstname, lastname, and email address.



### Note

Ambiguous Name Resolution (ANR) is a search algorithm associated with Lightweight Directory Access Protocol (LDAP) clients, and it allows for objects to be bound without complex search filters. ANR is useful when you are locating objects and attributes that may or may not be known by the client.



UDS usage considerations for on-premise deployments:

- Jabber on-premises (on-net) can use LDAP or UDS as a contact source.
- UDS is a set of HTTP-based services provided by Unified CM. The UDS contact source is one UDS service, which provides contact and number resolution.
- When Jabber is connected remotely over Expressway mobile and remote access, it always uses UDS as a contact source. Again, your design must comply with cluster sizing recommendations.

UDS is an integrated network service that runs on all Unified CM servers in a cluster and is critical to server discovery. In the case of an IM-only deployment, although voice and video are not part of the deployment, Unified CM call processing subscriber pairs are still required to handle and distribute the UDS service load. The number of IM-only users will dictate the number of Unified CM subscriber pairs required. For example, a standard Unified CM cluster with 40,000 users and/or endpoints would require 4 subscriber pairs in order to support 40,000 IM-only users.

## LDAP Directory

You can configure a corporate LDAP directory to satisfy a number of different requirements, including the following:

- User provisioning — You can provision users automatically from the LDAP directory into the Cisco Unified Communications Manager database using directory integration. Cisco Unified CM synchronizes with the LDAP directory content so that 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. Cisco IM and Presence synchronizes all the user information from Cisco Unified Communications Manager to provide authentication for client users.
- User lookup — You can enable LDAP directory lookups to allow Cisco clients or third-party XMPP clients to search for contacts in the LDAP directory.

## AD Groups and Enterprise Groups

Cisco Jabber users can search for groups in Microsoft Active Directory and add them to their contact lists.

Cisco Unified CM synchronizes its database with the Microsoft Active Directory groups at specified intervals (specified in LDAP Directory Synchronization Schedule parameters in the LDAP Directory configuration), and it also updates Jabber end-user contact lists upon synchronization.

If a Cisco Jabber user wants to add a group to the contact list while the AD Groups Sync feature is enabled, the Cisco Jabber client sends a group request to the IM and Presence Service node. The IM and Presence Service node provides the following information for each group member:

- Display Name
- User ID and Title
- Phone number
- Mail ID

## AD Group Considerations for Groups and User Filters

- Group filters must be configured and validated by the administrator of the Cisco CallManager Application.
- The administrator should ensure that the User filters and Group filters are named appropriately and assigned to the right filter fields meant for User and Group filters.
- DirSync service does not validate the filter string format for syntax or logical accuracy; the administrator must verify the accuracy of the filters.
- For every filter string there should be one string added for ignoring security groups while performing synchronization.

## WebEx Directory Integration

WebEx Directory Integration is achieved through the WebEx Administration Tool. WebEx imports a comma-separated value (CSV) file of your enterprise directory information into its WebEx Messenger service. For more information, refer to the documentation at

<https://www.webex.com/webexconnect/orgadmin/help/index.htm?toc.htm?17444.htm>

### Directory Search

When a contact cannot be found in the local Jabber desktop client cache or contact list, a search for contacts can be made. The WebEx Messenger user can utilize a predictive search whereby the cache, contact list, and local Outlook contact list are queried as the contact name is being entered. If no matches are found, the search continues to query the corporate directory (WebEx Messenger database).

## Common Deployment Models for Jabber Clients

Cisco Jabber desktop clients support the following deployment models:

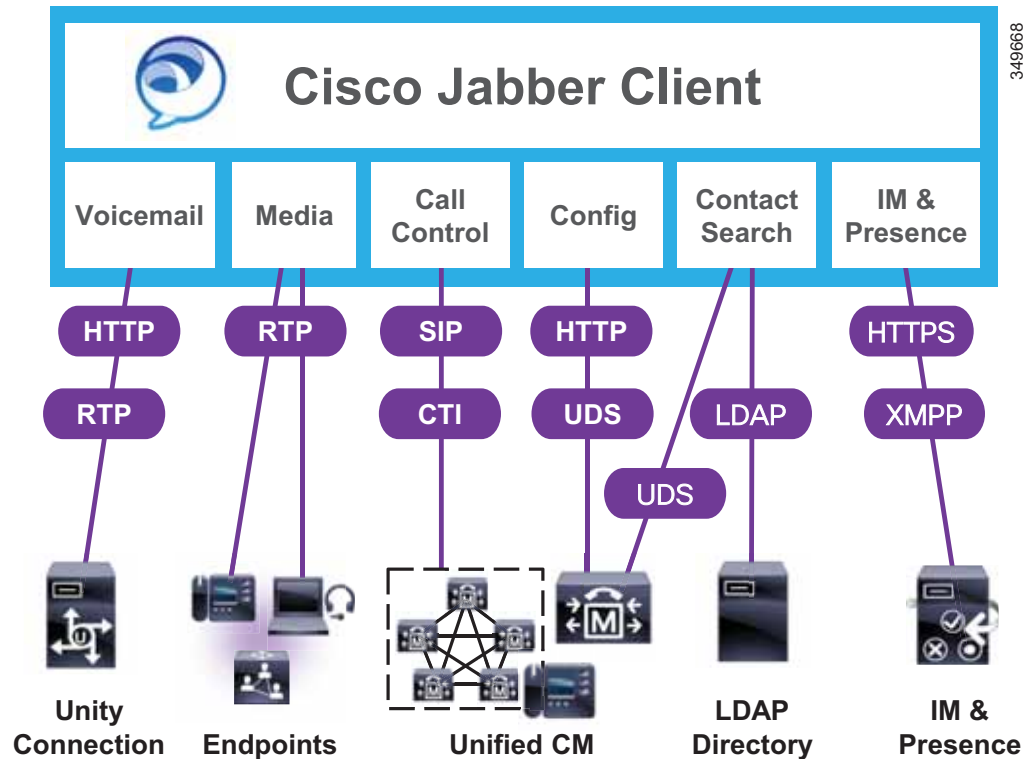
- [On-Premises Deployment Model, page 20-11](#)
- [Cloud-Based Deployment Model, page 20-12](#)
- [Hybrid Cloud-Based and On-Premises Deployment Model, page 20-13](#)
- [Centralized IM and Presence Deployments, page 20-32](#)

Your choice of deployment will depend primarily upon your product choice for IM and presence and the requirement for additional services such as voice and video, voicemail, and deskphone control.

## On-Premises Deployment Model

In the on-premises deployment model, all services are set up and configured on an enterprise network that you manage and maintain. (See [Figure 20-2](#).)

**Figure 20-2** *Jabber On-Premises Deployment Model*



The on-premises deployment model for Cisco Jabber for Windows relies on the following components:

- Cisco Unified Communications Manager provides all user and device configuration capabilities.
- Cisco Unified Communications Manager and Cisco conferencing devices provide audio and video conferencing capabilities.
- Cisco Unity Connection provides voicemail capabilities.
- Cisco IM and Presence provides instant messaging and presence services.
- Microsoft Active Directory or another supported LDAP directory provides contact sources.

These components are the essential requirements to achieve a base deployment of Cisco Jabber clients. After you set up and configure a base deployment, you can set up and configure additional deployment options such as:

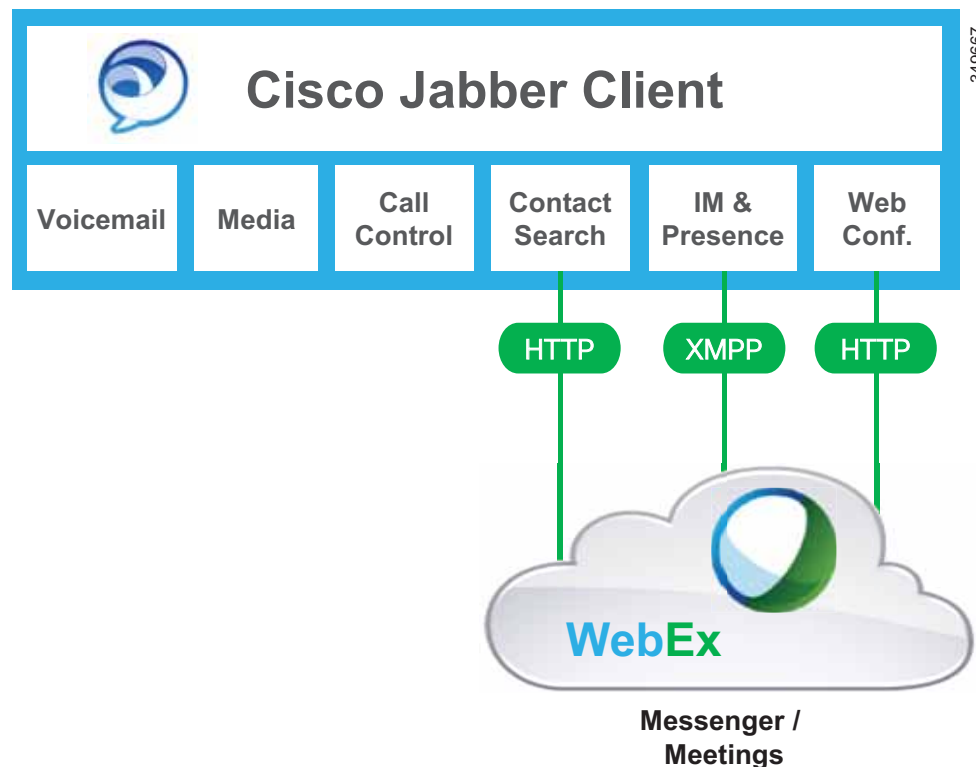
- Voice — Provides audio call capabilities.
- Video — Provides capabilities to enable users to transmit and receive video calls.
- Voicemail — Provides voicemail capabilities that users can retrieve directly in the Cisco Jabber client user interface or when users dial their voicemail number.

- Desktop sharing — Enables users to share their desktops via Binary Flow Control Protocol (BFCP).
- Microsoft Office integration — Provides user availability status and messaging capabilities directly through the user interface of Microsoft Office applications such as Microsoft Outlook.

## Cloud-Based Deployment Model

In the cloud-based deployment model, all (or most) services are hosted in the cloud using Cisco WebEx. When implementing a cloud-based deployment model using Cisco WebEx, you manage and monitor your cloud-based deployment with the Cisco WebEx Administration Tool. (See [Figure 20-3](#).)

**Figure 20-3** Jabber Cloud-Based Deployment Model (WebEx)



The cloud-based deployment model for Cisco Jabber for Windows relies on Cisco WebEx Messenger service for the following services:

- Instant messaging and chat capabilities
- Presence capabilities for users
- Native desktop sharing
- User configuration and contact sources

These services are the essential components required to achieve a base deployment of Cisco Jabber for Windows. After you set up and configure a base deployment, you can set up and configure additional deployment options such as:

- Cisco WebEx Meeting Center — Offers hosted collaboration features such as online meetings and events.
- Microsoft Office integration — Provides user availability status and messaging capabilities directly through the user interface of Microsoft Office applications such as Microsoft Outlook. This integration is set up by default.
- Calendar integration — Calendar integration with WebEx Meeting Center, Outlook, and IBM Lotus Notes is also supported.

For information on WebEx Messenger service configuration for Jabber Clients, refer to the *Cisco WebEx Messenger Administrator's Guide*, available at

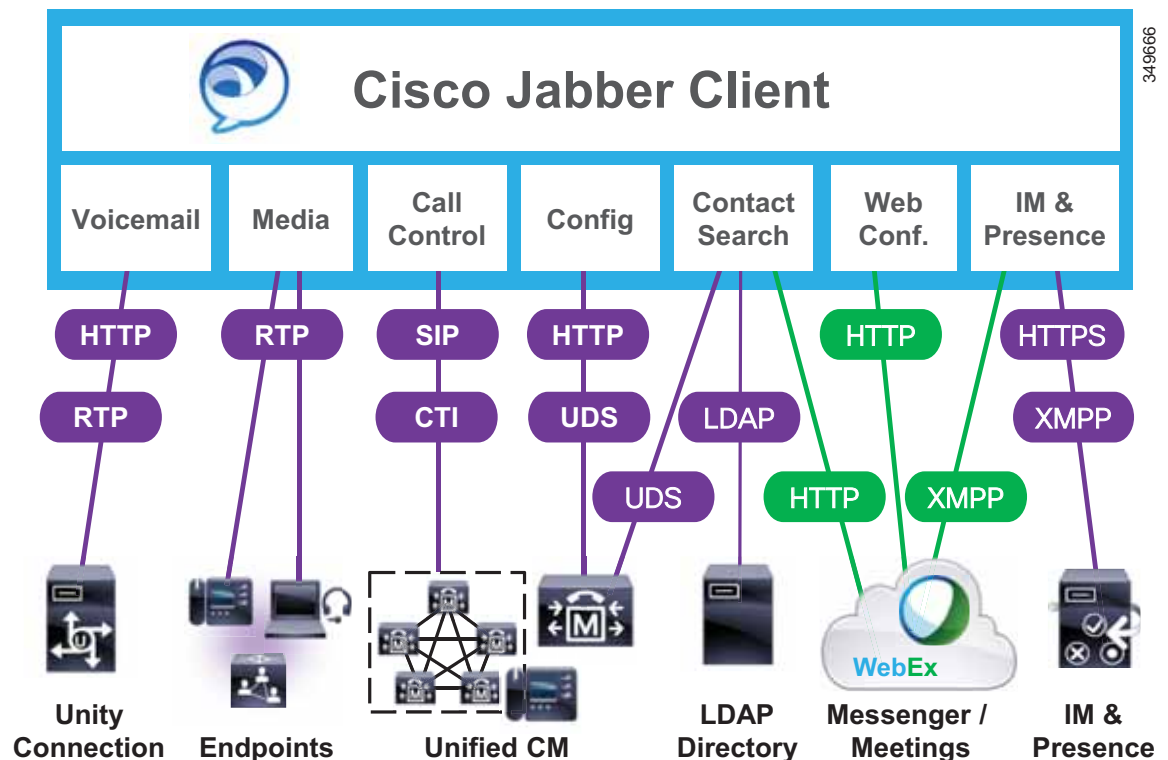
<https://www.webex.com/webexconnect/orgadmin/help/index.htm>

## Hybrid Cloud-Based and On-Premises Deployment Model

In a hybrid deployment, the cloud-based services hosted on Cisco WebEx Messenger service are combined with the following components of an on-premises deployment (see [Figure 20-4](#)):

- Cisco Unified Communications Manager provides user and device services.
- Cisco Unity Connection provides voicemail services.

**Figure 20-4** Jabber Hybrid Cloud-Based and On-Premises Deployment Model



349666

# Client-Specific Design Considerations

The following sections discuss design considerations that are specific to Cisco Collaboration desktop clients for Mac and Windows. For common design considerations for these client types, refer to the design guidance provided in the section on [Cisco Jabber Desktop Client Architecture](#), page 8-23.

## Phone-Specific Presence and Busy Lamp Field

Endpoints connected to Unified CM can receive the line status of one or more other endpoints as idle, busy, unknown. The status is shown in the call history, in the directory, and by the use of the busy lamp field (BLF) feature. While presence on the call history and directory is received only after a lookup performed by the user, BLF constantly monitors the line status of a telephone or a video phone and represents it on a specific presence-enabled speed-dial configured in the monitoring device.

All telephony presence requests for users, whether inside or outside the cluster, are processed and handled by Cisco Unified CM.

A Unified CM watcher that sends a presence request will receive a direct response, including the presence status, if the watcher and presence entity are within the same Unified CM cluster.

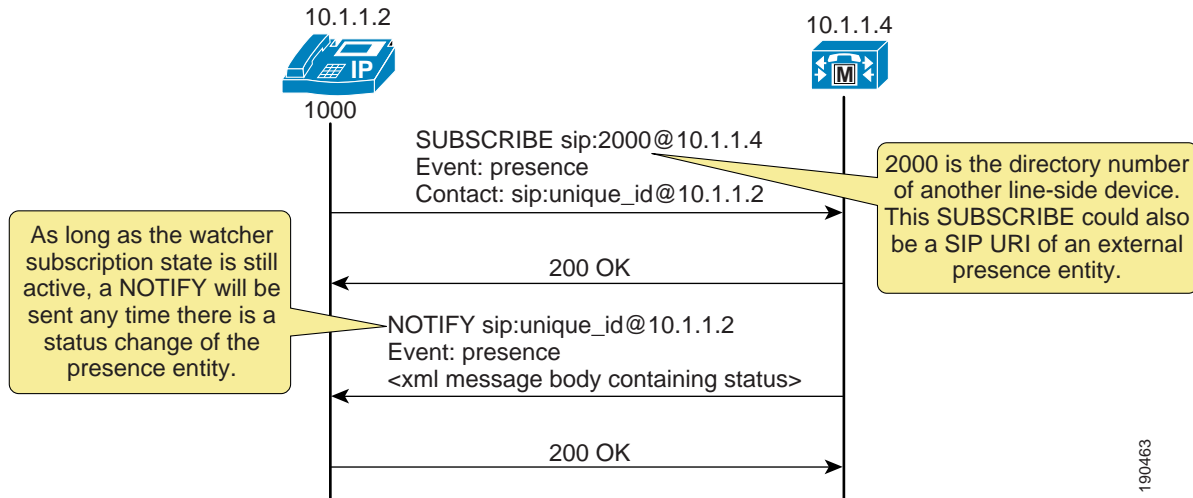
If the presence entity exists outside the cluster, Unified CM will query the external presence entity through the SIP trunk. If the watcher has permission to monitor the external presence entity based on the SUBSCRIBE calling search space and presence group (both described in the section on [Unified CM Presence Policy](#), page 20-17), the SIP trunk will forward the presence request to the external presence entity, await the presence response from the external presence entity, and return the current presence status to the watcher.

A watcher that is not in a Unified CM cluster can send a presence request to a SIP trunk. If Unified CM supports the presence entity, it will respond with the current presence status. If Unified CM does not support the presence entity, it will reject the presence request with a SIP error response.

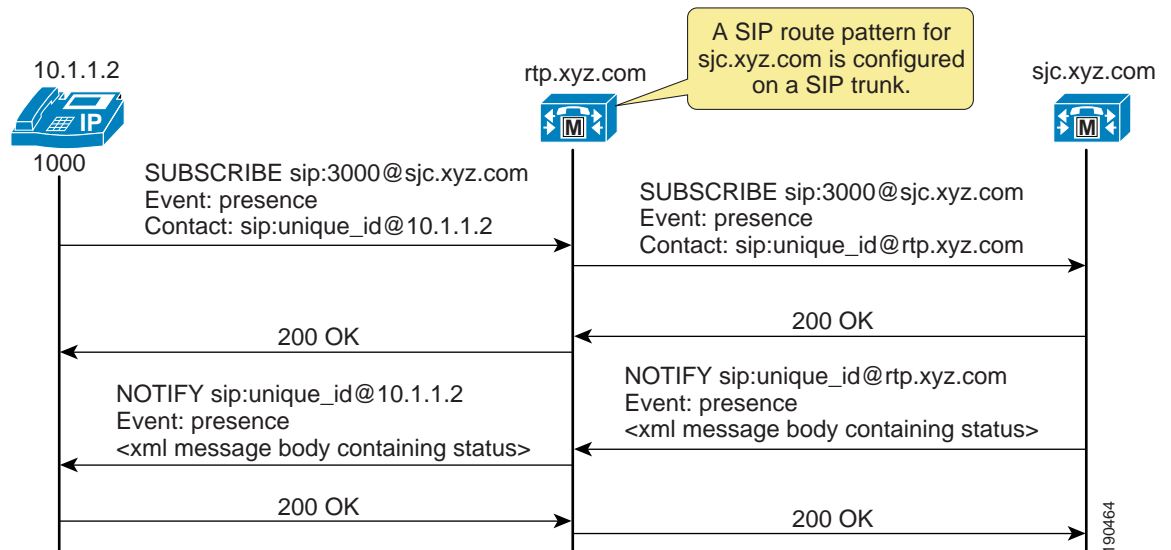
## Unified CM Presence with SIP

Unified CM uses the term *SIP line* to represent endpoints supporting SIP that are directly connected and registered to Unified CM and the term *SIP trunk* to represent trunks supporting SIP. SIP line-side endpoints acting as presence watchers can send a SIP SUBSCRIBE message to Unified CM requesting the presence status of the indicated presence entity.

If the presence entity resides within the Unified CM cluster, Unified CM responds to a SIP line-side presence request by sending a SIP NOTIFY message to the presence watcher, indicating the current status of the presence entity. (See [Figure 20-5](#).)

**Figure 20-5** SIP Line SUBSCRIBE/NOTIFY Exchange

If the presence entity resides outside the Unified CM cluster, Unified CM routes a SUBSCRIBE request out the appropriate SIP trunk, based on the SUBSCRIBE calling search space, presence group, and SIP route pattern. When Unified CM receives a SIP NOTIFY response on the trunk, indicating the presence entity status, it responds to the SIP line-side presence request by sending a SIP NOTIFY message to the presence watcher, indicating the current status of the presence entity. (See [Figure 20-6](#).)

**Figure 20-6** SIP Trunk SUBSCRIBE/NOTIFY Exchange

SUBSCRIBE messages for any directory number or SIP URI residing outside the Unified CM cluster are sent or received on a SIP trunk in Unified CM. The SIP trunk could be an interface to another Unified CM or it could be an interface to the Cisco IM and Presence Service.



## Unified CM Speed Dial Presence

Unified CM supports the ability for a speed dial to have presence capabilities by means of a busy lamp field (BLF) speed dial. BLF speed dials work as both a speed dial and a presence indicator. However, only the system administrator can configure a BLF speed dial; a system user is not allowed to configure a BLF speed dial.

The administrator must configure the BLF speed dial with a target directory number or URI that is resolvable to a directory number or URI within the Unified CM cluster or a SIP trunk destination. BLF SIP line-side endpoints can also be configured with a SIP URI for the BLF speed dial, but SCCP line-side endpoints cannot be configured with a SIP URI for BLF speed dial. The BLF speed dial indication is a line-level indication and not a device-level indication.









