



# Cisco IM and Presence

---

**Revised: November 19, 2013; OL-30952-01**

On-premises Cisco IM and Presence 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, 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 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).

---

This chapter explains the basic concepts of presence and instant messaging within the Cisco Unified Communications System and provides guidelines for how best to deploy the various components of the presence and instant messaging solution. This chapter covers the following topics:

- [Presence, page 20-2](#)
- [Phone-Specific Presence and Busy Lamp Field, page 20-4](#)
- [User Presence: Cisco IM and Presence Architecture, page 20-9](#)
- [On-Premises Cisco IM and Presence Enterprise Instant Messaging, page 20-27](#)
- [Third-Party Presence Server Integration, page 20-39](#)

# 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
Cisco IM and Presence 10.x supports deployments using only Open Virtualization Archive (OVA) templates on Cisco Unified Computing System (UCS) virtualized servers. Cisco IM and Presence 10.x cannot be deployed on Cisco MCS physical servers.	Various sections throughout this chapter	November 19, 2013

## 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.

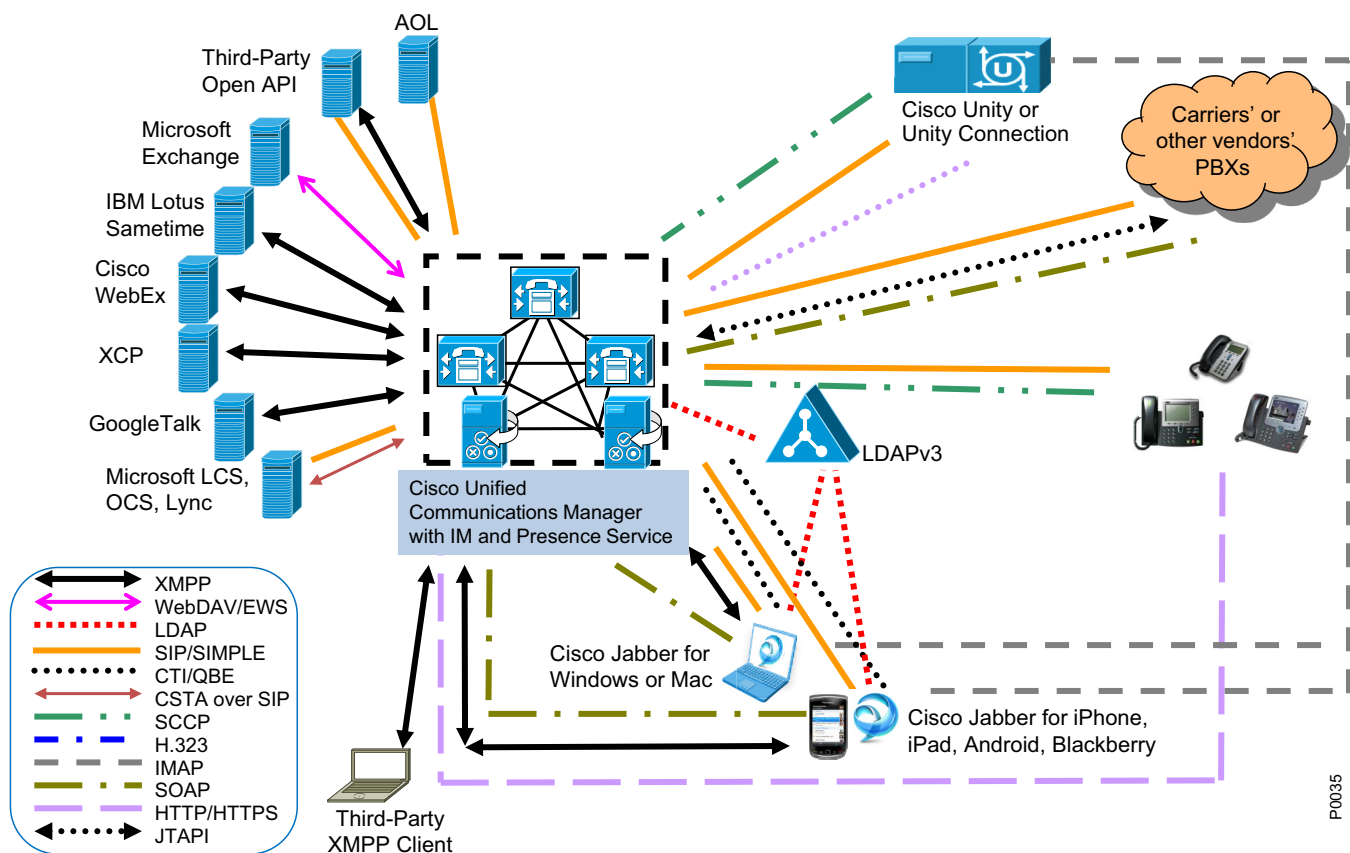
Terminology surrounding presence refers to a watcher, presence entity (*presentity*), and presence server. The presence entity publishes its current status to the presence server by using a PUBLISH or REGISTER message for SIP/SIMPLE clients, or by using an XML Presence Stanza for XMPP clients. It can 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 Components