### Note

A maximum of 30,000 BLF speed dials can be configured per cluster.

For a listing of the phone models that support BLF speed dials, consult the Cisco Unified IP Phone administration guides available on <https://www.cisco.com/>.

Figure 20-7 lists the various types of BLF speed dial indications from the phones.

**Figure 20-7 Indicators for Speed Dial Presence on Cisco Unified IP Phones 7900 Series**

State	Icon	LED
Idle		
Busy		
Unknown		

190465

## Unified CM Call History Presence

Unified CM supports presence capabilities for call history lists (the Directories button on the phone). Call history list presence capabilities are controlled via the **BLF for Call Lists** Enterprise Parameter within Unified CM Administration. The **BLF for Call Lists** Enterprise Parameter impacts all pages using the phone Directories button (Missed, Received, and Placed Calls, Personal Directory, or Corporate Directory), and it is set on a global basis.

For a listing of the phone models that support presence capabilities for call history lists, consult the Cisco Unified IP Phone administration guides available on <https://www.cisco.com/>.

The presence indicators for call history lists are the same as those listed in the Icon column in Figure 20-7; however, no LED indications are available.

## Unified CM Presence Policy

Unified CM provides the capability to set policy for users who request presence status. You can set this policy by configuring a calling search space specifically to route SIP SUBSCRIBE messages for presence status and by configuring presence groups with which users can be associated to specify rules for viewing the presence status of users associated with another group.

### Unified CM Subscribe Calling Search Space

The first aspect of presence policy for Unified CM is the SUBSCRIBE calling search space. Unified CM uses the SUBSCRIBE calling search space to determine how to route presence requests (SUBSCRIBE messages with the Event field set to Presence) that come from the watcher, which could be a phone or a trunk. The SUBSCRIBE calling search space is associated with the watcher and lists the partitions that the watcher is allowed to "see." This mechanism provides an additional level of granularity for the presence SUBSCRIBE requests to be routed independently from the normal call-processing calling search space.

The SUBSCRIBE calling search space can be assigned on a device basis or on a user basis. The user setting applies for originating subscriptions when the user is logged in to the device through Extension Mobility or when the user is administratively assigned to the device.

With the SUBSCRIBE calling search space set to <None>, BLF speed dial and call history list presence status does not work and the subscription messages is rejected as "user unknown." When a valid SUBSCRIBE calling search space is specified, the indicators work and the SUBSCRIBE messages are accepted and routed properly.



#### Note

Cisco strongly recommends that you do not leave any calling search space defined as <None>. Leaving a calling search space set to <None> can introduce presence status or dialing plan behavior that is difficult to predict.

### Unified CM Presence Groups

The second aspect of the presence policy for Unified CM is presence groups. Devices, directory numbers, and users can be assigned to a presence group, and by default all users are assigned to the Standard Presence Group. A presence group controls the destinations that a watcher can monitor, based on the user's association with their defined presence group (for example, Contractors watching Executives is disallowed, but Executives watching Contractors is allowed). The presence group user setting applies for originating subscriptions when the user is logged in to the device via Extension Mobility or when the user is administratively assigned to the device.

When multiple presence groups are defined, the Inter-Presence Group Subscribe Policy service parameter is used. If one group has a relationship to another group via the Use System Default setting rather than being allowed or disallowed, this service parameter's value will take effect. If the Inter-Presence Group Subscribe Policy service parameter is set to **Disallowed**, Unified CM will block the request even if the SUBSCRIBE calling search space allows it. The Inter-Presence Group Subscribe Policy service parameter applies only for presence status with call history lists and is not used for BLF speed dials.

Presence groups can list all associated directory numbers, users, and devices if you enable dependency records. Dependency records allow the administrator to find specific information about group-level settings. However, use caution when enabling the Dependency Record Enterprise parameter because it could lead to high CPU usage.

## Unified CM Presence Guidelines

Unified CM enables the system administrator to configure and control user phone state presence capabilities from within Unified CM Administration. Observe the following guidelines when configuring presence within Unified CM:

- Select the appropriate model of Cisco Unified IP Phones that have the ability to display user phone state presence status.
- Define a presence policy for presence users.
  - Use SUBSCRIBE calling search spaces to control the routing of a watcher presence-based SIP SUBSCRIBE message to the correct destinations.
  - Use presence groups to define sets of similar users and to define whether presence status updates of other user groups are allowed or disallowed.
- Call history list presence capabilities are enabled on a global basis; however, user status can be secured by using a presence policy.
- BLF speed dials are administratively controlled and are not impacted by the presence policy configuration.

**Note**

Cisco Business Edition can be used in ways similar to Unified CM to configure and control user presence capabilities. For more information, refer to the chapter on [Call Processing, page 9-1](#).

## User Presence: Cisco IM and Presence Architecture

The Cisco IM and Presence Service uses standards-based XMPP for instant messaging and presence. The Cisco IM and Presence Service also supports SIP for interoperability with SIP IM providers. Cisco IM and Presence also provides an HTTP interface that has a configuration interface through Simple Object Access Protocol (SOAP); a presence interface through Representational State Transfer (REST); and a presence, instant messaging, and Bidirectional-streams Over Synchronous HTTP (BOSH) interface through the Cisco AJAX XMPP Library (CAXL). The Cisco AJAX XMPP Library web tool kit communicates to the BOSH interface on the Extensible Communications Platform within Cisco IM and Presence. The Cisco IM and Presence Service collects, aggregates, and distributes user capabilities and attributes using these standards-based SIP, SIMPLE, XMPP, and HTTP interfaces.

Cisco or third-party applications can integrate with presence and provide services that improve the end-user experience and efficiency. The core components of the Cisco IM and Presence Service consist of: the Extensible Communications Platform (XCP), which handles presence, instant messaging, roster, routing, policy, and federation management; the Rich Presence Service, which handles presence state gathering, network-based rich presence composition, and presence-enabled routing functionality; and support for ad-hoc group chat storage with persistent chat and message archiving handled to an external database. If persistent chat is enabled, ad-hoc rooms are stored to the external PostgreSQL, Microsoft SQL, or Oracle database for the duration of the ad-hoc chat. If persistent chat is disabled, ad-hoc chats are stored in volatile memory for the duration of the chat.

Applications (either Cisco or third-party) can integrate presence and provide services that improve the end user experience and efficiency. In addition, Cisco Jabber is a supported client of the Cisco IM and Presence Service that also integrates instant messaging and presence status.

The Cisco IM and Presence Service also contains support for interoperability with Microsoft Lync Server 2010 and 2013 and the Microsoft Lync client for any Cisco Unified IP Phone connected to a Unified CM. The Microsoft Lync client interoperability includes click-to-dial functionality, phone control capability through Remote Call Control (RCC), and presence status of Cisco Unified IP Phones.

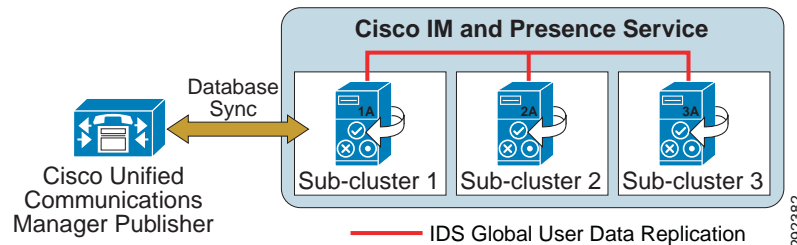
## On-Premises Cisco IM and Presence Service Cluster

The Cisco IM and Presence Service uses the same underlying appliance model and hardware used by Unified CM as well as Unified CM on the Cisco Unified Computing System (UCS) platform, including a similar administration interface. For details on the supported platforms, refer to the latest version of the *Cisco Unified Communications Manager Compatibility Matrix*, available at

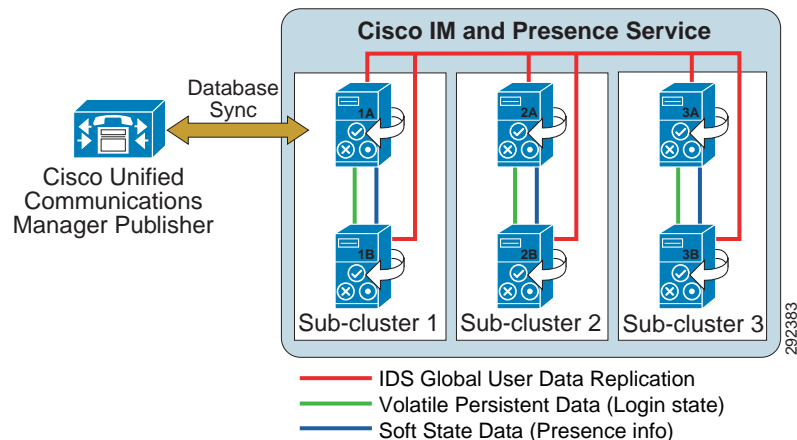
[https://www.cisco.com/en/US/products/sw/voicesw/ps556/products\\_device\\_support\\_tables\\_list.html](https://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html)

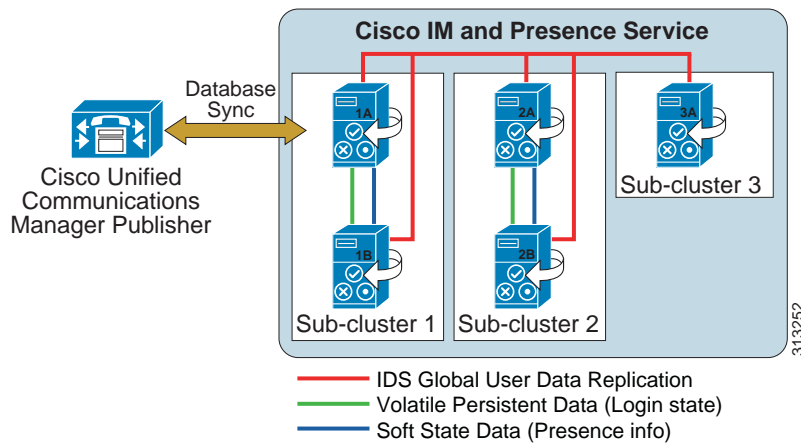
A Cisco IM and Presence Service cluster consists of up to six servers, including one designated as a publisher, which utilize the same architectural concepts as the Unified CM publisher and subscriber. Within a Cisco IM and Presence Service cluster, individual servers can be grouped to form a subcluster, and the subcluster can have at most two servers associated with it. Figure 20-8 shows the basic topology for a Cisco IM and Presence Service cluster, while Figure 20-9 shows a highly available topology. The Cisco IM and Presence Service cluster can also have mixed subclusters, where one subcluster is configured with two servers while other subclusters contain a single server, as shown in Figure 20-10.

**Figure 20-8 Basic Deployment of On-Premises Cisco IM and Presence Service**



**Figure 20-9 High Availability Deployment of On-Premises Cisco IM and Presence Service**



**Figure 20-10** Mixed Deployment of On-Premises Cisco IM and Presence Service

The on-premises Cisco IM and Presence Service utilizes and builds upon the database used by the Unified CM publisher by sharing the user and device information.

To support Availability Integration with Cisco Unified CM, the CUCM Domain SIP Proxy service parameter must match the DNS domain of the Unified CM cluster. By default, the CUCM Domain SIP Proxy service parameter is set to the DNS domain of the IM and Presence database publisher node. Therefore, if the DNS domain of the IM and Presence database publisher node differs from the DNS domain of the Unified CM cluster, you must update this service parameter using the Cisco Unified CM IM and Presence Administration user interface on the IM and Presence database publisher node. For more information on specifying the DNS domain associated with the Cisco Unified Communications Manager cluster, refer to the latest version of *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*, available at

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

Keep in mind that IM and Presence maintains access control list (ACL) entries for all Unified CM nodes. These entries are FQDN-based and are generated by appending the Unified CM hostname to the DNS domain of the IM and Presence publisher. So if the DNS domain of IM and Presence publisher (database) is different than that of the Unified CM cluster, invalid ACL entries will be generated, which would cause issues.



#### Note

A single Unified CM cluster supports only a single IM and Presence Service cluster; therefore, a separate IM and Presence Service cluster is required for each Unified CM cluster.

Intracuster traffic participates at a very low level between the Cisco IM and Presence Service and Unified CM, and between the Cisco IM and Presence Service publisher and subscriber servers. Both clusters share a common hosts file and have a strong trust relationship using IPTables. At the level of the database and services, the clusters are separate and distinct; however, the configuration and administration is primarily done on the Unified CM cluster, with limited configuration and administration done on the IM and Presence Service cluster. There is currently no Transport Layer Security (TLS) or IPsec utilization for intracuster traffic.

The Cisco IM and Presence Service publisher communicates directly with the Unified CM publisher via the AVVID XML Layer Application Program Interface (AXL API) using the Simple Object Access Protocol (SOAP) interface. When first configured, the Cisco IM and Presence Service publisher performs an initial synchronization of the entire Unified CM user and device database. All Cisco IM and Presence Service users are configured in the Unified CM End User configuration. During the synchronization, Cisco IM and Presence Service populates these users in its database from the Unified CM database and does not provide end-user configuration from its administration interface. After synchronization, users must be enabled for IM and Presence Service through the Cisco Unified Communications Manager administrator interface before the Cisco IM and Presence Service can manage them.

**Note**

Cisco IM and Presence Service supports synchronization of up to 160,000 users, equivalent to Unified CM. However, the maximum number of licensed presence users for a Cisco IM and Presence Service cluster is 75,000 using the 25k-user IM and Presence VM template across 3 sub-cluster pairs, assuming a megacluster deployment.

The initial Cisco IM and Presence Service database synchronization from Unified CM might take a while, depending on the amount of information in the database as well as the load that is currently on the system. Subsequent database synchronizations from Unified CM to Cisco IM and Presence Service are performed in real time when any new user or device information is added to Unified CM.

**Note**

When Cisco IM and Presence Service is performing the initial database synchronization from Unified CM, do not perform any administrative activities on Unified CM while the synchronization agent is active.

## On-Premises Cisco IM and Presence Service High Availability

The Cisco IM and Presence Service cluster consists of up to a maximum of six servers, which can be configured into multiple subclusters with the maximum of three subclusters for high availability. A subcluster contains a maximum of two servers and allows for users associated with one server of the subcluster to use the other server in the subcluster automatically if a failover event occurs. Cisco IM and Presence Service does not provide failover between subclusters.

When deploying a Cisco IM and Presence Service cluster for high availability, you must take into consideration the maximum number of users per server to avoid oversubscribing any one server within the subcluster in the event of a failover.

You can achieve high availability using two different setups: active/active or 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.

### Deployment Consideration

The IM and Presence Service cluster supports a maximum of 75,000 users in Full UC mode, across 3 single IM and Presence nodes deployed with the 25,000-user VM configuration template but with no high availability.

A high availability deployment for 75,000 users would require 3 IM and Presence subcluster pairs deployed with the 25,000-user VM configuration template option.

**Note**

The 25,000-user VM configuration should be used for megacluster deployments, which must be reviewed and approved by Cisco prior to deployment. If your deployment is not a megacluster, then use a lower capacity VM configuration template, such as the 15,000-user or 5,000-user VM configuration template. However, if it is more desirable to use the 25k-user IM and Presence VM configuration in your non-megacluster deployment, contact Cisco with your design topology and request approval prior to deploying the 25k-user VM configuration. Exceptions may be provided based on a design review of the IM and Presence configuration using the 25k-user VM template.

## On-Premises Cisco IM and Presence Service Deployment Models

Unified CM provides a choice of the following deployment models:

- Single site
- Multisite WAN with centralized call processing
- Multisite WAN with distributed call processing
- Clustering over the WAN
- Centralized IM and Presence

Cisco IM and Presence Service is supported with all the Unified CM deployment models. However, Cisco recommends locating the Cisco IM and Presence Service publisher in the same physical datacenter as the Unified CM publisher due to the initial user database synchronization. All on-premises Cisco IM and Presence servers should be physically located in the same datacenter within the Cisco IM and Presence Service cluster, with the exception of geographic datacenter redundancy and clustering over the WAN (for details, see [Clustering Over the WAN](#), page 20-29).

For more information on Unified CM deployment models, see the chapter on [Collaboration Deployment Models](#), page 10-1.

Cisco IM and Presence Service deployment depends on high-availability requirements, the total number of users, and the server being used. Detailed configuration and deployment steps can be found in the *Deployment Guide for Cisco IM and Presence*, available at

[https://www.cisco.com/en/US/products/ps6837/products\\_installation\\_and\\_configuration\\_guides\\_list.html](https://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html)

A highly available Cisco IM and Presence Service cluster requires two servers per subcluster. This allows for users to fail-over between the servers within the subcluster; however, the total number of users supported and the time to failover vary based on which features are enabled, the average size of contact lists, the rate of traffic placed on the servers, and the placement of the servers if deployed across a WAN. Once a Cisco IM and Presence Service subcluster is configured for two servers, it always operates as highly available if **High Availability** is configured in the Unified CM administration **System > Presence Redundancy Group**. High availability can be deployed using an Active/Standby model or an Active/Active model, and these modes are controlled by the Enterprise Parameter **User Assignment Mode for Presence Server**. By default all users are balanced across all servers in the cluster, and Cisco recommends leaving this parameter set to its default value.

**Note**

Each subcluster is a Presence Redundancy Group.

*Cisco IM and Presence Active/Standby mode* — (Setting **User Assignment Mode for Presence Server** to **None**) is attained by manually assigning users to the first server in the subcluster, leaving the second server with no users assigned but all processes synchronized and ready for a failover if the first server in



the subcluster fails. For example, in [Figure 20-9](#) the first user would be assigned to server 1A, the second user to server 2A, the third user to server 3A, the fourth user to server 1A, the fifth user to server 2A, the sixth user to server 3A, and so forth. The users should be assigned equally across all the 'A' servers in the cluster.

*Cisco IM and Presence Active/Active mode* — (Setting **User Assignment Mode for Presence Server to balanced**), which is the default and recommended setting for load distribution, will automatically assign users equally across all servers in the subclusters. Each server is synchronized and ready for a failover if the other server in the subcluster fails. For example, in [Figure 20-9](#) the first user would be assigned to server 1A, the second user to server 2A, the third user to server 3A, the fourth user to server 1B, the fifth user to server 2B, the sixth user to server 3B, and so forth. The users are assigned equally across all the servers in the cluster.

*Cisco IM and Presence Active/Active* deployments with a balanced **User Assignment Mode for Presence Server** allows for redundancy flexibility based on the features being used, the size of user contact lists, and the traffic (user data profiles) being generated. A Cisco IM and Presence Active/Active deployment with a fully redundant mode, regardless of features, requires the total number of supported users to be reduced in half (for example, a deployment of 15,000 Users OVAs in a balanced high-availability redundant configuration supports up to 15,000 users per subcluster). A Cisco IM and Presence Active/Active deployment with a non-redundant mode requires a more detailed look at the Cisco IM and Presence Service features being utilized, the average size of the users contact lists, as well as the traffic being generated. For example, for a deployment with presence and instant messaging enabled and calendaring and mobility integration disabled, with an average contact list of 30 users and a user data profile of a few presence and instant message updates, it is possible to support more than 15,000 users per subcluster.

A Cisco IM and Presence Service cluster deployment that is not highly available allows each server in the subcluster to support up to the maximum number of users for the server, and the total number of supported users for all servers in the cluster can be up to the maximum number of users for the IM and Presence Service cluster. Once a second server is added in a subcluster, the subcluster will still act as if in a high-available deployment; however, if a server failure occurs, an attempt to fail-over might not result in success if the online server reaches its capacity limit based on the Cisco IM and Presence Service features enabled, the average user contact list size, and the traffic being generated by the users.

## On-Premises Cisco IM and Presence Service Deployment Examples

### *Example 20-1 Single Unified CM Cluster with Cisco IM and Presence Service*

Deployment requirements:

- 4,000 users that could scale up to 13,000 users
- Single Cisco Unified Communications Manager cluster
- Instant message logging and compliance are not needed
- High availability is not needed

Hardware and software platform:

- Cisco UCS virtual machine for one 15,000-user VM configuration Full UC template

Deployment:

- One single-server subcluster using User Assignment Mode for Presence Server = balanced

**Example 20-2 Two Unified CM Clusters with Cisco IM and Presence Service**

Deployment requirements:

- 11,000 users that could scale up to 24,000 users
- Two Cisco Unified Communications Manager clusters
- Instant message logging and compliance are not needed
- High availability is not needed

Hardware and software platform:

- Cisco UCS virtual machines for two 15,000-user VM configuration Full UC templates

Deployment:

- Two Cisco IM and Presence Service clusters (one per Cisco Unified Communications Manager cluster), each with one server using User Assignment Mode for Presence Server = **balanced**

**Example 20-3 Single Unified CM Cluster with Cisco IM and Presence Service**

Deployment requirements:

- 500 users that could scale up to 2500 users
- Single Cisco Unified Communications Manager cluster
- Instant message archiving is required
- High availability is required

Hardware:

- Cisco UCS virtual machines for two 5,000-user VM configuration Full UC templates

Deployment:

- One two-server subcluster using User Assignment Mode for Presence Server set to **balanced**, with a PostgreSQL, Microsoft SQL, or Oracle database instance for the cluster

**Example 20-4 Single Cisco Business Edition Cluster with Cisco IM and Presence Service**

Deployment requirements:

- 150 users that could scale up to 1,000 users
- Single Cisco Business Edition
- Instant message archiving and persistent chat are required
- High availability is required

Hardware:

- Cisco Business Edition 6000H using the 1,000-user VM configuration Full UC template

Deployment:

- One two-server subcluster using User Assignment Mode for Presence Server set to **balanced**, with a unique PostgreSQL, Microsoft SQL, or Oracle database instance per server in the cluster for persistent chat functionality

**Example 20-5 Megacluster with Cisco IM and Presence Service**

This is just an example of what megacluster deployment might consist of, if needed to deploy more than 40,000 users and/or devices.

**Note**

All deployments requiring more than 4 Unified CM subscriber pairs must be reviewed and approved by the Cisco Megacluster team prior to deployment. For more details on the megacluster approval and review process, refer to the information at <https://wiki.cisco.com/display/CCM/Megacluster>.

IM and Presence deployment requirements:

- Six nodes using the 25,000-user IM and Presence VM configuration template
- Node distributed as 3 subcluster subscriber pairs in high availability mode

Unified CM deployment requirements:

- Nineteen nodes using 10,000-user Unified CM VM configuration template
- Unified CM deployed with dedicated publisher
- Dedicated TFTP1 server and backup TFTP2 server
- Eight subscriber pair virtual nodes
- Instant message compliance is required
- High availability is required

Hardware platform:

- Cisco UCS B-Series with Unified CM 10,000-user VM configuration template and 25,000-user IM and Presence VM configuration template

**Example 20-6 Multiple Unified CM Clusters with Cisco IM and Presence Service on a Single UCS B-Series Server**

Deployment requirements:

- 75,000 users belonging to five different Unified CM clusters
- Instant message compliance is required
- High availability is required

Hardware and software platform:

- Cisco UCS B-Series with ten 15,000-user VM configuration Full UC templates

Deployment

- Five Cisco IM and Presence Service clusters in a single platform UCS B-Series, each one serving one of the five Unified CM clusters with 15,000 users each.

## On-Premises Cisco IM and Presence Service Performance

Cisco IM and Presence Service clusters support single-server as well as multi-server configurations. The maximum number of users supported for a Cisco IM and Presence Service cluster is based on the platform being used in the deployment. For example, if a Cisco IM and Presence Service cluster is deployed with three 2,000-user VM configuration templates, each forming their own subcluster, then a total of 6,000 users would be supported. For a Cisco IM and Presence Service cluster, the maximum number of full UC users supported is 75,000 and cannot exceed the maximum number of supported devices for cluster deployments. The maximum number of IM-only users supported is 75,000. For a complete list of platform requirements for the Cisco IM and Presence Service, as well as the maximum number of users supported per platform, refer to the documentation available at

[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/uc\\_system/virtualization/virtualization-cisco-ucm-im-presence.html](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html)

The Cisco IM and Presence Service supports deployments using only VM configuration templates on virtualized servers; physical server support is not available for the Cisco IM and Presence Service.

Cisco recommends using identical VM configurations for all IM and Presence nodes in a cluster. However, mixing VM configurations of different capacities within a cluster is allowed as long as the VM configuration used for the IM and Presence publisher node is of equal capacity or larger than the VM configuration used on any of the subscriber nodes in the same cluster.

Similar guidelines apply to redundancy and high availability models. Within a cluster, the VM configuration used on the IM and Presence standby and/or backup virtual subscriber node must not be larger than the VM configuration of the IM and Presence publisher or its own respective active and/or primary subscriber.

If you are mixing VM configurations within the same IM and Presence cluster, consider the possible impact to performance and capacity due to the various VM configurations being used. The overall cluster capacity might ultimately be dictated by the capacity of the smallest VM configuration within the cluster.



### Note

IM and Presence integration with Unified CM does not imply that they are part of the same cluster but rather two separate clusters.

## On-Premises Cisco IM and Presence Service Deployment

Cisco IM and Presence Service can be deployed in any of the following configurations:

- [Single-Cluster Deployment, page 20-26](#)
- [Intercluster Deployment, page 20-29](#)
- [Clustering Over the WAN, page 20-29](#)
- [Federated Deployment, page 20-36](#)

### Single-Cluster Deployment

Figure 20-11 represents the communication protocols between the Cisco IM and Presence Service, the LDAP server, and Cisco Unified Communications Manager for basic functionality. For complete information on Cisco IM and Presence Service administration and configuration, refer to the Cisco IM and Presence installation, administration, and configuration guides, available at

[https://www.cisco.com/en/US/products/ps6837/tsd\\_products\\_support\\_series\\_home.html](https://www.cisco.com/en/US/products/ps6837/tsd_products_support_series_home.html)

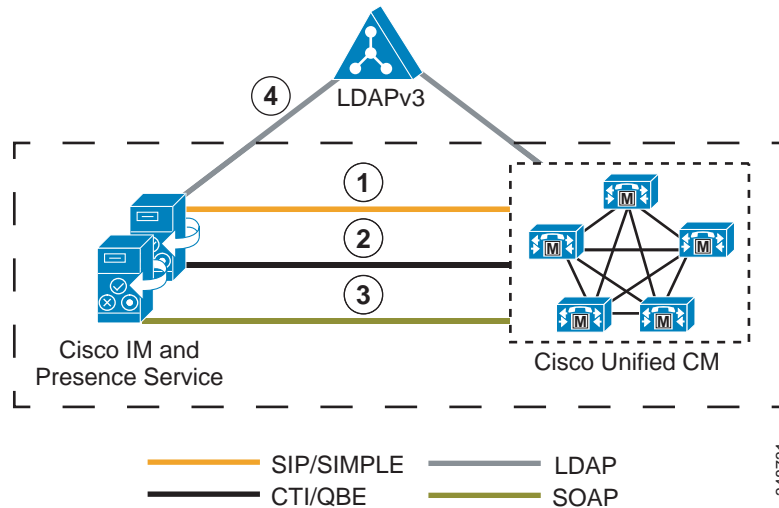
**Figure 20-11 Interactions Between Cisco IM and Presence Service Components**

Figure 20-11 depicts the following interactions between Cisco IM and Presence Service components:

1. The SIP connection between the Cisco IM and Presence Service and Unified CM handles all the phone state presence information exchange.

Unified CM configuration requires the Cisco IM and Presence Service to be added as application servers on Unified CM and also requires a SIP trunk pointing to the Cisco IM and Presence Service. The address configured on the SIP trunk could be a Domain Name System (DNS) server (SRV) fully qualified domain name (FQDN) that resolves to the Cisco IM and Presence Services, or it could simply be an IP address of an individual Cisco IM and Presence Service. The Cisco IM and Presence Service handles the configuration of the Cisco Unified Communications Manager application server entry automatically through AXL/SOAP once the administrator adds a node in the system topology page through Cisco IM and Presence Service administration.

If DNS is highly available within your network and DNS SRV is an option, configure the SIP trunk on Unified CM with a DNS SRV FQDN of the Cisco IM and Presence Service publisher and subscriber. Also configure the Presence Gateway on the Cisco IM and Presence Service with a DNS SRV FQDN of the Unified CM subscribers, equally weighted. This configuration will allow for presence messaging to be shared equally among all the servers used for presence information exchange.

If DNS is not highly available or not a viable option within your network, use IP addressing. When using an IP address, presence messaging traffic cannot be equally shared across multiple Unified CM subscribers because it points to a single subscriber.

Unified CM provides the ability to further streamline communications and reduce bandwidth utilization by means of the service parameter IMP PUBLISH Trunk, which allows for the PUBLISH method (rather than SUBSCRIBE/NOTIFY) to be configured and used on the SIP trunk interface to Cisco IM and Presence Service. Once the IMP PUBLISH Trunk service parameter has been enabled, the users must be associated with a line appearance and not just a primary extension.

2. The Computer Telephony Integration Quick Buffer Encoding (CTI-QBE) connection between Cisco IM and Presence Service and Unified CM is the protocol used by presence-enabled users in Cisco IM and Presence Service to control their associated phones registered to Unified CM. This CTI communication occurs when Cisco Jabber is using Desk Phone mode to do Click to Call or when Microsoft Office Communicator is doing Click to Call through Microsoft Office Communications Server 2007 or Microsoft Lync.

- a. Unified CM configuration requires the user to be associated with a CTI Enabled Group, and the primary extension assigned to that user must be enabled for CTI control (checkbox on the Directory Number page). The CTI Manager Service must also be activated on each of the Unified CM subscribers used for communication with the Cisco IM and Presence Service publisher and subscriber. Integration with Microsoft Office Communications Server 2007 or Microsoft Lync requires that you configure an Application User, with CTI Enabled Group and Role, on Unified CM.
- b. Cisco IM and Presence Service CTI configuration (CTI Server and Profile) for use with Cisco Jabber is automatically created during the database synchronization with Unified CM. All Cisco Jabber CTI communication occurs directly with Unified CM and not through the Cisco IM and Presence Service.

Cisco IM and Presence Service CTI configuration (Desktop Control Gateway) for use with Microsoft Office Communications Server 2007 or Microsoft Lync requires you to set the Desktop Control Gateway address (Cisco Unified Communications Manager Address) and a provider, which is the application user configured previously in Unified CM. Up to eight Cisco Unified Communications Manager Addresses can be provisioned for increased scalability. Only IP addresses can be used for Desktop Control Gateway configuration in the Cisco IM and Presence Service. Administrators should ensure that any configuration and assignment of Cisco Unified Communications Manager addresses is evenly distributed for the purpose of load balancing.

3. The AXL/SOAP interface handles the database synchronization from Unified CM to populate the Cisco IM and Presence Service database.
  - a. No additional configuration is required on Unified CM.
  - b. Cisco IM and Presence Service security configuration requires you to set a user and password for the Unified CM AXL account in the AXL configuration.

The Sync Agent Service Parameter, User Assignment, set to **balanced** by default, will load-balance all users equally across all servers within the Cisco IM and Presence Service cluster. The administrator can also manually assign users to a particular server in the Cisco IM and Presence Service cluster by changing the User Assignment service parameter to **None**.

4. The LDAP interface is used for LDAP authentication of users. For more information regarding LDAP synchronization and authentication, see the chapter on [Directory Integration and Identity Management, page 16-1](#).

Unified CM is responsible for all user entries via manual configuration or synchronization directly from LDAP, and Cisco IM and Presence Service then synchronizes all the user information from Unified CM. If a user logs into the Cisco IM and Presence Service and LDAP authentication is enabled on Unified CM, Cisco IM and Presence Service will go directly to LDAP for the user authentication using the Bind operation.

When using Microsoft Active Directory, consider the choice of parameters carefully. Performance of Cisco IM and Presence Service might be unacceptable when a large Active Directory implementation exists and the configuration uses a Domain Controller. To improve the response time of Active Directory, it might be necessary to promote the Domain Controller to a Global Catalog and configure the LDAP port as 3268.

## Intercluster Deployment

The deployment topology in previous sections is for a single Cisco IM and Presence Service cluster communicating with a single Unified CM cluster. Presence and instant messaging functionality is limited by having communications within a single cluster only. Therefore, to extend presence and instant messaging capability and functionality, these standalone clusters can be configured for peer relationships for communication between clusters within the same domain. This functionality 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.

To create a fully meshed presence topology, each Cisco IM and Presence Service cluster requires a separate peer relationship for each of the other Cisco IM and Presence Service clusters within the same domain. The address configured in this intercluster peer could be a DNS FQDN that resolves to the remote Cisco IM and Presence Service cluster servers, or it could also simply be the IP address of the Cisco IM and Presence Service cluster servers.

The interface between each Cisco IM and Presence Service cluster is two-fold, an AXL/SOAP interface and a signaling protocol interface (SIP or XMPP). The AXL/SOAP interface, between publisher-only servers of an IM and Presence Service cluster, handles the synchronization of user information for home cluster association, but it is not a full user synchronization. The signaling protocol interface (SIP or XMPP) is a full mesh between all servers within the deployment. It handles the subscription and notification traffic, and it rewrites the host portion of the URI before forwarding if the user is detected to be on a remote Cisco IM and Presence Service cluster within the same domain.

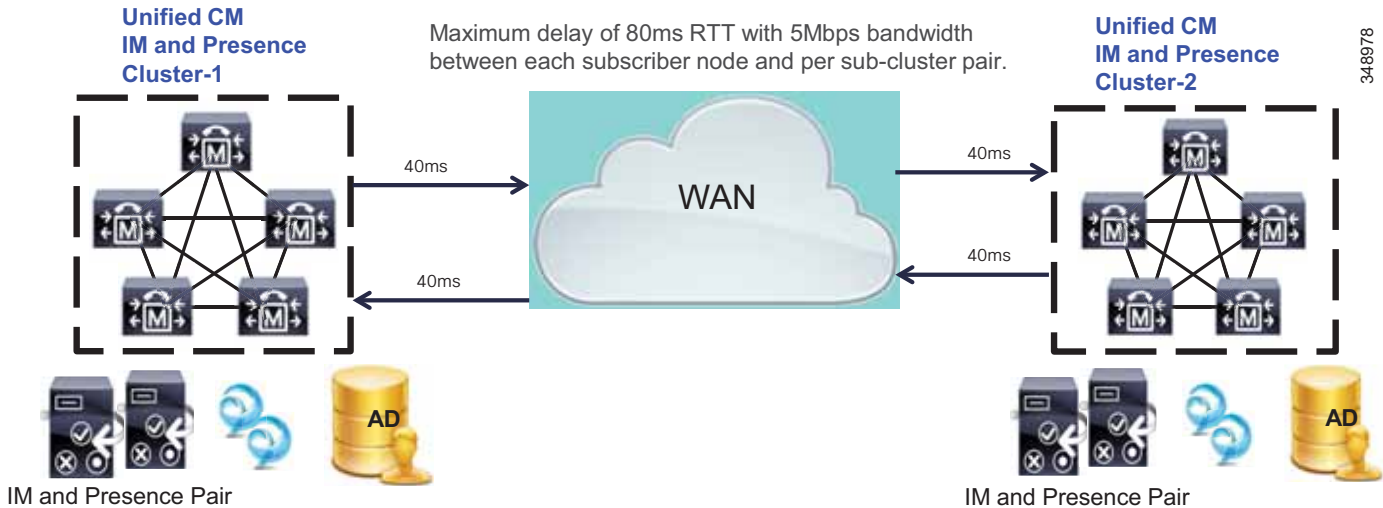
## Clustering Over the WAN

A Cisco IM and Presence Service cluster can be deployed with one of the nodes of a subcluster deployed across the Wide Area Network (WAN). This allows for geographic redundancy of a subcluster and high availability for the users between the nodes across the sites. The following guidelines must be used when planning for a Cisco IM and Presence Service deployment with clustering over the WAN.

### Geographic Data Center Redundancy and Remote Failover

A Cisco IM and Presence Service cluster can be deployed between two sites with a single subcluster topology, where one server of the subcluster is in one geographic site and the other server of the subcluster is in another site. This deployment must have a minimum bandwidth of 5 Mbps, a maximum latency of 80 ms round-trip time (RTT), and TCP method event routing (see [Figure 20-12](#)).



**Figure 20-12 Intra-Cluster Bandwidth and Delay**

### High Availability and Scale

Cisco IM and Presence Service high availability allows for users on one node within a subcluster to automatically fail-over to the other node within the subcluster. With a Cisco IM and Presence Service subcluster containing a maximum of two nodes, remote failover is essentially between two sites, one site for each node. A scalable highly available capacity for a Cisco IM and Presence Service cluster is up to three subclusters; therefore, a scalable highly available remote failover topology would consist of the following two sites:

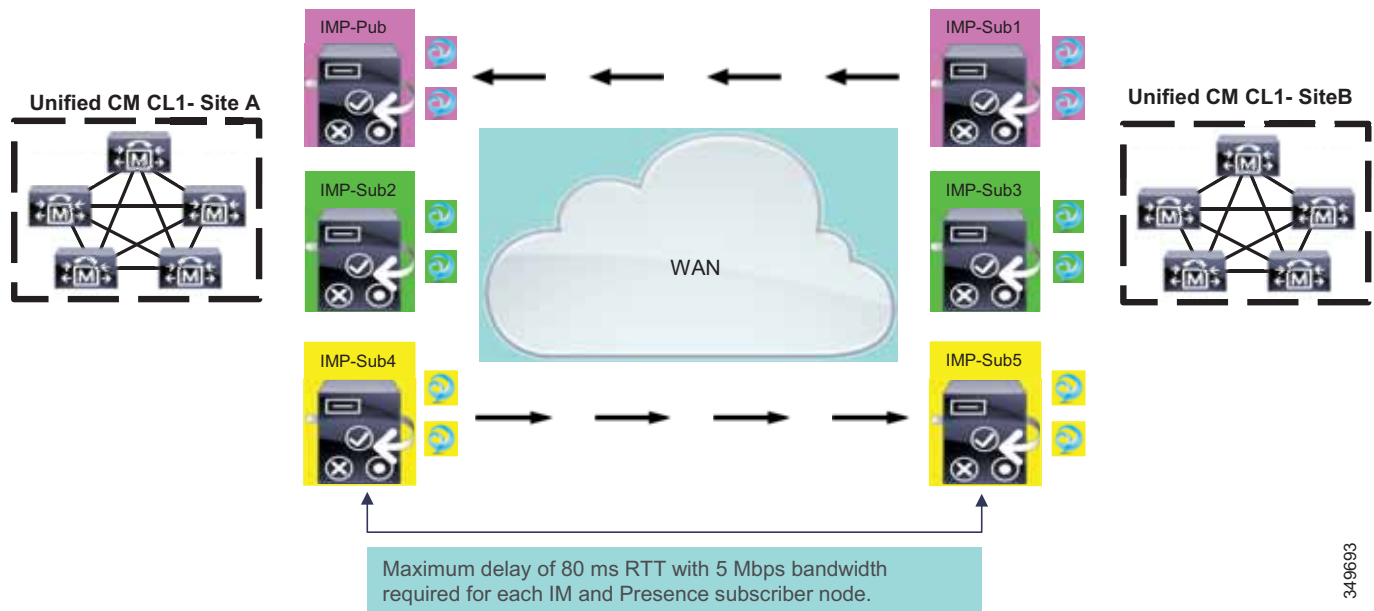
- Site A: Subcluster 1 node A, subcluster 2 node A, and subcluster 3 node A
- Site B: Subcluster 1 node B, subcluster 2 node B, and subcluster 3 node B

This deployment must have a minimum bandwidth of 5 Mbps per subcluster, a maximum latency of 80 ms round-trip time (RTT), and TCP method event routing. Each new subcluster added to the deployment requires an additional 5 Mbps of dedicated bandwidth to handle the database and state replication.

In the split subcluster model, the subcluster pairs are split across the WAN and deployed at two separate locations. The split subcluster model supports a maximum of 6 nodes deployed at 6 different locations, assuming the bandwidth and delay requirements are followed, with a maximum round-trip time (RTT) of 80 ms and 5 Mbps of bandwidth for each of the 6 nodes.

Split subcluster deployments have the following requirements:

- The Unified CM publisher and IM and Presence publisher must reside on the same side of the WAN, otherwise issues can arise with upgrades, especially with refresh (dual) upgrades.
- All IM and Presence nodes must have a minimum bandwidth of 5 Mbps, and an additional 5 Mbps for the cluster for database synchronization.
- Every IM and Presence node must also reside within and not exceed 80 ms RTT delay.
- All users must be distributed evenly across all split cluster nodes (see [Figure 20-13](#)). For example, assuming a subcluster supports 15,000 users, then each node of the split subcluster would support 7,500 on the 15k-user VM configuration template.

**Figure 20-13** IM and Presence Subcluster Split Across the WAN

349693

### Local Failover

A Cisco IM and Presence Service cluster deployment between two sites may also contain a subcluster topology per site (single node or dual node for high availability), where one subcluster is in one geographic site and the other subcluster is in another geographic site. This topology allows for the users to remain at their local site (highly available or not) without the requirement or need to fail-over to a different site or location. This deployment must have a minimum bandwidth of 5 Mbps dedicated bandwidth between each subcluster in the respective sites, a maximum latency of 80 ms round-trip time (RTT), and TCP method event routing.

### Bandwidth and Latency Considerations

With a Cisco IM and Presence Service cluster that has a topology of nodes split across a WAN, the number of contacts within a user's client can impact the bandwidth needs and criteria for the deployment. The traffic generated within and between Cisco IM and Presence Service clusters is directly proportional to the characteristics of the presence user profile, and thus the amount of bandwidth required for deployment. Cisco recommends 25% or fewer remote contacts for a client in environments where the bandwidth is low (10 Mbps or less), and at all times the maximum round-trip latency must be 80 ms or less.

### Persistent Chat and Compliance Logging Considerations

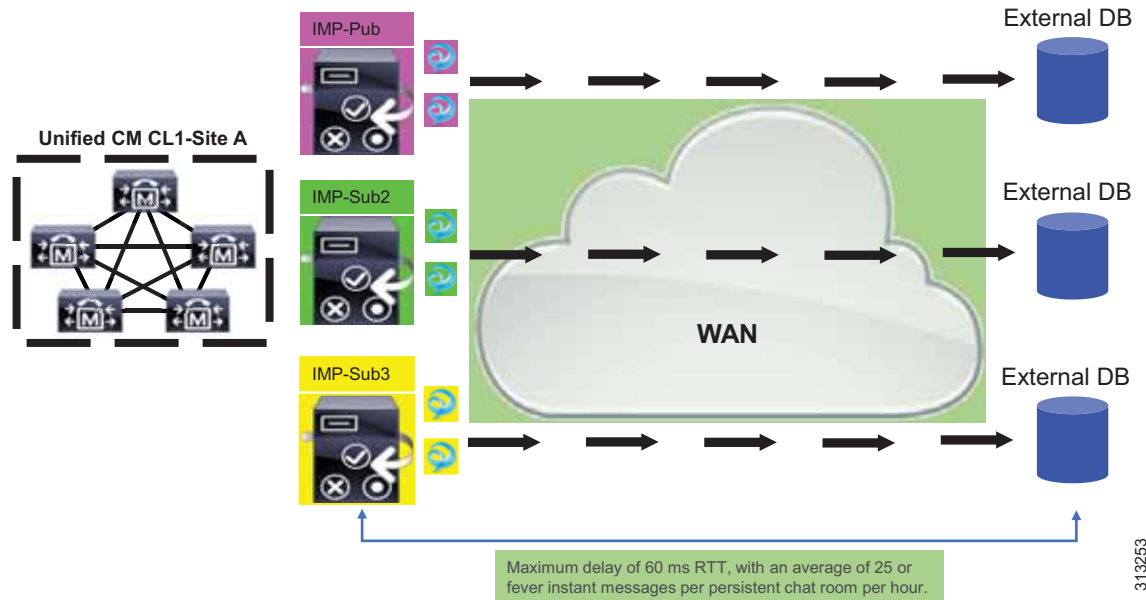
If Cisco IM and Presence Service is enabled for persistent chat, message archiving, or compliance logging, and if a subcluster is split across a WAN, then Cisco recommends placing the external database server(s) on the same side of the WAN as the Cisco IM and Presence Service subscriber node(s) with which it is associated.