Cisco IM and Presence encompasses the following components, illustrated in Figure 20-1:

- Cisco IM and Presence Service
- Cisco Unified Communications Manager (Unified CM)
- Cisco Jabber
- Cisco Unity Connection
- Cisco Unified MeetingPlace Express VT
- Lightweight Directory Access Protocol (LDAP) Server v3.0
- Cisco Unified IP Phones
- Third-party presence server
- Third-party XMPP clients
- Third-party applications

**Figure 20-1** Cisco IM and Presence Interfaces



## On-Premises Cisco IM and Presence 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).

A user can also have only IM and Presence capabilities. This deployment requires a Unified CM publisher for configuration, along with an IM and Presence cluster as well as Jabber clients. In this arrangement, telephony voice features would be provided through another vendor's system or PBX.

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 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, employeenumber, telephonenumber, or UserPrincipalName) and *default\_domain* is the domain configured in the IM and Presence administration.

The Jabber Identifier (JID) can be the default *user@default\_domain* or the JID can be based on the DirectoryURI. The DirectoryURI is configured in the Unified CM LDAP Directory administration configuration, and it allows for the IM and Presence address (JID) to be based on an email ID or msRTCSIP-PrimaryUserAddress. 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.

**Note**

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

## 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 20-7), 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.

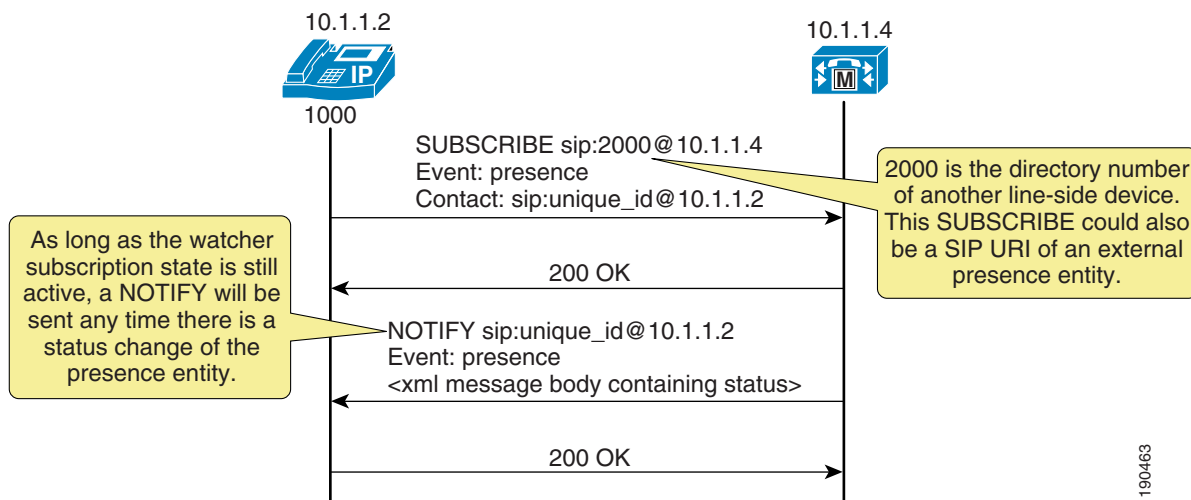
A watcher that is not in a Unified CM cluster can send a presence request to a SIP trunk. If Unified CM supports the presence entity, it will respond with the current presence status. If Unified CM does not support the presence entity, it will reject the presence request with a SIP error response.

## Unified CM Presence with SIP

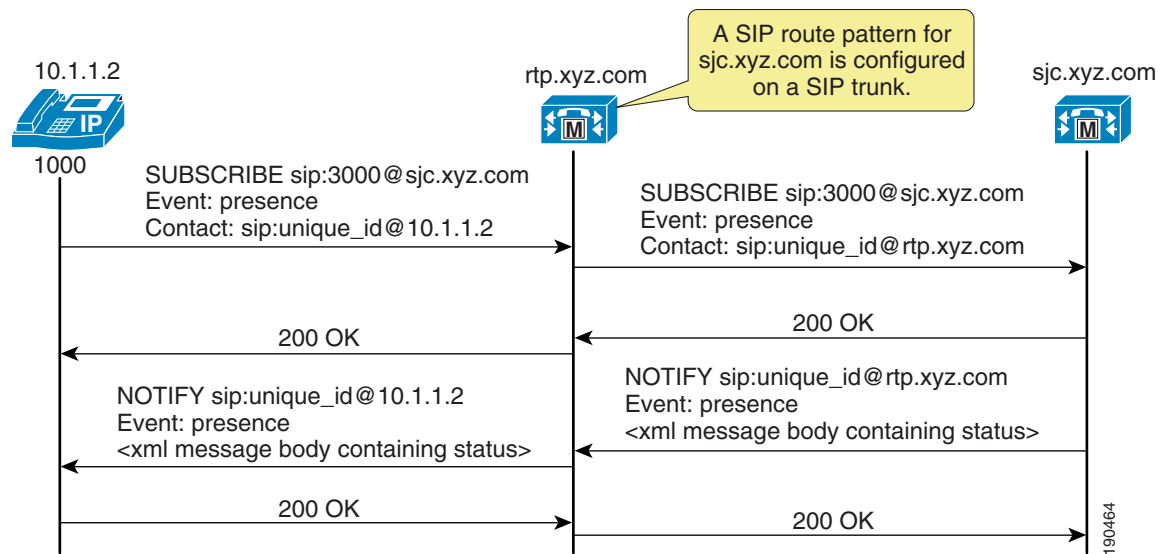
Unified CM uses the term *SIP line* to represent endpoints supporting SIP that are directly connected and registered to Unified CM and the term *SIP trunk* to represent trunks supporting SIP. SIP line-side endpoints acting as presence watchers can send a SIP SUBSCRIBE message to Unified CM requesting 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 20-2](#).)

**Figure 20-2** 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 20-3](#).)

**Figure 20-3 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 Presence with SCCP

Unified CM supports Skinny Client Control Protocol (SCCP) line-side endpoints acting as presence watchers. There are no SCCP trunks. SCCP endpoints can request presence status of the indicated presence entity by sending SCCP messages to Unified CM.

If the presence entity resides within the Unified CM cluster, Unified CM responds to the SCCP line-side presence request by sending SCCP messages to the presence watcher, indicating the current status of the presence entity.

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 SCCP line-side presence request by sending SCCP messages to the presence watcher, indicating the current status of the presence entity.

## 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.

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

Figure 20-4 lists the various types of BLF speed dial indications from the phones.

**Figure 20-4** 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 <http://www.cisco.com/>.

The presence indicators for call history lists are the same as those listed in the Icon column in Figure 20-4; 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 database for the duration of the ad-hoc chat. This allows a room owner to escalate an ad-hoc chat to a persistent chat; otherwise, these ad-hoc chats are purged from PostgreSQL at the end of the 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.

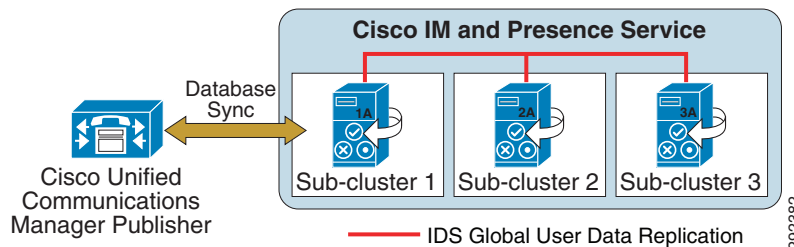
## On-Premises Cisco IM and Presence Cluster