With the ability to support multiple database instances on a single server and the recommendation for an external database server to reside on the same side of the WAN as its associated IM and Presence node, if a Cisco IM and Presence Service cluster is split across a WAN, then Cisco recommends deploying two external database servers as the best practice.

**Note**

It is not a requirement for an external database server and its associated IM and Presence node(s) to be located in the same data center. However, the maximum supported latency between the external database server and the IM and Presence subscriber node(s) must not be greater than 60 ms round trip time (30 ms in each direction), and the minimum bandwidth allocation must align with clustering over the WAN requirements for the Cisco IM and Presence Service. Also, the average number of instant message per persistent chat room should not exceed 25 per hour. (See [Figure 20-14](#).)

**Figure 20-14** Persistent Chat with External Database Across the WAN



313253

**Note**

Cisco recommends using Oracle Database 12c for deploying an external database across the WAN and/or for high availability.

### Centralized IM and Presence Deployments

Centralized IM and Presence can provide presence services to multiple remote Cisco Unified CM voice and video clusters. In a centralized deployment, the IM and Presence Service manages all presence related services for all the users across the remote Unified CM clusters, and each remote Unified CM cluster manages its own users' voice and video needs.

The centralized IM and Presence model provides an option for large enterprises to distribute the Unified CM clusters at multiple locations without the need to deploy an IM and Presence cluster at each of those locations. Hence, only a single centralized IM and Presence cluster is required for presence service for multiple remote Unified CM clusters.

Deployments with many locations but very few users at each location can benefit greatly from this model. For example, a hospital might have 50 locations with 100 users at each location that require voice, video, and presence service. It would not be feasible to deploy 50 clusters of Unified CM and 50 clusters of IM and Presence. Instead, a more efficient and simpler approach would be to use a single centralized IM and Presence cluster serving the 50 remote Unified CM clusters, thus greatly reducing cost with the reduction of virtual servers.

The centralized IM and Presence cluster must be deployed with the 15k/25k-user IM and Presence VM template. The Unified CM publisher for the centralized cluster must be deployed using the 10k-user Unified CM VM template. (See [Figure 20-15](#).)

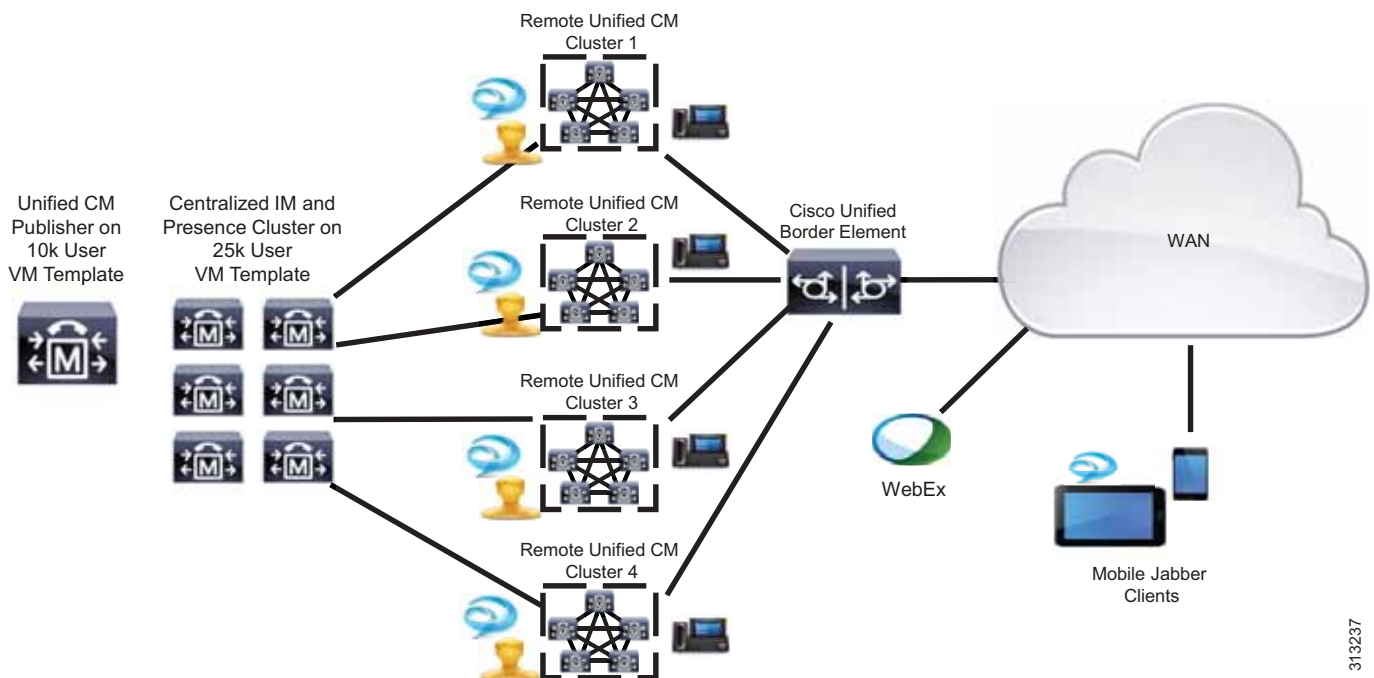
**Note**

The centralized deployment design must be reviewed and approved via the Cisco Megacluster review process when more than 40,000 clients and/or devices are deployed.

For more details on configuring a centralized IM and Presence deployment, refer to the latest version of the guide on *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*, available at

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

**Figure 20-15** Centralized IM and Presence Deployment



[Figure 20-16](#) illustrates the following login flow steps for centralized IM and Presence when single sign-on (SSO) is not used:

- Steps 1 to 2: Query DNS to get the SRV record.
- Steps 3 to 4: Query UDS to get the home Unified CM cluster.
- Steps 5 to 8: Get the Access Token and Refresh Token from the Unified CM cluster through LDAP authentication.
- Step 9: Read **UC Service Profile** -> **IM& Presence Profile** and get the IM and Presence node information.
- Step 10: The Jabber client registers to the IM and Presence cluster using the same Access Token through SOAP and XMPP interfaces.

- Step 11: The IP Multimedia Subsystem (IMS) API invokes the AuthZ service to validate the token, and the response is sent back to the Jabber client.

**Note**

The service parameter **Enable User for Unified CM IM and Presence** must be disabled (unchecked) on the remote Cisco Unified CM clusters.

**Figure 20-16** Centralized IM and Presence Login Flow without Single Sign-On (SSO)

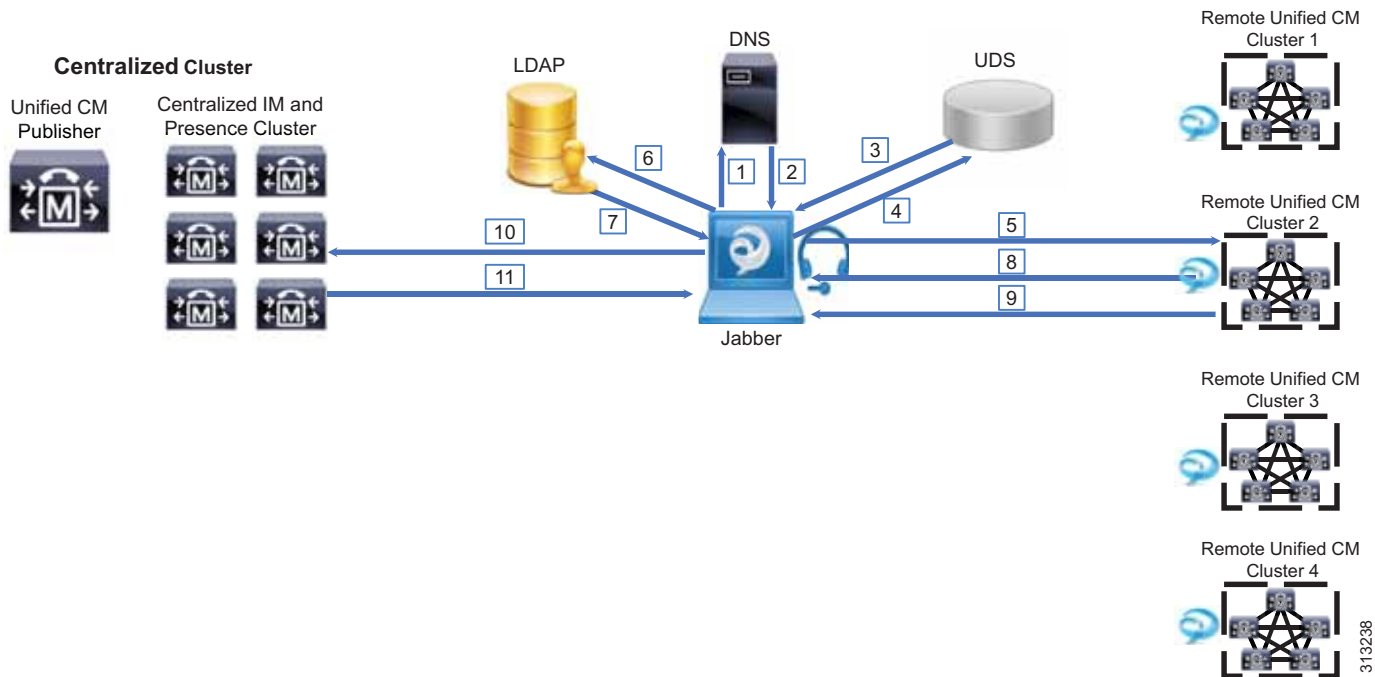


Figure 20-17 illustrates the following login flow steps for centralized IM and Presence when single sign-on (SSO) is used:

- Steps 1 to 2: Query DNS to get the SRV record.
- Steps 3 to 4: Query UDS to get the home Unified CM cluster.
- Steps 5 to 8: Get the Access Token and Refresh Token from the Unified CM cluster through Identity Provider (IdP) authentication.
- Step 9: Read **UC Service Profile -> IM & Presence Profile** and get the IM and Presence node information.
- Step 10: The Jabber client registers to the IM and Presence cluster using the same Access Token through SOAP and XMPP interfaces.
- Step 11: The IP Multimedia Subsystem (IMS) API invokes the AuthZ service to validate the token, and the response is sent back to the Jabber client.

**Note**

The service parameter **Enable User for Unified CM IM and Presence** must be disabled (unchecked) on the remote Cisco Unified CM clusters.

Figure 20-17 Centralized IM and Presence Login Flow with Single Sign-On (SSO)

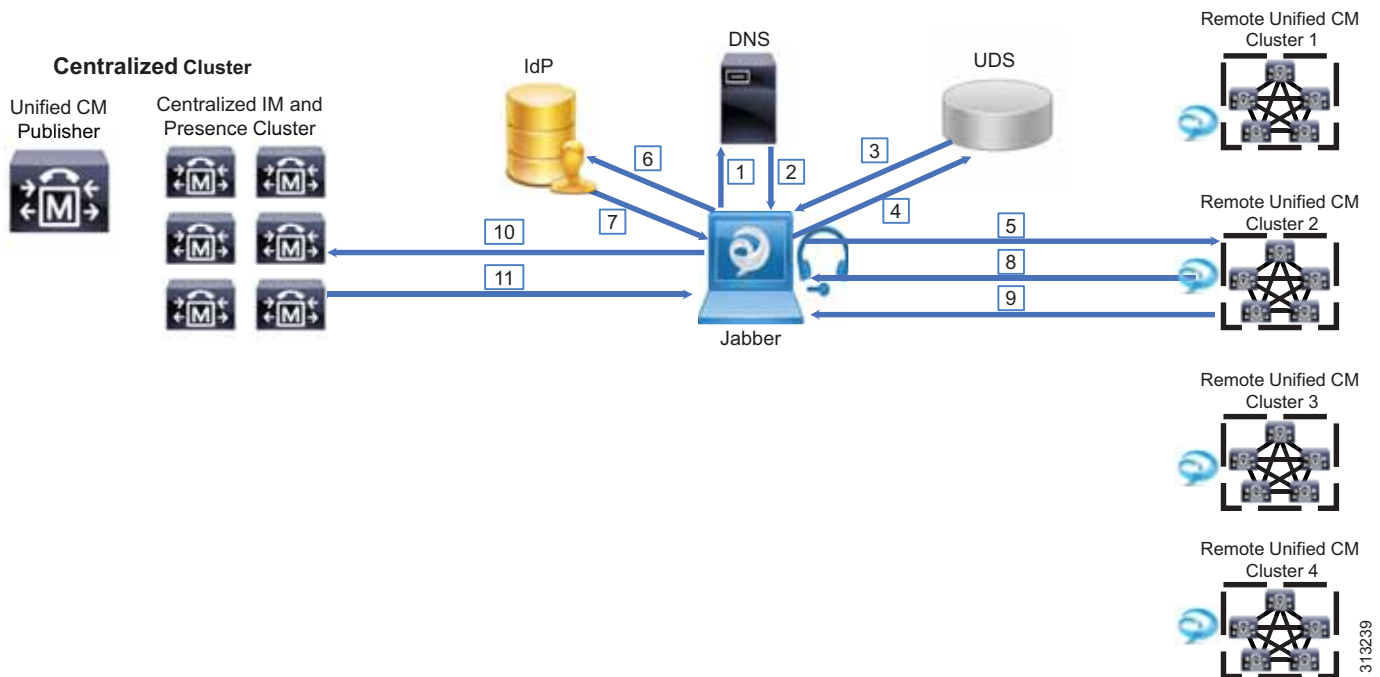
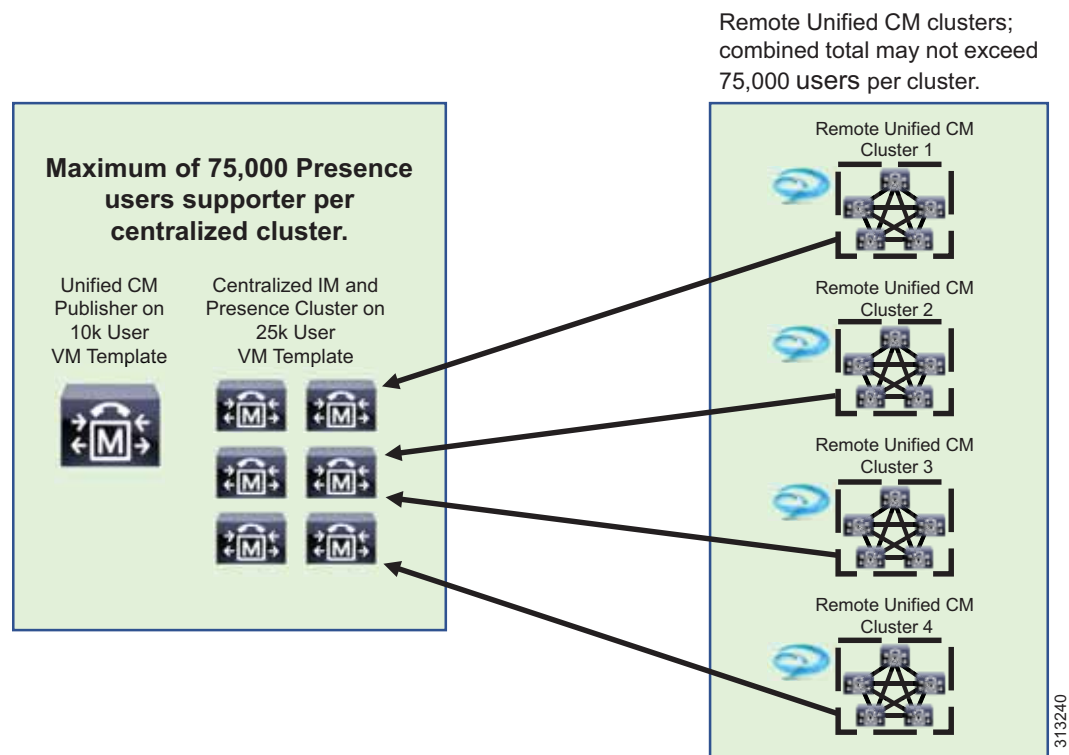


Figure 20-18 Maximum Number of Supported Users for Centralized IM and Presence



## Federated Deployment

Cisco IM and Presence Service allows for business-to-business communications by enabling inter-domain federation, which provides the ability to share presence and instant messaging communications between different domains. Inter-domain federation requires explicit DNS domains to be configured, as well as a security appliance (Cisco Adaptive Security Appliance) in the DMZ to terminate federated connections with the enterprise.

### Multi-Domain Support

The IM and Presence Service provides the ability to configure more than a single domain for federation. The domains are automatically discovered by the system when using DirectoryURI, or the administrator can add the domains manually. When a federated deployment involves multiple domains, then DNS SRV records need to be published for each email domain. Each DNS SRV record should resolve to an identical set of results where XMPP federation is a list of all XMPP federation nodes and SIP federation is the Public FQDN of the Routing IM & Presence node.

Federation with multiple email domains also requires regeneration of the security certificates `cup-xmpp` (certificate presented to XMPP clients) and `cup-xmpp-s2s` (certificate presented to federated systems). For both of these certificates, all the domains must be included as Subject Alt Name (SAN) entries. The manual administrative configuration gives the administrator the option to pre-populate the domains so that it is not necessary to regenerate the certificates every time a new domain automatically gets discovered.

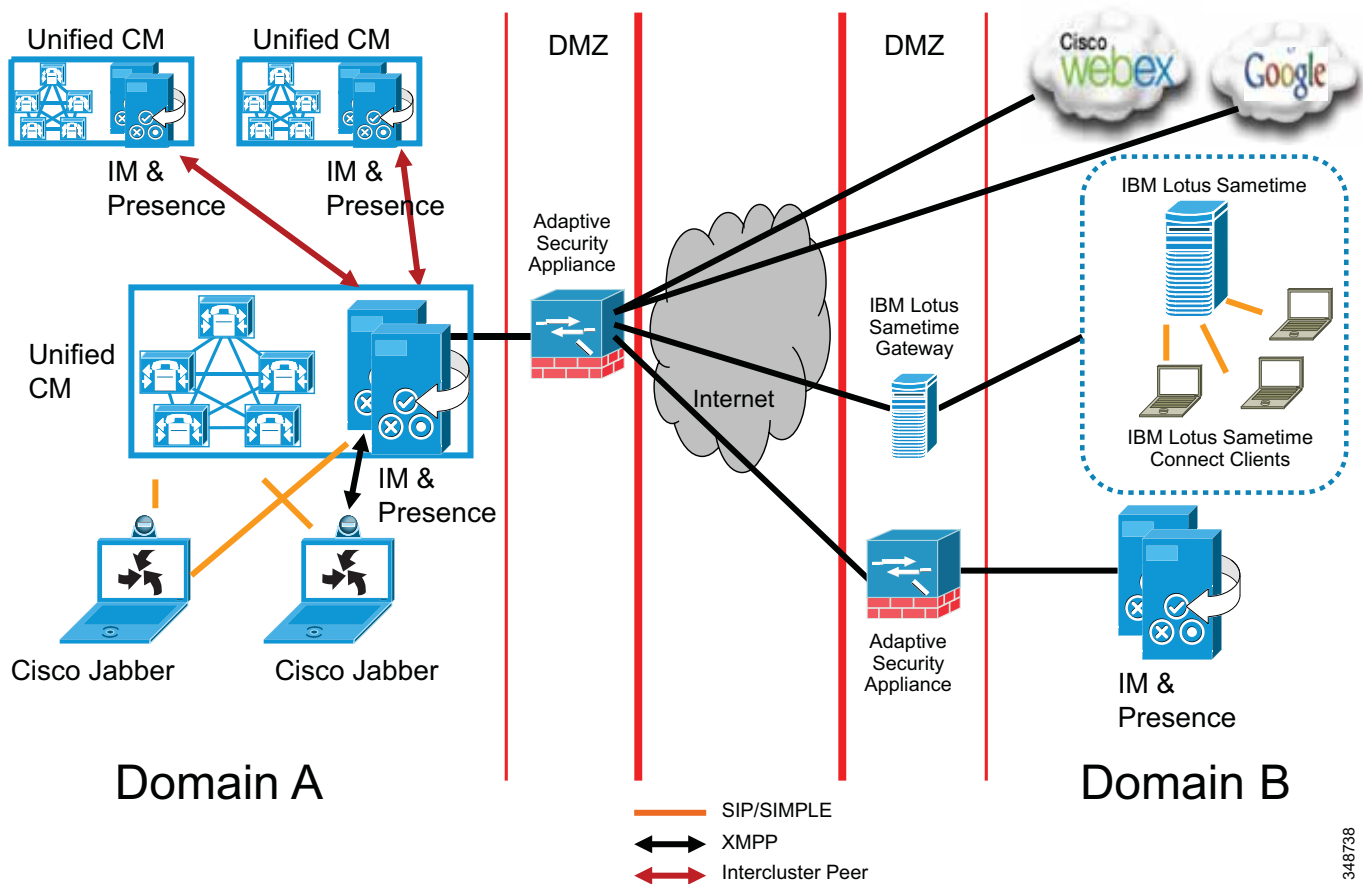
If all the federated domains are within the same trust boundary, where a deployment has all components within a single datacenter, then the use of the Adaptive Security Appliance is not required. For information on inter-domain federation, refer to the latest version of *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*, available at

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

Figure 20-19 shows the basic inter-domain federation deployment between two different domains, indicated by Domain A and Domain B. The Adaptive Security Appliance (ASA) in the DMZ is used as a demarcation into the enterprise. XMPP traffic is passed through, whereas SIP traffic is inspected. All federated incoming traffic is routed through the Cisco IM and Presence Service that is enabled as a federation node, and is routed internally to the appropriate server in the cluster where the user resides. For intercluster deployments, intercluster peers propagate the traffic to the appropriate home cluster within the domain. All federated outgoing traffic is directed outward through any node in the IM and Presence Service cluster that has XMPP federation enabled. Multiple nodes can be enabled as federation nodes within large enterprise deployments, where each request is routed based on a round-robin implementation of the data returned from the DNS SRV lookup.