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

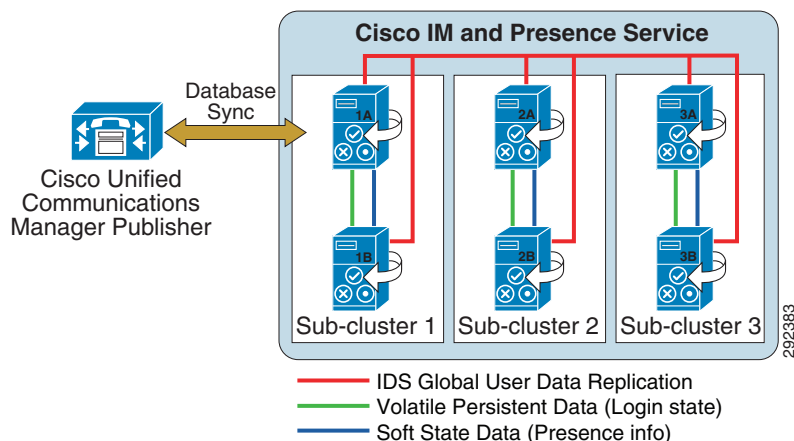
[http://www.cisco.com/en/US/products/sw/voicesw/ps556/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html)

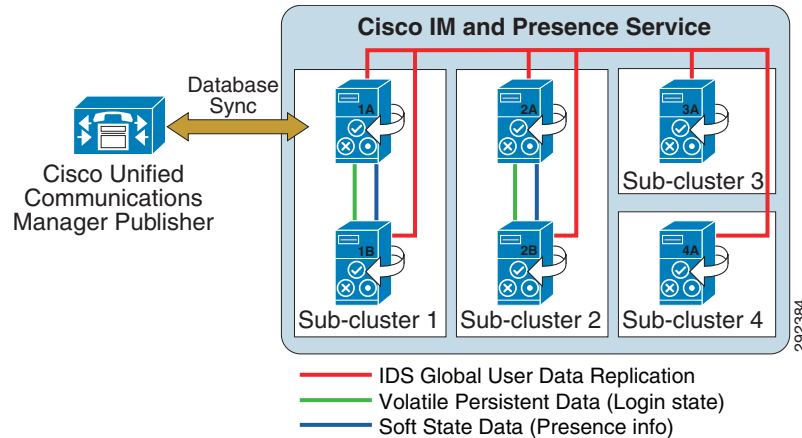
A Cisco IM and Presence cluster consists of up to six servers, including one designated as a publisher, which utilize the same architectural concepts as the Unified CM publisher and subscriber. Within a Cisco IM and Presence cluster, individual servers can be grouped to form a subcluster, and the subcluster can have at most two servers associated with it. [Figure 20-5](#) shows the basic topology for a Cisco IM and Presence cluster, while [Figure 20-6](#) shows a highly available topology. The Cisco IM and Presence 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 20-7](#).

**Figure 20-5 Basic Deployment of On-Premises Cisco IM and Presence**



**Figure 20-6 High Availability Deployment of On-Premises Cisco IM and Presence**



**Figure 20-7 Mixed Deployment of On-Premises Cisco IM and Presence**

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.

**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 Cisco IM and Presence and Unified CM and between the Cisco IM and Presence 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 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 publisher performs an initial synchronization of the entire Unified CM user and device database. All Cisco IM and Presence users are configured in the Unified CM End User configuration. During the synchronization, Cisco IM and Presence 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 through the Cisco Unified Communications Manager administrator interface before they can be managed by Cisco IM and Presence.

The initial Cisco IM and Presence 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 are performed in real time when any new user or device information is added to Unified CM. For planning purposes, use the values in [Table 20-2](#) as guidelines when executing the initial database synchronization of Unified CM with Cisco IM and Presence.

**Note**

Cisco IM and Presence 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 cluster is 45,000 in full Unified Communications mode and 75,000 in IM-only mode.

**Table 20-2**      *Approximate Synchronization Times for Cisco IM and Presence*

Server Platform (OVA Template)	Number of Users	Approximate Synchronization Time
OVA 500 Users (Full UC)	500	5 minutes
OVA 1000 Users (Full UC)	1,000	5 minutes
OVA 2000 Users (Full UC)	2,000	5 minutes
OVA 5000 Users (Full UC)	5,000	10 minutes
OVA 15,000 Users (Full UC)	15,000	15 minutes

**Note**

When the on-premises 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.

If the database entries are not updating or if the Sync Agent service is stopped, you can check for broken connections with the synchronization agent by using the Real-Time Monitoring Tool (RTMT) to monitor the Critical Alarm **Cisco Unified Presence ServerSyncAgentAXLConnectionFailed**.

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

The Cisco IM and Presence cluster consists of up to six servers, which can be configured into multiple subclusters, with a 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 does not provide failover between subclusters.

When deploying a Cisco IM and Presence 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.

## On-Premises Cisco IM and Presence 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

Cisco IM and Presence is supported with all the Unified CM deployment models. However, Cisco recommends locating the Cisco IM and Presence 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 cluster, with the exception of geographic datacenter redundancy and clustering over the WAN (for details, see [Clustering Over the WAN, page 20-20](#)).

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

Cisco IM and Presence 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

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

A highly available Cisco IM and Presence 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 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 20-6](#) 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**) 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 20-6](#) 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 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 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 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 features enabled, the average user contact list size, and the traffic being generated by the users.

## On-Premises Cisco IM and Presence Deployment Examples

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

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 C210 M2 TRC #1, #2, or #3 with one OVA 15,000 Users 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*

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:

- Two Cisco UCS C240 M3 TRC #1, each with two OVA 15,000 Users Full UC templates

Deployment:

- Two Cisco IM and Presence 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*

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 with two OVA 5000 Users Full UC templates

Deployment:

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

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

Deployment requirements:

- 100 users that could scale up to 500 users
- Single Cisco Business Edition
- Instant message archiving and persistent chat are required
- High availability is required

Hardware:

- Cisco Business Edition 6000 using the OVA 1000 Users Full UC template

Deployment:

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

**Example 20-5 Multiple Unified CM Clusters with Cisco IM and Presence**

Deployment requirements:

- 5,000 users that could scale up to 60,000 users
- Multiple Cisco Unified Communications Manager clusters
- Instant message compliance is required
- High availability is required

Hardware and software platform:

- Cisco UCS B200 M3 TRC #1 or #2 with OVA 15,000 Users Full UC template and Cisco Unified CM

Deployment:

- Start with a single UCS B200 M3 TRC #1 or #2 with Unified CM and Cisco IM and Presence. Add another UCS B200 as soon as the number of users increases above 15,000, and split Unified CM and Cisco IM and Presence between the two hardware platforms. With a large number of users within a single Cisco IM and Presence cluster, set the User Assignment Mode for Presence Server enterprise parameter to **balanced**. Set up a third-party compliance server for instant messaging compliance for each server in each Cisco IM and Presence cluster.

**Example 20-6 Multiple Unified CM Clusters with Cisco IM and Presence 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 B440 M2 TRC #1 with ten OVA 15,000 Users Full UC template

Deployment

- Five Cisco IM and Presence clusters in a single platform UCS B440, each one serving one of the five Unified CM clusters with 15,000 users each.

## On-Premises Cisco IM and Presence Deployment for Instant Messaging Only

A Cisco IM and Presence cluster (or clusters) can be deployed to provide enterprise-class presence and instant messaging in an environment where Unified CM is not deployed for call control for specific users. Unified CM is still required to establish user accounts entered either manually or through LDAP synchronization. A Cisco IM and Presence instant messaging only deployment synchronizes user information from Unified CM in the same way as is done with a full Unified Communications deployment. If Unified CM is not deployed or if the existing deployed Unified CM will not be used for instant messaging only, a single Unified CM virtualized instance will have to be set up to provide for user configuration.

For existing Cisco IM and Presence deployments where a Unified CM cluster is already deployed, users can also be added for use with the instant messaging only mode. This allows for a mix of full Unified Communications users in addition to instant messaging only users, in accordance with the end-user license agreement.

## 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 cluster is based on the platform being used in the deployment. For example, if a Cisco IM and Presence cluster is deployed with three 2,000 Users OVA templates, each forming their own subcluster, then a total of 6,000 users would be supported. For a Cisco IM and Presence cluster, the maximum number of full UC users supported is 45,000 and 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

[http://docwiki.cisco.com/wiki/Virtualization\\_for\\_Unified\\_CM\\_IM\\_and\\_Presence](http://docwiki.cisco.com/wiki/Virtualization_for_Unified_CM_IM_and_Presence)

Cisco IM and Presence 10.x supports deployments using only OVA templates on virtualized servers; physical server support is not available in Cisco IM and Presence 10.x releases. Cisco strongly recommends using the same OVA template for all virtualized servers within an IM and Presence cluster. However, different OVA templates with equal or greater performance characteristics than the publisher may also be used.