Figure 20-19 IM and Presence Service XMPP Federation (Inter-Domain)

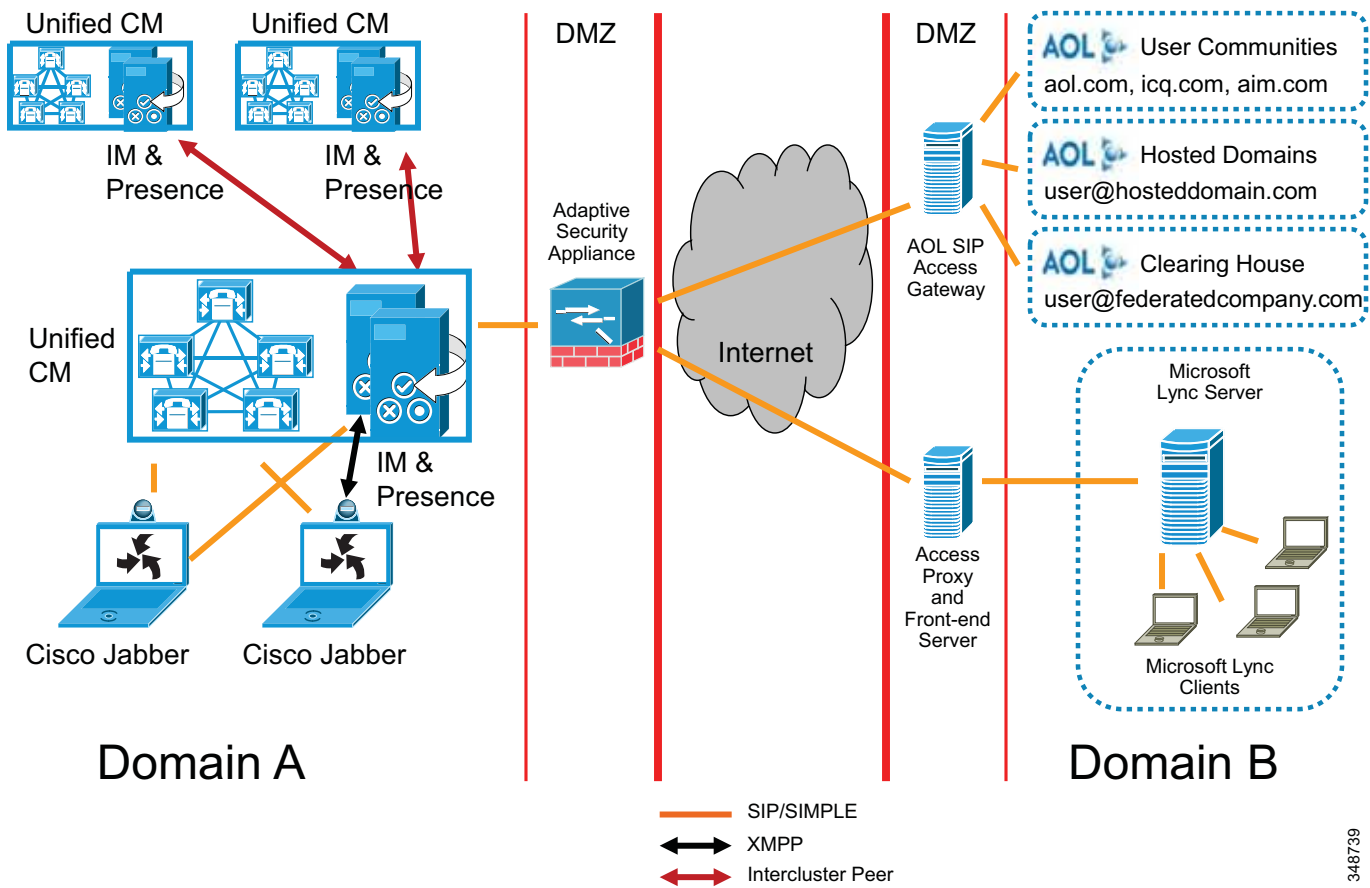


348738

Cisco IM and Presence Service also provides configuration through SIP to allow for inter-domain federation with Microsoft and AOL, as depicted in Figure 20-20. Cisco IM and Presence Service inter-domain federation with Microsoft Lync Server provides basic presence (available, away, busy, offline) and point-to-point instant messaging. Rich presence capability (On the Phone, In a Meeting, On Vacation, and so forth), as well as advanced instant messaging features, are not supported. Cisco IM and Presence Service inter-domain federation with AOL allows federation with users of AOL public communities (aim.com, aol.com), with users of domains hosted by AOL, and with users of a far-end enterprise that federates with AOL (that is, AOL is being used as a clearing house).

**Note**

A SIP federation (inter-domain to AOL) on Cisco IM and Presence Service must be configured for each domain of the AOL network, which can consist of both hosted networks and public communities. Each unique hosted domain must be configured; however, only a single aol.com public community needs to be configured because the AOL network allows a user to be addressed as user@aol.com or user@aim.com

**Figure 20-20** IM and Presence Service SIP Federation (Inter-Domain)

348739

Table 20-2 lists the state mappings between Cisco IM and Presence Service and Microsoft Lync Server.

**Table 20-2** Mapping of Presence States

Cisco Status	Cisco Color	Status to Microsoft Lync Server	Status to AOL
Do not disturb	Red	Busy	Away
Busy	Yellow	Busy	Away
On the phone	Yellow	Busy	Away
In a meeting	Yellow	Busy	Away
Idle on all clients	Yellow	Away	Away
Available	Green	Available	Available
Unavailable/offline	Grey	Offline	Offline

**Note**

Cisco IM and Presence Service must publish a DNS SRV record (SIP, XMPP, and each text conferencing node) for the domain to allow for other domains to discover the Cisco IM and Presence Services through DNS SRV. With a Microsoft Lync Server deployment, this is required because Cisco IM and Presence Service is configured as a Public IM Provider on the Access Edge server. If the Cisco IM and Presence Service cannot discover the Microsoft domain using DNS SRV, you must configure a static route on Cisco IM and Presence Service for the external domain.

The Cisco IM and Presence Service SIP federation deployment can be configured with redundancy using a load balancer between the Adaptive Security Appliance and the Cisco IM and Presence Service, or redundancy can also be achieved with a redundant Adaptive Security Appliance configuration. For XMPP federation, redundancy can be achieved using DNS SRV records.

For additional configuration and deployment considerations regarding a federated deployment, refer to the latest version of *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*, available at

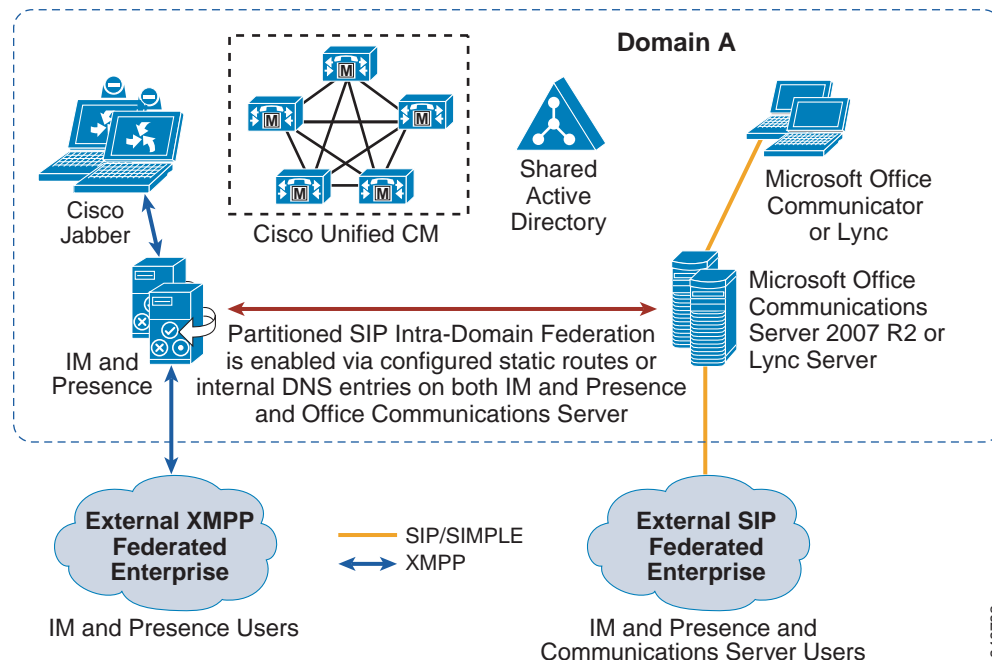
<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>

An intra-domain partitioned federated deployment, shown in Figure 20-21, is a secondary option that allows for Cisco IM and Presence Service and Microsoft Lync Server to federate presence and instant messaging within the same presence domain. The users are partitioned across both deployments, within the single presence domain, and are licensed either on Cisco IM and Presence Service or on the Microsoft Lync Server.

**Note**

The user cannot be licensed on both the Cisco and Microsoft platforms at the same time.

**Figure 20-21 Cisco IM and Presence Service Intra-Domain Federation**



348732

The partitioned intra-domain federation between the Cisco and Microsoft platforms is based on the SIP/SIMPLE protocol and allows for basic presence and instant messaging exchange, as supported with the Cisco IM and Presence Service inter-domain federation support for Microsoft. Rich presence and group chat functionality are not supported with the partitioned intra-domain presence federation.

Inter-domain federation and partitioned intra-domain federation can be supported simultaneously with the following qualifications:

- XMPP federation may be enabled on the Cisco IM and Presence Service deployment but is available only to Cisco IM and Presence Service licensed users.
- SIP federation may be enabled either on Cisco IM and Presence Service or on Microsoft Office Communications Server 2007 R2 or Lync Server; however, for SIP Federation to be available to both Cisco and Microsoft users, it must be enabled on Microsoft Office Communications Server 2007 R2 or Lync Server.
- If SIP/SIMPLE inter-domain federation with Microsoft Lync or Office Communications Server is required in parallel with the partitioned intra-domain federation, then the Microsoft Office Communications Server or Lync Server can be configured to manage that external federation. Cisco IM and Presence Service administration must be configured with static routes to the Microsoft environment for the external domain. Alternatively, Cisco IM and Presence Service could manage the SIP federation, while Microsoft Lync or Office Communications Server could manage the XMPP federation.

## On-Premises Cisco IM and Presence Service SAML SSO for Jabber



### Note

The supported end point for SAML SSO deployment is Cisco Jabber.

The Security Assertion Markup Language Single Sign-On (SAML SSO) feature enhances the end user experience by avoiding the need to log in multiple times to multiple applications within the collaboration solution.

SAML SSO provides a secure mechanism to use credentials and relevant information of the end user across multiple Unified Communications applications such as Unified CM, Cisco Unity Connection, IM and Presence, Jabber clients, and so on.

For the SAML SSO feature to work correctly, ensure that the network architecture scales to meet the number of users for each cluster, assuming that each user may have as many as five or more services that require authentication and a minimum of two devices associated to each user. For a deployment across multiple Unified Communications applications, all SAML requests must authenticate with the IdP for Cisco Jabber clients to log in successfully.



### Note

SSO is supported by Unified Communications services with SAML and OAuth only.

Cisco Jabber with SAML SSO does impact performance during logins, and the current maximum login rate for 5,000 users is within half an hour. This is assuming that you have distributed devices and users evenly across all nodes and that Cisco Jabber is in softphone mode.

Cisco Jabber is the only supported client and/or endpoint for IM and Presence deployments that supports SAML SSO.

For sizing information and examples, see the section on [SAML SSO Cisco Jabber Client, page 25-20](#), in the chapter on [Collaboration Solution Sizing Guidance, page 25-1](#).

# On-Premises Cisco IM and Presence Service Enterprise Instant Messaging

Cisco IM and Presence Service incorporates the supported enterprise instant messaging features of the Extensible Communications Platform (XCP), while allowing for some modifications to enhance support for multi-device user experience. Cisco IM and Presence Service changes the XCP instant messaging routing architecture to allow for initial instant messages to be routed to all of the user's non-negative priority logged-in devices, rather than routing to the highest priority device as is done with existing XCP installations. Backward compatibility support for point-to-point instant messaging between Cisco IM and Presence Service SIP clients and XMPP clients is provided by IM internal gateway functionality.

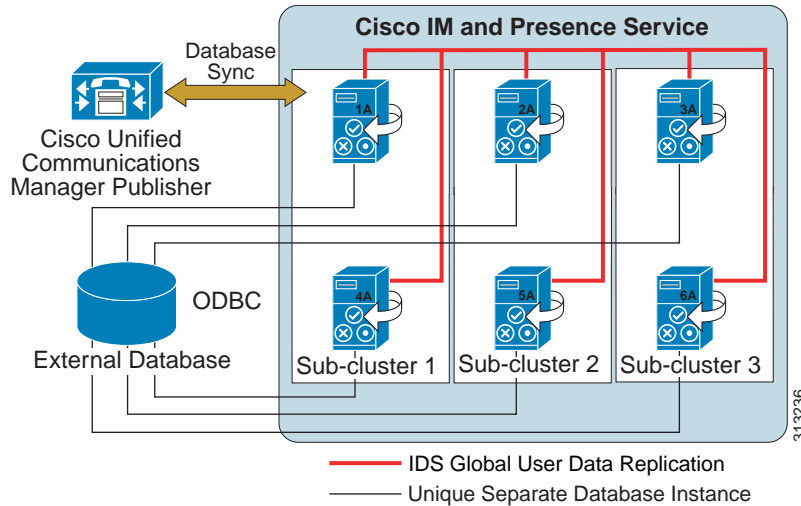
The IM and Presence Service supports IM exchange in both ad hoc chat rooms and persistent chat rooms. By default, the Text Conference (TC) component on the IM and Presence Service is set up and configured to handle IM exchange in ad hoc chat rooms.

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

Persistent chat rooms are group chat sessions that remain in existence even when all users have left the room, and they do not terminate like ad hoc group chat sessions. The intent is that users can 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, and then participate in the discussion of that topic in real-time.

For persistent chat you must have 1:1 mapping of the external database instance for each of the nodes in the cluster. The size of the database should be taken into consideration. Archiving messages is optional, and it increases the traffic on the node to which the external database instance is attached. In large deployments, disk space is a concern because it can be filled very quickly, so you must ensure that your database is large enough to handle the volume of information being logged.

Cisco IM and Presence Service uses the basic interfaces of the external database and does not provide any administration, interface hooks, or configuration of the database. Cisco requires a separate database instance for each server in the cluster when Cisco IM and Presence Service is deployed with persistent group chat. (See [Figure 20-22](#).) The database instances can share the same hardware but are not required to do so.

**Figure 20-22 Cisco IM and Presence Service Persistent Chat**

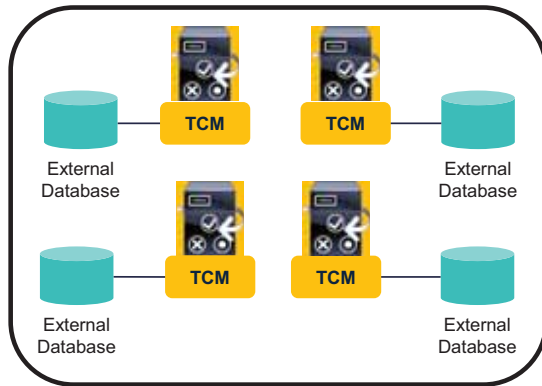
If persistent chat is enabled, an external database must be associated with the Cisco XCP Text Conference Manager service, and the database must be active and reachable otherwise the Text Conference Manager service will not start. If the connection with the external database fails after the Text Conference Manager service has started, the Text Conference Manager service will remain active and functional; however, messages will no longer be written to the database, and new persistent chat rooms cannot be created until the connection recovers.

## Deployment Considerations for Persistent Chat

- Persistent chat can be deployed on one or more nodes in a cluster (see [Figure 20-23](#)).
- Each node that supports persistent chat must be assigned to a dedicated database instance.
- An external database server may support multiple database instances.
- Persistent chat is a cluster-wide setting.
- At least one node in the cluster must be assigned to an external database.
- The Cisco XCP Text Conference Manager service will not run on a node that is not assigned to an external database.
- Pure instant (ad hoc) conferencing does not require any external database.

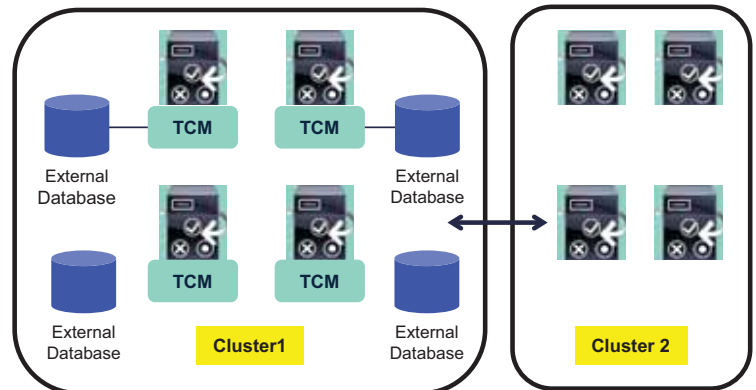
**Figure 20-23 Persistent Chat Deployment**

IM and Presence cluster with Cisco XCP Text Conference Manager (TCM) on 4 nodes, but it can run on up to 6 nodes.



Users can create or join chat rooms on any node.

IM and Presence clusters with Cisco XCP Text Conference Manager (TCM) on one cluster only.



Users in Cluster 2 can create or use chat rooms on any node in Cluster 1.

349692

## Chat Room Limits for IM and Presence Service

The IM and Presence Service supports point-to-point file transfer between XMPP clients. Table 20-3 lists the chat room limits for the IM and Presence Service

**Table 20-3 Chat Room Limits for IM and Presence Service**

Number of	Maximum
Persistent chat rooms per node	1,500 rooms
Total rooms per node (ad hoc and persistent)	16,500 rooms
Occupants per room	1,000 occupants
Messages retrieved from the archive. This is the maximum 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

Text conferencing, sometimes referred to as multi-user chat, is defined as ad-hoc group chat and persistent group chat and is supported as part of the XCP feature set. In addition, offline instant messaging (storing instant messages for users who are currently offline) is also supported as part of the XCP feature set. Cisco IM and Presence Service handles storage for each of these instant messaging features in different locations. Offline instant messaging is stored locally in the Cisco IM and Presence Service IDS database.

Ad-hoc group chat is stored locally in memory on the Cisco IM and Presence Service. Persistent group chat requires an external database to store chat rooms and conversations. The external databases supported are PostgreSQL (see <https://www.postgresql.org/>), Microsoft SQL, and Oracle (see <https://www.oracle.com>).



**Note**

Cisco does not provide any database best practices or any data extraction tools. Those tasks and tools are expected to be provided by a database administrator.

**Note**

When Oracle is used as the external database, tablespace information must be configured.

## Managed File Transfer

Managed file transfer (MFT) allows an IM and Presence Service client such as Cisco Jabber to transfer files to other users, ad hoc group chat rooms, and persistent chat rooms. The files are stored in a repository on an external file server, and the transaction is logged to an external database.

This configuration is specific to file transfers and has no impact on the message archiver feature for regulatory compliance.

**Note**

There is no high availability solution for MFT or persistent chat because there is only one connection from the IM and Presence node to each external third-party database.

### Software

- Cisco IM and Presence Service, Release 10.5(2) or later
- PostgreSQL or Microsoft SQL
- Oracle, versions 9i, 10g, or 11g
- File server versions Centos 6.5 or greater

**Note**

Oracle Data Guard may be used as an external database, but it has not been tested by Cisco.

**Note**

If you are required to have an encrypted connection to the external database, you must use Oracle 11g. No other supported database version allows encrypted connections.

You can install the database on either a Linux or a Windows operating system. See the PostgreSQL, Microsoft SQL, and Oracle documentation for details on the supported operating systems and platform requirements.

IPv4 and IPv6 are supported, as is dual-stack mode.

### Transfer Process

The flow for transferring a file to a single recipient involves the following steps:

1. The sender's client uploads the file via HTTP, and the server responds with a URI for the file.
2. The file is stored in the repository on the file server.
3. An entry is written to the external database log table to record the upload.
4. The sender's client sends an IM to the recipient; the IM includes the URI of the file.
5. The recipient's client requests the file via HTTP.

6. The file is read (retrieved) from the repository.
7. The download request is recorded in the log table.
8. The file is downloaded to the recipient.

The flow for transferring a file to a group chat or persistent chat room is similar, except that the sender sends the IM to the chat room, and each chat room participant sends a separate request to download the file.

## Managed File Transfer on IM and Presence Service

When you enable managed file transfer on an IM and Presence Service node, consider the following information:

- If you deploy any combination of the persistent group chat, message archiver, or managed file transfer features on an IM and Presence Service node, you can assign the same physical external database installation and file server to all of these features. However, you should consider the potential IM traffic and file transfers (size and number) when you determine the server capacity.
- The node public key is invalidated if the node's assignment is removed. If the node is reassigned at a later date, a new node public key is automatically regenerated. The external file server will also need to be reconfigured.
- The Cisco XCP File Transfer Manager service must be active on each node where managed file transfer is required.

## Managed File Transfer Capacities

All Jabber users have the option to transfer files at will, which can potentially impact the system based on the file transfer usage. Refer to [Table 20-4](#) to help calculate your capacity needs.

The values in [Table 20-4](#) are based strictly on a transferred file size of 500 kilobytes (KB). These value may be adjusted to calculate different capacities; for example, any one of the following scenarios is equivalent to 1,500 transfers per hour:

- 1,500 users, each downloading or uploading a single 500 KB file in an hour
- 3,000 users, each transferring a 250 KB file per hour
- 750 Jabber users sending a single 500 KB file to 750 other Jabber users

The maximum number of supported transfers is 12,000 with a 500 KB file.