## On-Premises Cisco IM and Presence Deployment

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

- [Single-Cluster Deployment, page 20-17](#)
- [Intercluster Deployment, page 20-19](#)
- [Clustering Over the WAN, page 20-20](#)
- [Federated Deployment, page 20-21](#)
- [Instant Messaging Only Deployment, page 20-25](#)

## Single-Cluster Deployment

Figure 20-8 represents the communication protocols between Cisco IM and Presence, the LDAP server, and Cisco Unified Communications Manager for basic functionality. For complete information on Cisco IM and Presence administration and configuration, refer to the Cisco IM and Presence installation, administration, and configuration guides, available at

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

**Figure 20-8 Interactions Between Cisco IM and Presence Components**

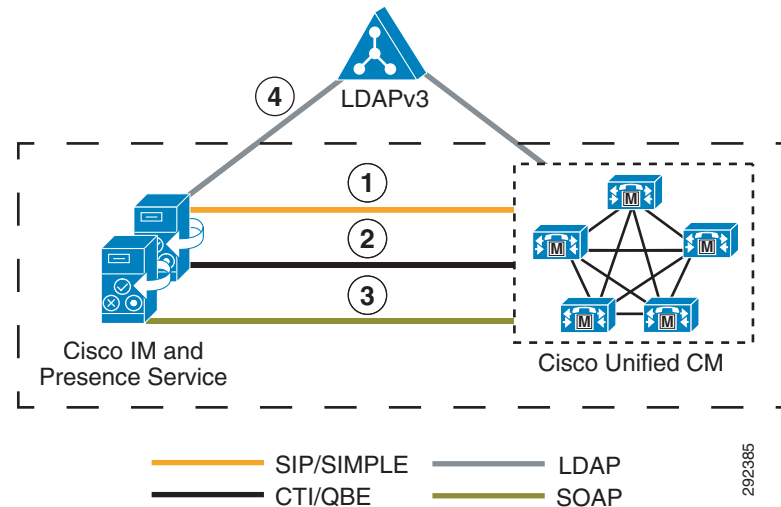


Figure 20-8 depicts the following interactions between Cisco IM and Presence components:

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 Services 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 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 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. 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 and Unified CM is the protocol used by presence-enabled users in Cisco IM and Presence 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 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 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 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 database.
  - a. No additional configuration is required on Unified CM.
  - b. Cisco IM and Presence 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 cluster. The administrator can also manually assign users to a particular server in the Cisco IM and Presence 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 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 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 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 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 cluster requires a separate peer relationship for each of the other Cisco IM and Presence clusters within the same domain. The address configured in this intercluster peer could be a DNS SRV FQDN that resolves to the remote Cisco IM and Presence cluster servers, or it could also simply be the IP address of the Cisco IM and Presence cluster servers.

The interface between each Cisco IM and Presence 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 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 cluster within the same domain.

When Cisco IM and Presence is deployed in an intercluster environment, a presence user profile should be determined. The presence user profile helps determine the scale and performance of an inter-cluster presence deployment and the number of users that can be supported. The presence user profile helps establish the number of contacts (or buddies) a typical user has, as well as whether those contacts are mostly local cluster users or users of remote clusters.

The traffic generated between Cisco IM and Presence clusters is directly proportional to the characteristics of the presence user profile. For example, assume presence user profile A has 30 contacts with 20% of the users on a local Cisco IM and Presence cluster and 80% of the users on a remote Cisco IM and Presence cluster, while presence user profile B has 30 contacts with 50% of the users on a local Cisco IM and Presence cluster and 50% of the users on a remote Cisco IM and Presence cluster. In this case, presence user profile B will provide for slightly better network performance and less bandwidth utilization due to a smaller amount of remote cluster traffic.

## Clustering Over the WAN

A Cisco IM and Presence 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 deployment with clustering over the WAN.

- Geographic datacenter redundancy and remote failover

A Cisco IM and Presence 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.

- High availability and scale

Cisco IM and Presence 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 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 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.

- Local Failover

A Cisco IM and Presence 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 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 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

When Cisco IM and Presence is enabled for persistent chat, message archiving, or compliance logging and a subcluster is split across a WAN, the external database server(s) must reside on the same side of the WAN as the Cisco IM and Presence Services that use them. With the ability to support multiple database instances on a single server and the requirement for an external database server to reside on the same side of the WAN, if a Cisco IM and Presence cluster is split across a WAN, then two external database servers will be required.