**Table 20-4** *Jabber File Transfer Capacities*

Usage Level	Transfers per Hour	CPU % Total	CPU % AFT	AFT_LOG Table	AFT_LOG Size	JM Table Additional Size
Low usage	1,500	35%	25%	3,000	0.6 MB	1.5 MB
Medium usage	4,500	50%	40%	9,000	2.8 MB	4.5 MB
Maximum usage	12,000	65%+	55%	24,000	7.8 MB	12.0 MB

The File Transfer window has the following File Transfer Type controls:

- 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 and Persistent Group Chat both require an external database instance per IM and Presence node in an IM and Presence cluster.



#### Note

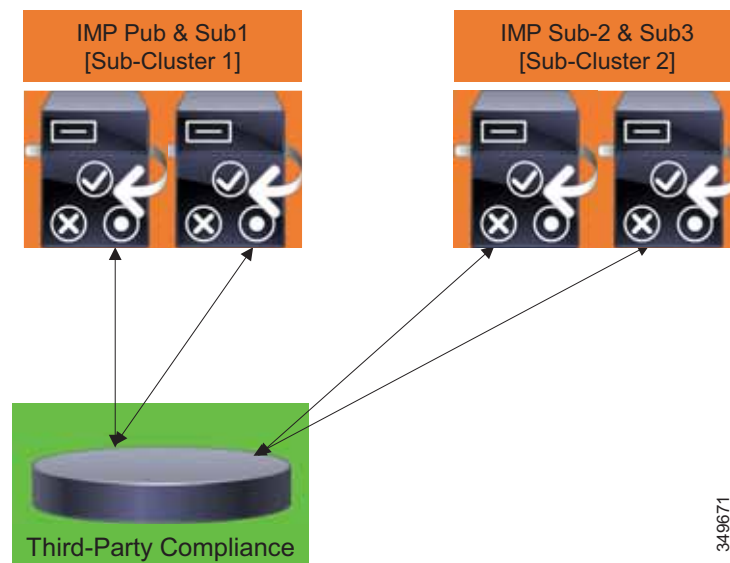
A node that has Managed File Transfer enabled should not be deployed in a cluster with a node that has Peer-to-Peer enabled. The recommended migration path is to configure the Peer-to-Peer nodes as Managed and Peer-to-Peer File Transfer nodes, and then change them to Managed File Transfer nodes.

## On-Premises Cisco IM and Presence Service Message Archiving and Compliance

As part of the architecture, Cisco IM and Presence Service contains a Message Archiver component that allows for logging of point-to-point, text conferencing, federated, and intercluster messages into an external database as part of a non-blocking compliance. Cisco IM and Presence Service message archival requires an external database (PostgreSQL, Microsoft SQL, or Oracle) instance per cluster. The same database can be shared with multiple clusters; however, a large number of users in a intercluster peer deployment would require more database instances due to capacity demands and a high number of data inserts. Although one external database instance per IM and Presence cluster is supported, the minimum recommendation is to deploy one external database instance per sub-cluster pair.

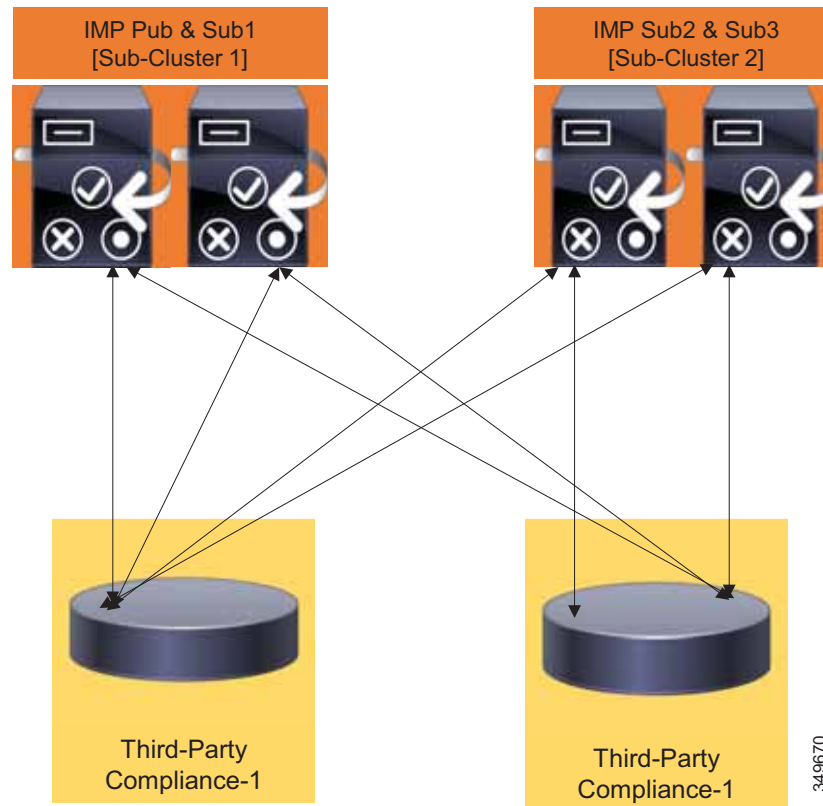
A blocking third-party compliance solution, which not only allows logging of messages but also applies policy to message delivery and message content, is provided through a third-party compliance server solution, as illustrated in [Figure 20-24](#). Cisco IM and Presence Service third-party compliance can be deployed with multiple compliance servers for each server in the cluster, multiple servers per compliance server, or some other combination. Use of a third-party compliance solution is mutually exclusive with using the Message Archiver feature.

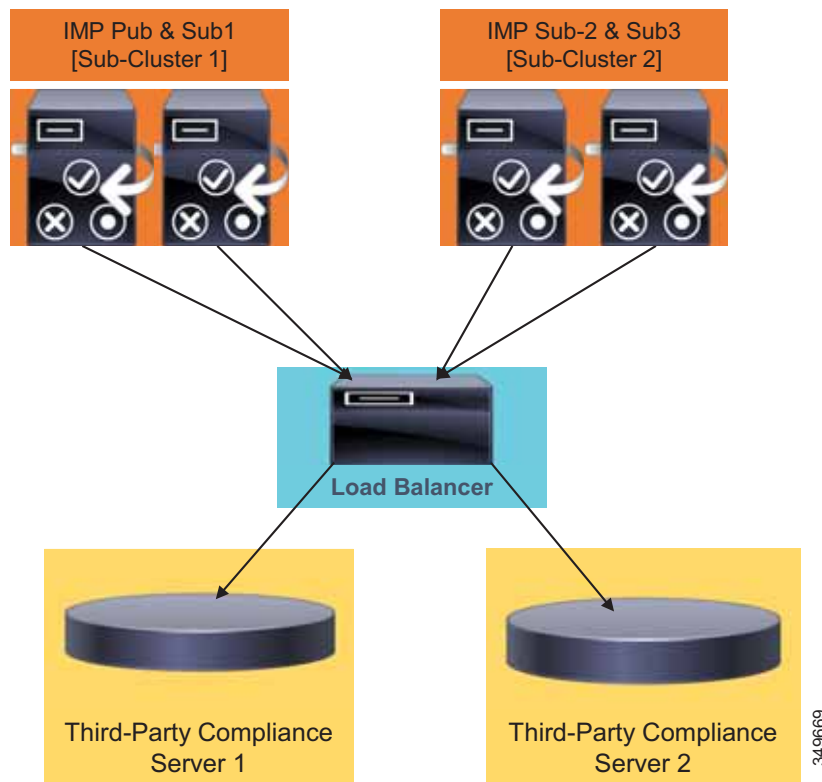
**Figure 20-24** On-Premises Cisco IM and Presence Service: Third-Party Compliance



All Cisco IM and Presence Service servers in the cluster are subject to compliance. [Figure 20-25](#) shows a deployment with a compliance server for each server in the IM and Presence Service cluster; whereas [Figure 20-26](#) shows a mapping of a single compliance server to multiple IM and Presence Service servers, or multiple compliance servers to a single IM and Presence Service server. The various deployment options allow for greater flexibility in compliance policy routing and cluster deployment.

**Figure 20-25** Cisco IM and Presence Service Third-Party Compliance



**Figure 20-26 Full High Availability Cluster-Wide Compliance**

Cluster-wide compliance allows for configuration of compliance profiles based on particular events, while allowing those events to be prioritized and routed to the appropriate compliance servers when there are overlapping events in the compliance profiles. Every compliance server must have a compliance profile assigned, and multiple compliance servers can share the same compliance profile.

Requirements for the IM and Presence Service external database differ depending on the feature(s) utilized. For example, enabling the Persistent Group Chat feature requires an external database for each IM and Presence sub-cluster pair, where every IM and Presence sub-cluster pair in the cluster points to a unique database instance but can share the same physical database installation.

The Message Archiver (compliance) feature requires at least one external database instance per IM and Presence cluster. The recommendation, however, is to have 1:1 mapping with two external database instances per sub-cluster pair and to define each IM and Presence node in the compliance profile assigned to the respective compliance server(s).

The Managed File Transfer feature requires one unique logical external database instance for each IM and Presence Service node in an IM and Presence Service cluster that has the Cisco XCP File Transfer Manager service activated.

**Note**

If you deploy any combination of the persistent group chat, message archiver (compliance), and managed file transfer features on an IM and Presence Service node, you can assign the same external database to each feature.

### Collaboration Client Message Logging Storage Requirements

The message archiving and Persistent Chat functionality use an external database to store messages offline. There are a number of factors to consider for the storage requirements of a deployment, such as the customer topology, how the database is tuned, and how messaging is used within the organization. The following calculations provide guidelines for these inputs to be used in estimating the raw database storage requirements of a deployment for external database storage.

Cisco IM and Presence Service supports both SIP and XMPP clients, and there are slightly different amounts of overhead per message based on the protocol. The overhead per message for message archiving could actually be larger or smaller depending on deployment, Jabber Identifier/UserID size, client type, and thread ID; therefore, an average overhead amount is used. For SIP-based messages the average overhead is 800 bytes and for XMPP messages the average overhead is 600 bytes.

The minimum storage requirements (in bytes) for message archiving per month for Cisco Jabber users can be calculated as follows:

$$(\text{Number of users}) * (\text{Number of messages/hour}) * (\text{Number of busy hours/month}) * (600 + (3 * \text{Number of characters/message}))$$

The message archiving requirements above must be doubled if **Enable Outbound Message Logging** is enabled on Cisco IM and Presence Service compliance configuration.

The minimum storage requirements (in bytes) for persistent chat per month for Cisco Jabber users can be calculated as follows:

$$(\text{Number of users}) * (\text{Number of Persistent Chat messages/hour}) * (\text{Number of busy hours/month}) * (700 + (3 * \text{Number of characters/message}))$$



#### Note

Persistent Chat is supported only with XMPP clients and uses an average overhead of 700 bytes.

[Table 20-5](#) provides an example spreadsheet to assist in determining the database space requirements. These calculations are provided as a very simplified calculation. This example does not attempt to provide any differentiation between database types or how storage may be used.

**Table 20-5** Example Spreadsheet for Estimating Database Storage Requirements

	A	B	C	D	E
1	Description	Message Archiver	Persistent Chat	Managed File Transfer	Total
2	Feature Enabled	Yes	Yes	Yes	
3	Message Archiver Outbound Message Logging Enabled	No			
4	Number of users	2500	2500	2500	
5	Estimated number of messages per hour per user	15	15	2	
6	Number of busy hours per month	200	200	200	
7	Average number of characters per message	250	250	250	
8	XMPP message overhead bytes per message	600	700	600	
9	Database text message encoding factor	3	3	3	
10	Percent buffer allowance multiplier	150.00%	150.00%	150.00%	
11	<b>Computations</b>				
12	Number of messages per month	7,500,000	7,500,000	1,000,000	16,000,000
13	Formula for above calculation	IF(B2="Yes", IF(B3="Yes", 2,1)* ROUNDUP(B4*B5*B6,0),0)	IF(C2="Yes", ROUNDUP(C4*C5*C6, 0),0)	IF(D2="Yes", ROUNDUP(D4*D5*D6, 0),0)	
14	Estimated total GBs storage used per month	9.9	10.7	1.4	22.0
15	Formula for above calculation	ROUNDUP((B12*((B7*B9)+B8))/1024000000,1)	ROUNDUP((C12*((C7*C9)+C8))/1024000000,1)	ROUNDUP((D12*((D7*D9)+D8))/1024000000,1)	
16	Estimated total database GBs to provision per month	14.9	16.1	2.1	33.1

These message archive and Persistent Chat numbers are the minimum storage requirements based on an average over time; therefore, a buffer multiplier of 1.5 (150%) should be used to account for very large UserIDs, larger than expected instant message lengths, and other factors that tend to increase the storage requirements. [Table 20-6](#) lists some examples of storage requirements for Cisco Collaboration Clients.



**Table 20-6**      *Examples of Cisco Collaboration Client Message Logging Storage Requirements*

Profile	Number of Users	Number of Messages per Hours	Number of Busy Hours per Month	Average Size of Message	Message Archive Storage Requirement	Persistent Chat Storage Requirement
Light	1,500	10	200	100	2.7 GB	3.0 GB
Medium	2,500	15	200	250	9.9 GB	10.7 GB
High	2,500	25	200	500	25.7 GB	26.9 GB

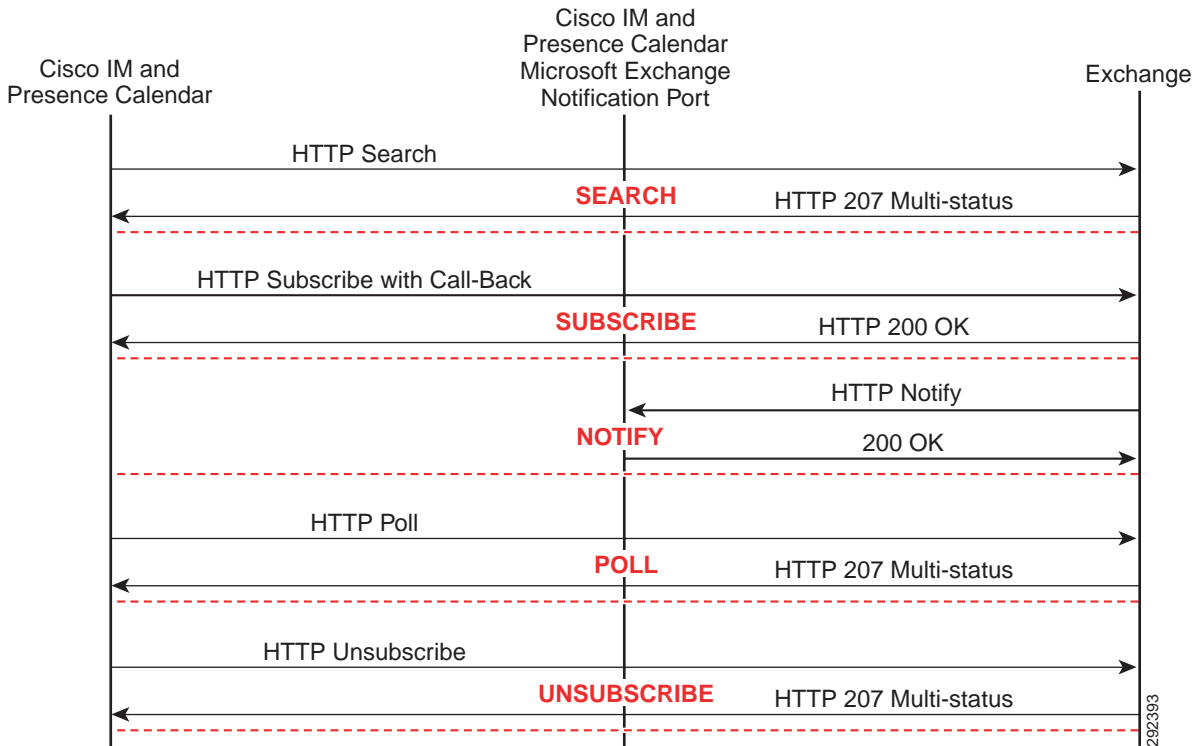
## On-Premises Cisco IM and Presence Service Calendar Integration

Cisco IM and Presence Service has the ability to retrieve calendar state and aggregate it into a presence status via the calendar module interface with Microsoft Exchange 2010 or 2013 server side integration. Cisco does not provide configuration, deployment, or best practice procedures for Microsoft Exchange, but Cisco does provide the guidelines listed in this section for integrating Cisco IM and Presence Service with the calendar module interface of Microsoft Exchange 2010 or 2013.

Microsoft Exchange integration is supported with Microsoft Active Directory 2008 and Active Directory 2012 as well as Windows Server 2008 and Windows Server 2012. Microsoft Exchange 2010 or 2013 makes the calendar data available from the server through Exchange Web Services (EWS), which allows submitting requests and receiving notifications from Microsoft Exchange. The integration with Microsoft Exchange is done through a separate Presence Gateway configuration for calendar applications. Once the administrator configures a Presence Gateway for Outlook, the user has the ability to enable or disable the aggregation of calendar information into their presence status.

The exchange ID that is used to retrieve calendar information is taken from the email ID of the LDAP structure for that user. If the email ID does not exist or if LDAP is not being used, then the Cisco IM and Presence Service user ID is mapped as the exchange ID.

Information is gathered via a subscription for calendar state from the Cisco IM and Presence Service to the Microsoft Exchange server. [Figure 20-27](#) depicts this communication.

**Figure 20-27** Outlook Web Access Communication Between Cisco IM and Presence Service and Microsoft Exchange

## Microsoft Outlook Calendar Integration

The IM and Presence Service can incorporate Microsoft Outlook Calendar free and busy data when publishing a user's availability. This feature helps users automatically maintain their availability and status information. Because it is based on a server-to-server integration, it is available to other users whether or not the originating user is logged in. The Microsoft Outlook Calendar feature requires the establishment of a gateway connection to the Microsoft Exchange Server and is compatible with Microsoft Exchange Servers 2003, 2007, and 2010.



### Note

Cisco IM and Presence Service can be deployed with a single Microsoft Exchange Server or with multiple Microsoft Exchange Servers, in a single forest only. Microsoft Exchange deployment allows for clustering of multiple Exchange servers; therefore, Cisco IM and Presence Service will honor the REDIRECT message to the exchange server that is hosting the user for which Cisco IM and Presence Service is requesting status.

## Multi-Language Calendar Support

In cases where the requirements for a calendar integration deployment specify more than one language, use the following design guidelines:

- Cisco IM and Presence Service, as well as Cisco Unified Communications Manager, must have the appropriate locales installed for the users to select their locale.
- Cisco IM and Presence Service supports all the standard Unified Communications locales for calendar integration.
- Users must be configured for the locale that is desired, either through the end user pages or administratively through the Bulk Administration Tool.
- Cisco IM and Presence Service sends the appropriate locale folder with the initial query. Queries are redirected, if required, through the response of the initial Front-End or Client Access Microsoft Exchange server.

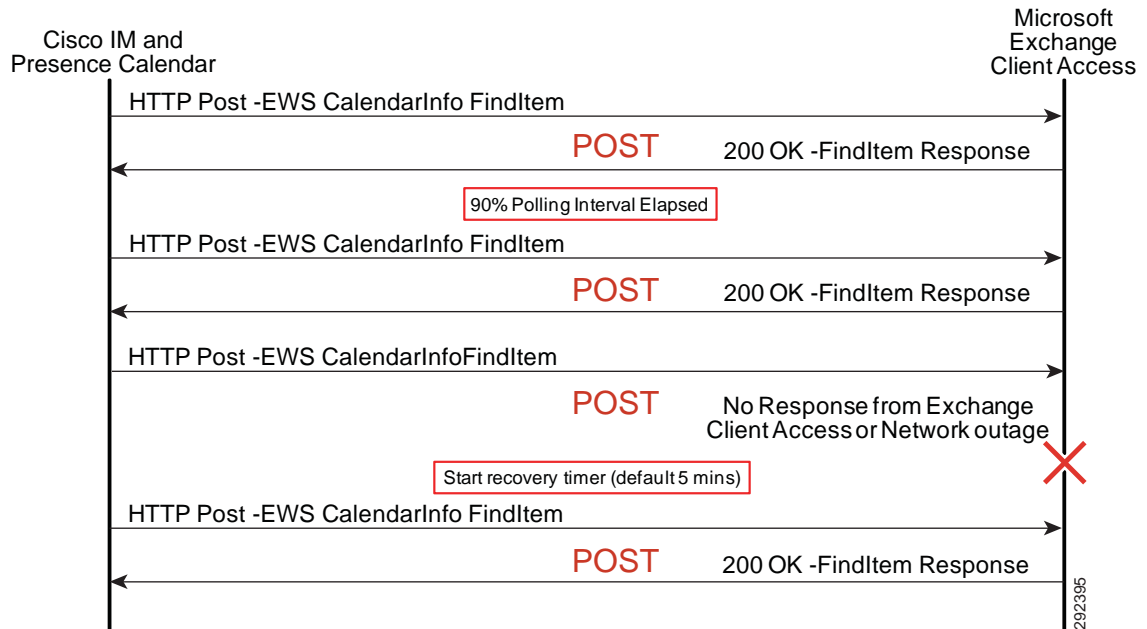
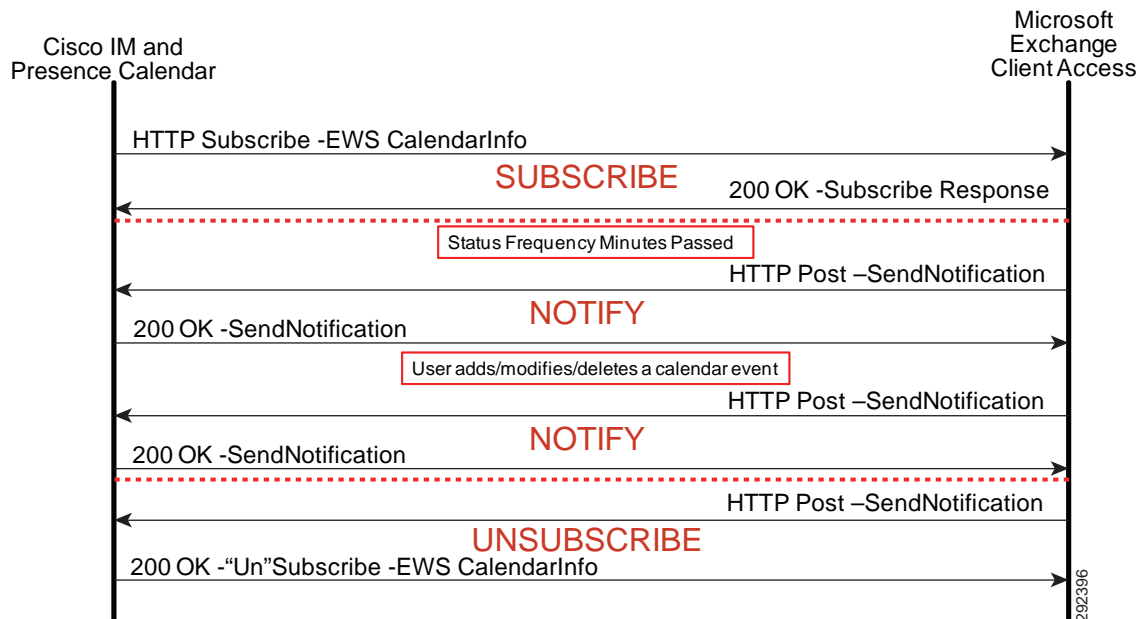
## Exchange Web Services Calendar Integration

Cisco IM and Presence Service can be configured to allow for Microsoft Exchange Web Services to collect calendar state information to be aggregated into an overall presence view of the user. If the users mailbox is located on the configured Exchange server, Cisco IM and Presence Service will communicate directly with the Exchange server; whereas, if the users mailbox is located on a different Exchange server than the one configured, Cisco IM and Presence Service will follow the Exchange server redirection to find the server where the users mailbox is located. Only Exchange Servers from the server farm can serve as the configured Exchange server, and you are required to specify only one of these servers from the server farm.

Microsoft Exchange Web Services specifies the protocol used to transact with the Exchange Client Access Servers independent of the language that the end-user uses; therefore, there is no need to utilize the locale to determine the language of the end-user. Cisco IM and Presence Service calendar integration is supported with a single Microsoft Exchange forest only.

Cisco IM and Presence Exchange Web Services calendar integration supports both a polling of calendar information as shown in [Figure 20-28](#) as well as a subscription/notification for calendar information as shown in [Figure 20-29](#). Various configuration parameters control the rate of polling intervals, the frequency of subscriptions, and the fault tolerance of timers. For additional configuration details, refer to the *Integration Note for Configuring Cisco IM and Presence with Microsoft Exchange*, available at

[https://www.cisco.com/en/US/products/ps6837/products\\_installation\\_and\\_configuration\\_guides\\_list.html](https://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html)

**Figure 20-28** Exchange Web Services Polling with Cisco IM and Presence Service Calendar**Figure 20-29** Exchange Web Services Subscription/Notification with Cisco IM and Presence Service Calendar

Exchange Web Services Auto Discover is also supported by Cisco IM and Presence Service if a service connection point (SCP) Active Directory object has been created for each server where the Client Access Server (CAS) role is installed. The calendar gateway is configured with Auto Discover using the domain

and optionally the site instead of a host and port. Cisco IM and Presence Service uses the auto-discover algorithm to determine which Exchange Web Services URL to use in contacting the correct Client Access Server Exchange Server.

## On-Premises Cisco IM and Presence Service Mobility Integration

Cisco IM and Presence Service has the ability to integrate contact lists and presence state with Cisco Jabber Mobile IM. Jabber Mobile IM continues to communicate directly with Cisco Unified CM, while Cisco Unified CM communicates with Cisco IM and Presence Service via AXL/SOAP and SIP.

An application user must be configured on Cisco IM and Presence Service and Cisco Unified CM before Cisco Unified CM can establish an administrative session with Cisco IM and Presence Service. Cisco Jabber Mobile IM end-user logins will generate a Cisco Unified CM SOAP request to Cisco IM and Presence Service for system configuration, user configuration, contact list, presence rules, and application dial rules, followed by Unified Communicator Change Notifier (UCCN) configuration and Presence SIP subscriptions.

## On-Premises Cisco IM and Presence Service Third-Party Open API

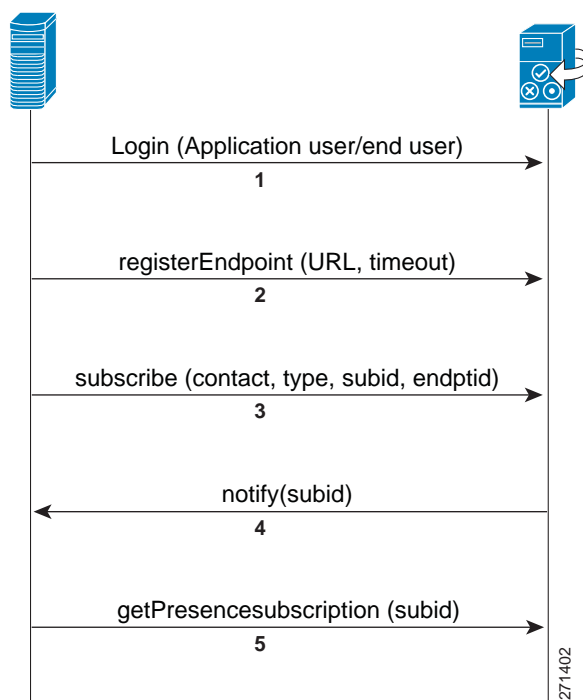
Cisco IM and Presence Service has the ability to integrate with third-party applications through HTTP in addition to SIP/SIMPLE and XMPP. The HTTP interface has a configuration interface as well as a presence interface via Representational State Transfer (REST). The Third-Party Open API provides two mechanisms to access presence: a real-time eventing model and a polling model.

For more information on the Third-Party Open API, refer to the Cisco Developer Community at

<https://developer.cisco.com/web/cdc>

### Real-Time Eventing Model

The real-time eventing model uses an application user on Cisco IM and Presence Service to establish an administrative session, which allows for end users to log in with that session key. Once the end user has logged in, the user registers and subscribes for presence updates using Representational State Transfer (REST). [Figure 20-30](#) highlights the Third-Party Open API real-time eventing model interaction with Cisco IM and Presence Service.

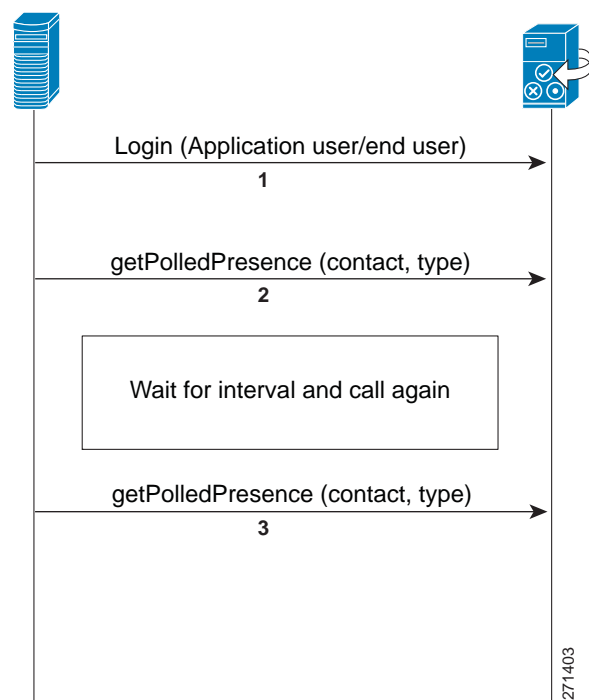
**Figure 20-30** Third-Party Open API Real-Time Eventing Model

The call flow in [Figure 20-30](#) illustrates the following sequence of events:

1. The application initiates a SOAP login request to Cisco IM and Presence Service via the super-user application user (APIUser), and Cisco IM and Presence Service returns a session key. The application can then log in the end-user with this session key (essentially, the end-user logs in via the application).
2. The end user registers the endpoint using the application-user session key.
3. The application initiates a subscribe request (using the session key) on behalf of the end user to retrieve user information, contact list, and presence rules.
4. Cisco IM and Presence Service sends a notification – unsecured.
5. The application requests the user's presence status.

#### Polling Model

The polling model uses an application user on Cisco IM and Presence Service to establish an administrative session, which allows for end users to log in with that session key. Once the end user has logged in, the application requests presence updates periodically, also using Representational State Transfer (REST). [Figure 20-31](#) highlights the Third-Party Open API polling model interaction with Cisco IM and Presence Service.

**Figure 20-31** Third-Party Open API Polling Model

The call flow in [Figure 20-31](#) illustrates the following sequence of events:

1. The application initiates a SOAP login request to Cisco IM and Presence Service via the super-user application user (APIUser), and Cisco IM and Presence Service returns a session key. The application can then log in the end-user with this session key (essentially, the end-user logs in via the application).
2. The application requests presence state and bypasses the eventing model.
3. The application requests presence state and bypasses the eventing model.



**Note** Both Basic presence and Rich presence can be retrieved; however, the polling model puts an additional load on the presence server.

### Extensible Messaging and Presence Protocol Interfaces

The XCP architecture allows for two additional open interfaces for presence, instant messaging, and roster management: a client XMPP interface and a Cisco AJAX XMPP Library interface. The client XMPP functionality enables third-party XMPP clients to integrate presence, instant messaging, and roster management, and it is a complementary interface to the SIP/SIMPLE interface on Cisco IM and Presence Service. The client XMPP interface is treated as a normal XMPP client within Cisco IM and Presence Service; therefore, sizing of the interface should be treated as a normal XMPP client.

The Cisco AJAX XMPP Library API provides a Web 2.0 style of interface to integrate XCP features into web applications and widgets, and it is made directly available from Cisco IM and Presence Service. The Cisco AJAX XMPP Library API is exclusively a client-side JavaScript library that communicates to the Bidirectional-streams Over Synchronous HTTP (BOSH) interface, which is essentially an XMPP over HTTP interface that allows the server to push data to a web browser through a long-polling technique.



Observe the following requirements when integrating either model of the Third-Party Open API with Cisco IM and Presence Service:

- Certificates are required for the presence interface (sipproxy.der) and the configuration interface (tomcat\_cert.der).
- No more than 1000 Third-Party Open API users can be integrated per Cisco IM and Presence Service deployment.
- To improve performance, balance the Third-Party Open API users across all servers in the Cisco IM and Presence Service cluster.

You can obtain additional information and support for use of the Cisco IM and Presence Service Third-Party Open API through Cisco Developer Services, available at:

<https://developer.cisco.com/web/cupapi>

Information and assistance for developers is also available from the Cisco Developer Community, which is accessible through valid Cisco login authentication at:

<https://developer.cisco.com/>

## Design Considerations for On-Premises Cisco IM and Presence Service

- If LDAP integration is possible, LDAP synchronization with Unified CM should be used to pull all user information (number, ID, and so forth) from a single source. However, if the deployment includes both an LDAP server and Unified CM that does not have LDAP synchronization enabled, then the administrator should ensure consistent configuration across Unified CM and LDAP when configuring user directory number associations.
- Cisco IM and Presence Service marks Layer 3 IP packets via Differentiated Services Code Point (DSCP). Cisco IM and Presence Service marks all IM and Presence traffic based on the Differential Service Value service parameter under SIP Proxy, which defaults to a value of DSCP 24 (PHB CS3).
- Presence Policy for Cisco IM and Presence Service is controlled strictly by a defined set of rules created by the user.
- Use the service parameter IMP PUBLISH Trunk to streamline SIP communication traffic with the Cisco IM and Presence Service.
- Associate presence users in Unified CM with a line appearance, rather than just a primary extension, to allow for increased granularity of device and user presence status. When using the service parameter IMP PUBLISH Trunk, you must associate presence users in Unified CM with a line appearance.
- A Presence User Profile (the user activity and contact list contacts and size) must be taken into consideration for determining the server hardware and cluster topology characteristics. The Cisco IM and Presence system architecture is based on an average contact list size of 75 contacts per user on a fully populated system. While per-user contact list size will vary across the system, if significant numbers of users on the system exceed the average list size of 75 contacts, system performance will be impacted. By default the maximum contact list size is 200. If some users will exceed 200 contacts, this maximum contact list size can be changed by modifying the Presence Settings of the IM and Presence cluster. For additional sizing information, see the sections on [Cisco IM and Presence, page 25-33](#), and [Roster Management, page 25-34](#).
- Use the User Assignment Mode for Presence Server enterprise parameter default of **balanced** for best overall cluster performance.

- Cisco IM and Presence Service requires an external database instance for each server in the cluster for persistent chat, and one database instance per cluster for message archiving. Third-party compliance supports mapping of all or a subset of servers in an IM and Presence Service cluster to one external compliance database. The three external database options are flexible deployments wherein there can be multiple compliance servers per IM and Presence server, multiple IM and Presence servers per compliance server, or a combination thereof.
- Compliance servers can be dedicated or shared with IM and Presence nodes in the same cluster. Cisco recommends deploying two compliance servers per sub-cluster pair, with both IM and Presence nodes defined in the compliance profile. One compliance server for the entire cluster is also supported but not recommended.
- You can install the database on either a Linux or a Windows operating system. Refer to the relevant database documentation for details on the supported operating systems and platform requirements:
  - PostgreSQL documentation available at <https://www.postgresql.org/docs/manuals/>
  - Oracle documentation available at <https://docs.oracle.com/en/database/database.html>
- Cisco IM and Presence Service supports a total of 75,000 users per cluster for full Unified Communications mode. The sizing for users must take into account the number of SIP/SIMPLE users and the number of XMPP users. XMPP users have slightly better performance because SIP/SIMPLE users employ the IM Gateway functionality into the XCP architecture.
- All eXtensible Communications Platform (XCP) communications and logging are stored in GMT and not localized to the installed location.
- For ease of user migration and contact list migration, Cisco IM and Presence Bulk Administration Tool supports bulk contact list importation using a comma-separated value (csv) file as input for this bulk importation.

For a complete listing of ports used by Cisco IM and Presence Service, refer to *Port Usage Information for Cisco IM and Presence*, available at

[https://www.cisco.com/en/US/products/ps6837/products\\_device\\_support\\_tables\\_list.html](https://www.cisco.com/en/US/products/ps6837/products_device_support_tables_list.html)

## Contact and Watcher List Recommendations



### Note

The guidelines provided in this section are based strictly on what has been validated by Cisco under specific test conditions. The recommendations are intended to help guide the deployment and distribution of presence users in an IM and Presence deployment with regard to managing contact lists and watcher lists in the cluster.

## IM and Presence Cluster

The IM and Presence standard deployment is designed to support 45,000 presence-enabled users in a fully loaded cluster across 3 IM and Presence sub-cluster pairs (6 nodes) and deployed using 15k-User IM and Presence VM templates.

The recommendation for contact lists and watcher lists is not to exceed a cluster average of 75 presence-enabled contacts per user in the cluster. This value is derived from validation tests of 100 total contacts per user on average, split with 75 presence-enabled users and 25 non-presence users in their respective buddy lists. The rest of this discussion focuses on the 75 presence-enabled users because that is the factor that impacts system performance and scalability the most.

To help manage the IM and Presence system performance and stability, it is crucial to properly maintain, manage, and monitor the IM and Presence roster tables, which basically consist of end-user contact lists and watcher lists for all presence users.


**Note**

The cluster average of 75 presence-enabled contacts per user is not the same as the service parameter(s) for **Maximum Contact List Size (per user)** and **Maximum Watchers (per user)**, where the default values are 150 and 200 respectively, depending on Cisco IM and Presence release version.

## Presence State Change Impact

To help understand how a state change impacts the system, consider the events from the perspective of a single user on a typical work day. Assume that user, named Bob, has 75 contacts in his buddy list and those 75 contacts also have Bob as a contact in their buddy lists (although that is not necessarily the case in most deployments).

When Bob first logs in to his desktop Jabber client, 75 notifications are generated and sent out to all the contacts in his buddy list. If Bob then uses his desk phone to make a call, another 75 notifications are sent to his contacts to update his status to "on the phone." Every status change for Bob initiates a notification per contact in his buddy list *if* Bob is also in that contact's buddy list.

All presence-enabled users initiate status change updates to all presence-enabled contacts in their buddy lists. Status changes include actions such as picking up the phone handset, making a call, hanging up, joining a meeting, and so on. So for every user with 75 presence-enabled contacts, every action generates 75 notifications at minimum.

For example, consider a deployment of 3,000 presence-enabled users, each of which has 75 contacts in their buddy list. If all 3,000 users join a conference or all-hands meeting at the same time, that would generate 225,000 presence update notifications. Similarly, in a deployment of 9,000 presence users, if all users perform actions that cause presence status changes at the same time, that would generate 675,000 presence update notifications. These notifications utilize system resources and impact system performance, especially during peak usage times. That is why it is crucial to distribute users evenly across the cluster and to avoid exceeding the recommended average of 75 contacts per user.

## Distribution of Presence Users

The budget, or maximum number of contact entries allowed, for the IM and Presence database can be calculated from the total number of configured presence users multiplied by the recommended average number of presence contacts (75) that each user can have in their buddy list. For example, the recommended budget (maximum number of IM and Presence contacts) for a fully loaded cluster of 45,000 users would be:

$$(45,000 \text{ users}) * (75 \text{ contacts per user}) = 3.375\text{M IM and Presence contacts for the cluster}$$

If there are 3 sub-cluster pairs (6 nodes) in the deployment with 15,000 users in each sub-cluster, then on average there would be:

$$15,000 \text{ users} * 75 \text{ contacts per user} = 1.125\text{M contacts per sub-cluster pair}$$

If each IM and Presence user has no more than 75 contacts in their buddy list, then the users can be distributed equally across the sub-clusters, as indicated in the above calculation. However, if some users require more than 75 contacts in their buddy lists, then a custom distribution is required, as described in the following section.


**Tip**

Make sure that the users with a high number of contacts (more than 75) do not all reside on the same IM and Presence node and, instead, are distributed evenly across the nodes.

### Custom Distribution

Again consider a fully loaded IM and Presence cluster with 45,000 users distributed across three sub-clusters. Assume, for example, that 1,000 users in the cluster need to have 500 presence-enabled contacts in their buddy lists. In this case those 1,000 users would require:

$$(1,000 \text{ users}) * (500 \text{ contacts per user}) = 500,000 \text{ IM and Presence database entries}$$

The maximum number of IM and Presence database entries allowed for the entire cluster is 3.375M. After accounting for the 1,000 users with 500 contacts each, the remaining available contact entries would be:

$$3,375,000 - 500,000 = 2,875,000 \text{ contact entries available for the remaining 44,000 presence users in the cluster.}$$

If the available contact entries are distributed evenly among the remaining 44,000 users in the cluster, that would provide:

$$2,875,000 / 44,000 = \text{maximum of 65 contacts per user}$$



#### Note

In the above example, the users with 500 contacts must be distributed evenly across the three sub-cluster pairs. It is also critical to ensure system stability by frequently monitoring and adjusting the distribution of IM and Presence users as their usage and resource requirements change. In addition, if the number of contacts required by any user in the cluster is higher than the default value of the service parameter **Maximum Contact List Size (per user)**, then that parameter setting and the setting for **Maximum Watchers (per user)** must both be changed to the higher value.

### Status Change Notify Impact

From the example above, the custom distribution with 500 contacts per user would generate 500 notifications for every status change compared to 75 notifications per status change with the evenly distributed option. The following examples illustrate the impact comparison between 1000 users with 75 contacts and 500 contacts:

- $1000 * 75 = (75,000 \text{ notifications}) / (3,600 \text{ seconds, or 1 hour}) = 21 \text{ notifications/sec per cluster, or 7 notifications/sec per sub-cluster pair.}$
- $1000 * 500 = (500,000 \text{ notifications}) / (3,600 \text{ seconds, or 1 hour}) = 139 \text{ notifications/sec per cluster, or 47 notifications/sec per sub-cluster pair.}$

## Mobile and Remote Access

Users can access their collaboration tools from outside the corporate firewall without a VPN client. Using Cisco collaboration gateways, the client can connect securely to your corporate network from remote locations such as public Wi-Fi networks or mobile data networks.

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 (Unified CM) when the endpoint is not within the enterprise network. Cisco Expressway provides secure firewall traversal and line-side support for Unified CM registrations.

Note that third-party SIP or H.323 devices can register to a Cisco VCS connected via a neighbor zone to a Cisco Expressway and, if necessary, interoperate with Unified CM registered devices over a SIP trunk.

For information on how to set up the Cisco Expressway servers, refer to the latest version of the *Cisco Expressway Basic Configuration Deployment Guide* and the *Mobile and Remote Access via Cisco Expressway Deployment Guide*, both available at

<https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html>

When using mobile and remote access, the following Jabber features are not supported:

- Directory access mechanisms other than UDS
- Certificate provisioning to remote endpoints
- File transfer
- Deskphone control mode.

## Third-Party Presence Server Integration

Cisco IM and Presence Service provides an interface based on SIP and SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE) for integrating SIP and SIMPLE applications into the Cisco Unified Communications solution. You can configure and integrate a third-party presence server or application with this SIP/SIMPLE interface to provide presence aggregation and federation.

## Microsoft Communications Server for Remote Call Control (RCC)

For all setup, configuration, and deployment of Microsoft products, refer to the documentation at:

<https://www.microsoft.com/>

Cisco does not provide configuration, deployment, or best practice procedures for Microsoft Communications products, but Cisco does provide the guidelines listed below for integrating Cisco IM and Presence Service with Microsoft Lync.

Cisco Systems has developed documentation to describe feature interoperability and configuration steps for integrating Cisco IM and Presence Service with Microsoft Lync. You can access this documentation at:

[https://www.cisco.com/en/US/products/ps6837/products\\_installation\\_and\\_configuration\\_guides\\_list.html](https://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html)

### Guidelines for Integrating Cisco IM and Presence Service with Microsoft Lync

The following guidelines apply when integrating the Cisco IM and Presence Service and Microsoft Lync:

- Communications between Cisco IM and Presence Service and Microsoft Lync uses the SIP/SIMPLE interface. However, Microsoft Lync tunnels Computer-Supported Telecommunications Applications (CSTA) traffic over SIP. Therefore, the CTI gateway on the Cisco IM and Presence Service must be configured to handle the CSTA-to-CTI conversion for Click to Call phone control.
- Cisco IM and Presence Service deployment with Microsoft Lync for Remote Call Control, should consist of a single subcluster pair of servers that make up the Cisco IM and Presence Service cluster.
- The following table lists the number of users supported per platform. The user count is based solely on the Unified CM platform equivalent, regardless of the IM and Presence Service platform.

Cisco Unified Communications Manager VM Configuration Template	Number of Microsoft Office Communicator or Lync Users Supported per Server	Number of Microsoft Office Communicator or Lync Users Supported per Cluster
1,000 User	1,000	4,000
2,500 User	2,500	10,000
7,500 User	7,500	30,000
10,000 User	10,000	40,000

- You must configure the same end-user ID in LDAP, Unified CM, and Microsoft Lync. This practice avoids any conflicts between Microsoft Lync authentication with Active Directory (AD) and the end-user configuration on Unified CM, as well as conflicts with user phone control on Unified CM. For Active Directory, Cisco recommends that the user properties of General, Account, and Communications all have the same ID. To ensure the Cisco IM and Presence Service users are consistent, LDAP Synchronization and Authentication should be enabled with Unified CM.
- You must configure Microsoft Lync Host Authentication to contain the Cisco IM and Presence Service publisher and subscriber.
- You can configure routing of the SIP messages to Cisco IM and Presence Service by means of Static Routes in the Microsoft Lync properties.
- You must configure an incoming and outgoing access control list (ACL) on the Cisco IM and Presence Service to allow for communications with Microsoft Lync.
- You must enable each user for use of Microsoft Lync in the Cisco IM and Presence Service configuration, in addition to enabling each user for presence in Unified CM.
- Take into account bandwidth considerations for Microsoft Lync login due to the exchange of configuration information between Microsoft Lync and the Microsoft Communications Server, and due to initial communication with the Cisco IM and Presence Service CTI gateway.
- To address the issue of a reverse look-up of a directory number that corresponds to a user, use the guidelines documented in the *Release Notes for Cisco IM and Presence*, available at

[https://www.cisco.com/en/US/products/ps6837/prod\\_release\\_notes\\_list.html](https://www.cisco.com/en/US/products/ps6837/prod_release_notes_list.html)

# In-the-Cloud Service and Architecture

This section describes the in-the-cloud service and architecture for Cisco IM and Presence Service. This hosted service provides the same user experience as the on-premises solution.

## Cisco WebEx Messenger

Cisco WebEx Messenger is a multi-tenant software-as-a-service (SaaS) platform for synchronous and asynchronous collaboration. The WebEx Messenger platform is hosted inside the Cisco WebEx Collaboration Cloud and it enables collaborative applications and integrations, which allows for organizations and end users to customize their work environments. For additional information on the Cisco WebEx Messenger service, refer to the documentation available at

<https://developer.cisco.com/web/webex-developer>

For more information on the Cisco Collaboration Cloud, refer to the documentation available at

[https://www.cisco.com/en/US/solutions/ns1007/collaboration\\_cloud.html](https://www.cisco.com/en/US/solutions/ns1007/collaboration_cloud.html)

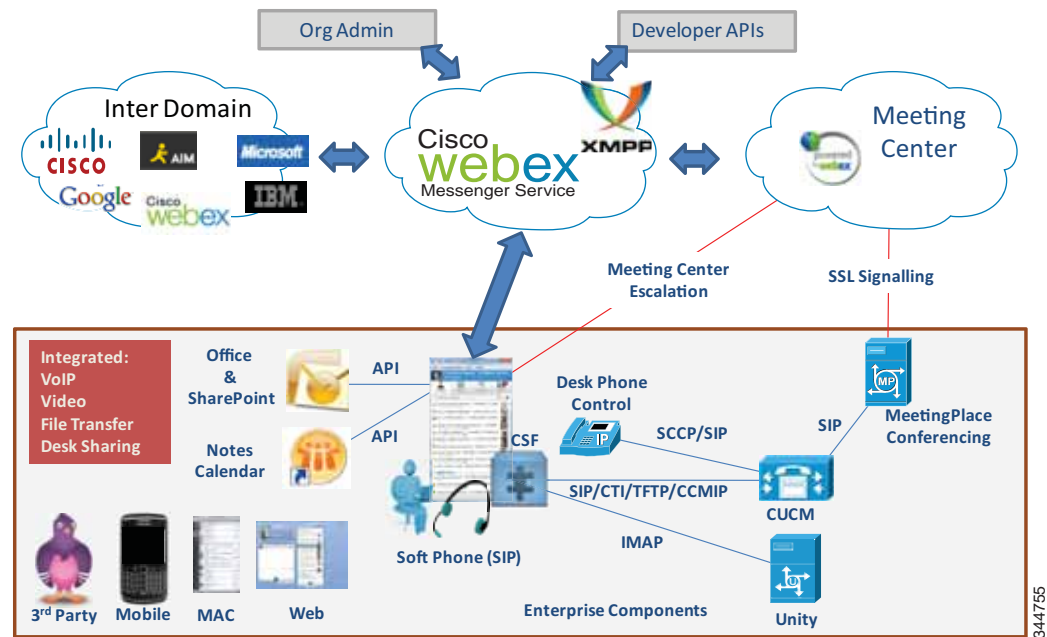
## Deploying Cisco WebEx Messenger Service

A Cisco WebEx Messenger solution deployment consists of the following components, as depicted in [Figure 20-32](#):

- A secure connection (SSL and AES) to the Cisco WebEx Messenger XMPP cloud platform for presence, instant messaging, VoIP, PC-to-PC video, media transfer (screen capture and file transfer), and desktop sharing
- Cisco WebEx Meetings
- XMPP federation with other WebEx Messenger organizations and third-party XMPP clients and XMPP instant messaging (IM) networks
- Cisco Unified Communications integration for call control, voice messaging, and call history
- Microsoft Outlook and IBM Lotus Notes calendar integration
- Integration to Microsoft Outlook for presence and click-to-communicate functionality



Figure 20-32 Deploying Cisco WebEx Messenger Service



344755

## Centralized Management

Cisco WebEx Messenger service provides a web-based administrative tool to manage the solution across the organization. Cisco WebEx Messenger service users are configured and managed through the Cisco WebEx Administration Tool, which enables administrators to set up basic security and policy controls for features and services. These policies can be applied enterprise-wide, by group, or individually. There are various methods to provision the user database that are further described in the Cisco WebEx administrator's guide available at

<https://www.webex.com/webexconnect/orgadmin/help/index.htm>

## Single Sign On

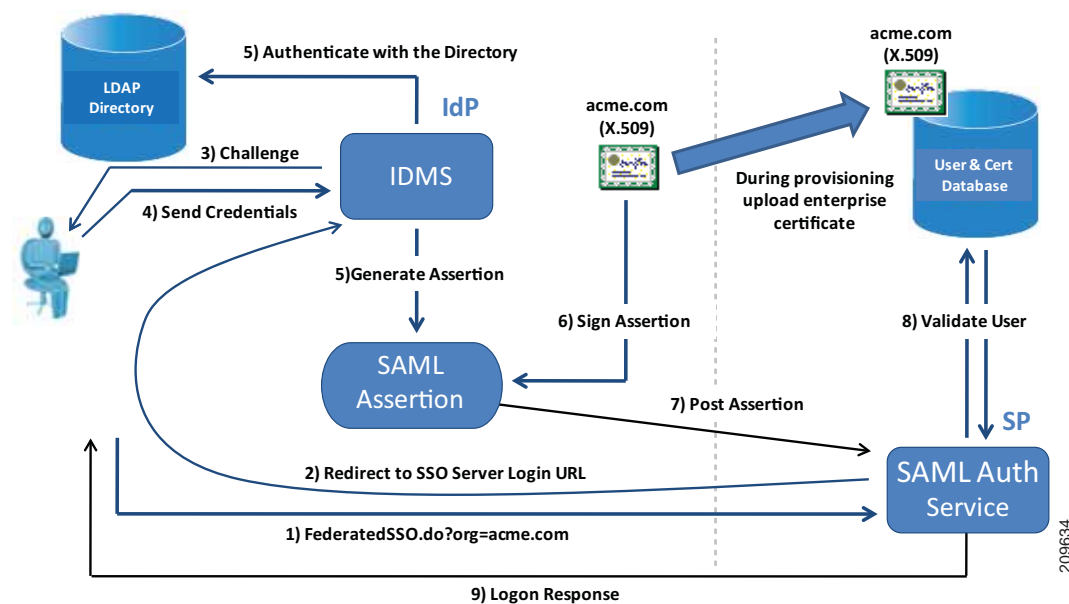
Single Sign On (SSO) enables companies to use their on-premises SSO system, including Security Assertion Markup Language (SAML) support, to simplify the management of Cisco WebEx Messenger or IM and Presence Service by allowing users to securely log into any of the Unified Communications applications in the solution using their corporate login credentials. The user's login credentials are not sent to Cisco, thus protecting the user's corporate login information. Figure 20-33 shows the credential handshake that occurs on user login to Cisco WebEx Messenger as well as Unified CM.



### Note

If Cisco Jabber is deployed with Cisco WebEx Meeting Server, Cisco Unified CM and WebEx Meeting Server must be in the same domain.

**Figure 20-33** User Login Authentication Process for Cisco WebEx Messenger Service



A user account can be configured to be created automatically the first time a user logs into Cisco IM client. Users are prevented from accessing the Cisco WebEx Messenger service if their corporate login account is deactivated.

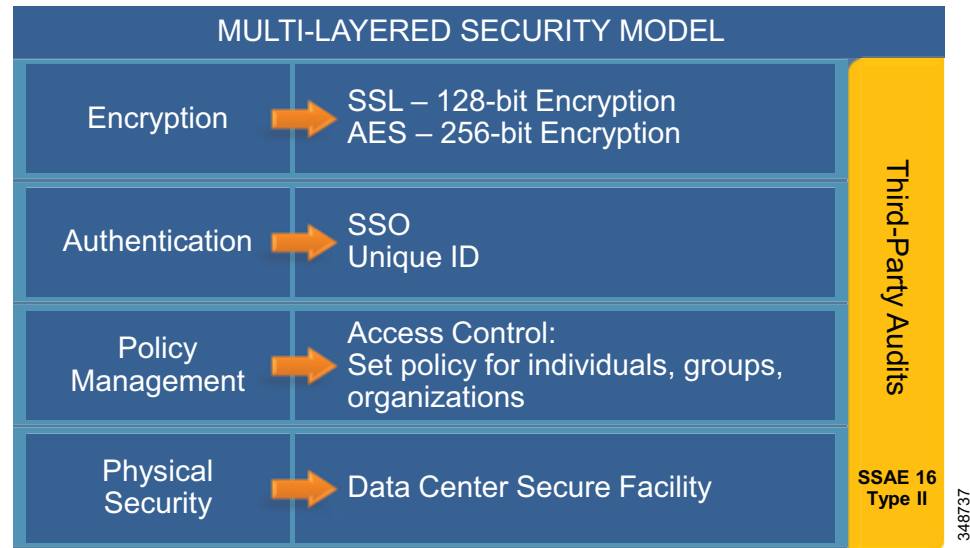
For more information on Single Sign On with WebEx Messenger service, refer to the documentation available at

<https://developer.cisco.com/web/webex-developer/sso-reference>

## Security

The Cisco WebEx security model consists of functional layers of security. Figure 20-34 illustrates the separate but interrelated elements that compose each layer.

**Figure 20-34 WebEx Security Model**



The bottom layer represents the physical security in the Cisco WebEx data centers. All employees go through an extensive background check and must provide dual-factor authentication to enter the datacenter.

The next level is policy management, where the WebEx Messenger organization administrator can set and manage access control levels by setting different policies for individual users, groups, or the entire Cisco WebEx Messenger organization. White-list policies, specific to external users or domains, can be created to allow instant messaging exchanges. The Cisco WebEx Messenger organizational model also allows for the creation of specific roles and groups across the entire user base, which allows the administrator to assign certain privileges to roles or groups as well as to set policies, including access control, for the entire organization.

Access to the Cisco WebEx Messenger service is controlled at the authentication layer. Every user has a unique login and password. Passwords are never stored or sent over email in clear text. Passwords can be changed only by the end-users themselves. The administrator can choose to reset a password, forcing the end-user to change his or her password upon the next login. Alternatively, an administrator may choose to use the Single Sign On (SSO) integration between Cisco WebEx Messenger service and the company's directory to simplify end-user access management. The Single Sign On integration is achieved through the use of an Identity Management System (IDMS).

The encryption layer ensures that all instant messaging communications between Cisco WebEx Messenger users is encrypted. All instant messaging communication between Cisco WebEx Messenger users and the server in the Messenger Collaboration cloud is encrypted by default using SSL encryption. An additional level of security is available whereby IM communication can be encrypted end-to-end using 256-bit AES level encryption.

The Cisco WebEx Messenger platform uses third-party audits such as the SSAE 16 Type II audit to provide customers with an independent semi-annual security report. This report can be reviewed by any customer upon request with the Cisco Security organization. For additional Cisco WebEx Messenger service security, refer to the *Cisco WebEx Connect Security White Paper*, available at

[https://www.cisco.com/en/US/products/ps10528/prod\\_white\\_papers\\_list.html](https://www.cisco.com/en/US/products/ps10528/prod_white_papers_list.html)

## Firewall Domain White List

Access control lists should be set specifically to allow all communications from the webex.com and webexconnect.com domains and all sub-domains for both webex.com and webexconnect.com. The WebEx Messenger platform sends email to end-users for username and password communications. These email messages come from the mda.webex.com domain.

## Logging Instant Messages

Cisco WebEx Messenger service instant messaging communications are logged on the local hard drive of the personal computer where the user is logged in. Instant message logging is a capability in Cisco WebEx Messenger service that can be enabled by means of policy through the Org Admin tool.

The end-user can set logging specifics, whether to enable or disable logging, and how long the logs are kept. These message history settings are located under General in the IM client preferences.

Customers looking for advanced auditing and e-discovery capabilities should consider third-party solutions. Currently Cisco does not provide support for advanced auditing of instant messaging communications. Cisco WebEx Messenger service, however, does allow for logging and archiving of instant messages exchanged between users. Archiving of the logs is possible through the use of third-party SaaS archiving services, or the logs can be delivered securely to an on-premises SMTP server.

For additional information on instant message archiving, refer to the Cisco WebEx administrator's guide available at

<https://www.webex.com/webexconnect/orgadmin/help/index.htm>

## Capacity Planning for Cisco WebEx Messenger Service

A single end-user requires only a 56 kbps dial-up Internet connection to be able to log in to WebEx Messenger service and get the basic capabilities such as presence, instant messaging, and VoIP calling. However, for a small office or branch office, a broadband connection with a minimum of 512 kbps is required in order to use the advanced features such as file transfer, screen capture, and PC-to-PC video calling. For higher quality video such as High Definition 720p, the minimum bandwidth connection recommendation is 2 Mbps.

For additional information on network and desktop requirements, refer to the Cisco WebEx administrator's guide available at

<https://www.webex.com/webexconnect/orgadmin/help/index.htm>

Cisco WebEx Messenger deployment network requirements are available at

<https://www.webex.com/webexconnect/orgadmin/help/17161.htm>

## High Availability for Cisco WebEx Messenger Service

WebEx Messenger is a Software-as-a-Service (SaaS) application. The end-user device must be connected to the Internet for the end user to log in to the IM client. A standard Internet connection is all that is required. If an end user is remote, it is not necessary for that user to be connected through the company VPN in order to log in to the WebEx Messenger service. Cisco WebEx Messenger service IM clients can be deployed in a highly available redundant topology. Deployment of the Cisco WebEx Messenger Software-as-a-Service architecture consists of various network and desktop requirements described in this section.

### High Availability

With the use of the multi-tenant Software-as-a-Service architecture, if any individual server in a group fails for any reason, requests can be rerouted to another available server in the Cisco WebEx Messenger Platform.

The Cisco WebEx Network Operations Team provides 24x7 active monitoring of the Cisco WebEx Collaboration Cloud from the Cisco WebEx Network Operations Center (NOC). For a comprehensive overview of the Cisco WebEx technology, refer to the information at

[https://www.cisco.com/en/US/solutions/ns1007/collaboration\\_cloud.html](https://www.cisco.com/en/US/solutions/ns1007/collaboration_cloud.html)

### Redundancy, Failover, and Disaster Recovery

The Cisco WebEx Global Site Backup architecture handles power outages, natural disaster outages, service capacity overload, network capacity overload, and other types of service interruptions. Global Site Backup supports both manual and automatic failover. The manual failover mode is typically used during maintenance windows. The automatic failover mode is used in case of real-time failover due to a service interruption.

Global Site Backup is automatic and transparent to the end users, it is available for all users, and it imposes no limits on the number of users that can fail-over.

Global Site Backup consists of the following main components:

- Global Site Service — Is responsible for monitoring and switching traffic at the network level.
- Database Replication — Ensures that the data transactions occurring on the primary site are transferred to the backup site.
- File Replication — Ensures that any file changes are maintained in synchronization between the primary and the backup site.

## Design Considerations for Cisco WebEx Messenger Service

Cisco WebEx Messenger is deployed as a Software-as-a-Service model, therefore design and deployment considerations are minimal. The Cisco WebEx Messenger solution has client options available for the Windows and Mac desktop as well as the popular mobile devices.

### Third-Party XMPP Clients Connecting to Cisco WebEx Messenger Service

Although Cisco does not officially support any other XMPP clients to connect to the Cisco WebEx Messenger Service, the nature of the XMPP protocol is to allow end users to connect to presence clouds with various XMPP clients using their WebEx Messenger service credentials. A list of XMPP software clients is available at

<https://xmpp.org/software/clients.shtml>

Organization policies cannot be enforced on third-party XMPP clients, and features such as end-to-end encryption, desktop share, video calls, PC-to-PC calls, and teleconferences are not supported with third-party clients. To allow non-WebEx Messenger service XMPP IM clients to authenticate to your WebEx Messenger service domain(s), DNS SRV records must be updated. The specific DNS SRV entry can be found in Cisco WebEx administration, under Configuration and IM Federation.

The use of non-Messenger service XMPP clients in Cisco WebEx administration, under Configuration and XMPP IM Clients, must be explicitly allowed.

For additional information on enabling third-party XMPP clients to connect to the WebEx Messenger platform, refer to the Cisco WebEx administrator's guide available at

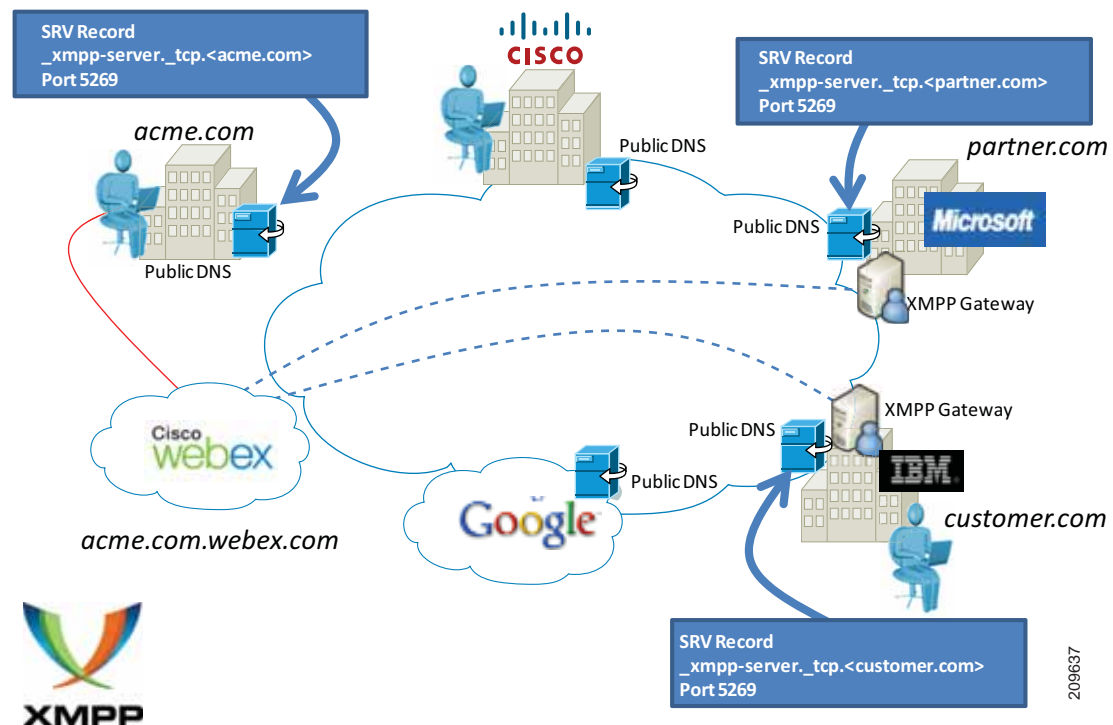
<https://www.webex.com/webexconnect/orgadmin/help/index.htm>

## Instant Messaging and Presence Federation Using Third-Party XMPP Clients

The Cisco WebEx Messenger service network can federate with XMPP-based instant messaging networks such as GoogleTalk and Jabber.org. (See Figure 20-35.) A list of public instant messaging networks based on XMPP is available at

<https://xmpp.org/>

**Figure 20-35 Inter-Domain Federation**



Currently the WebEx Messenger service does not interoperate with Yahoo! Messenger and Windows Live Messenger, but it can federate with AIM through a federation gateway.

## Other Resources and Documentation

The Cisco WebEx administrator's guide is available at

<https://www.webex.com/webexconnect/orgadmin/help/index.htm>