## Federated Deployment

Cisco IM and Presence 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.

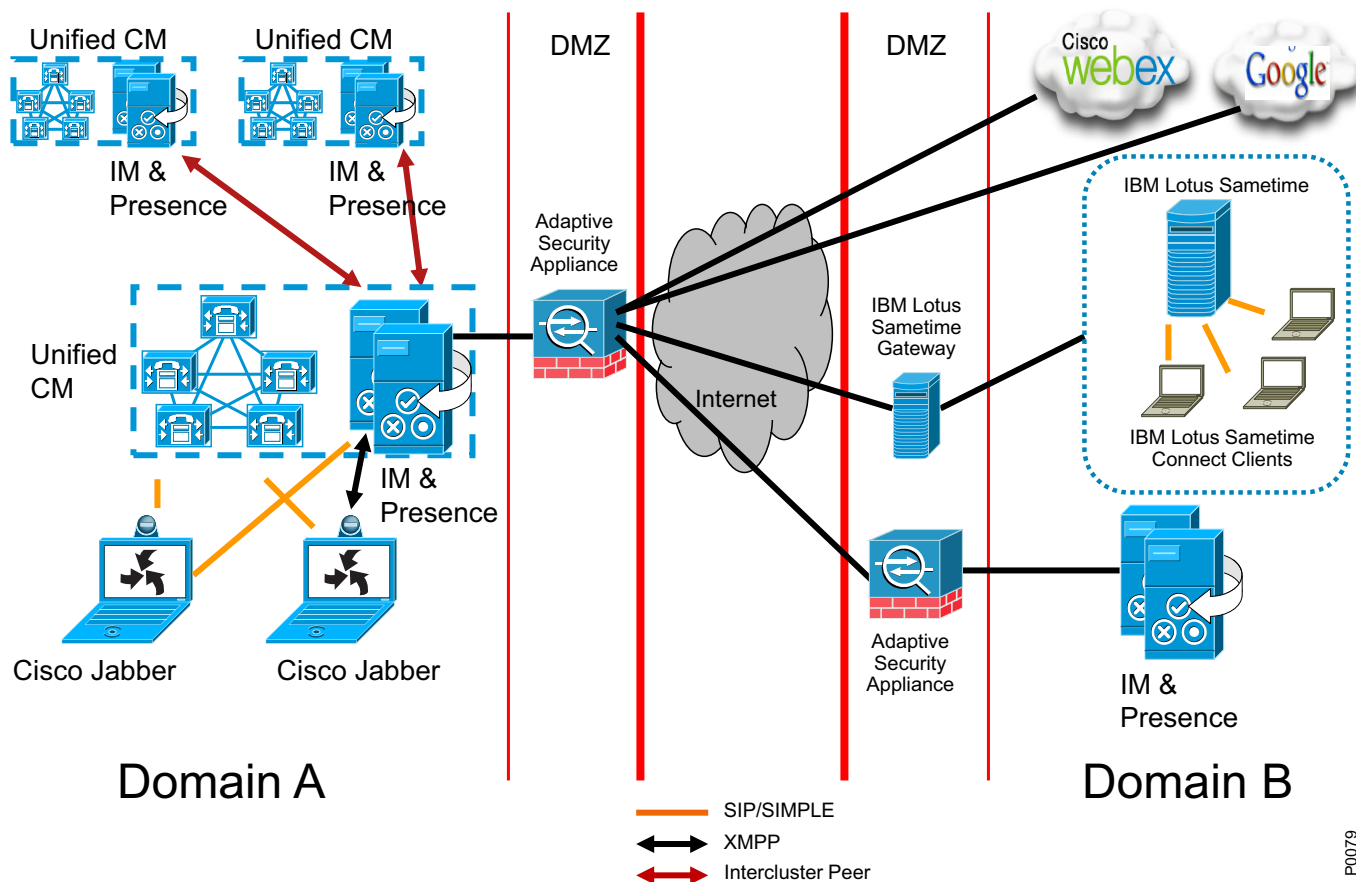
Cisco IM and Presence 10.x provides the ability to configure more than a single domain for federation. The domains are automatically discovered by the system when using DirectoryURI, or the domains can be added by the administrator manually. When a federated deployment involves multiple domains, then 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 *Integration Guide for Configuring Cisco IM and Presence Interdomain Federation*, available at

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

Figure 20-9 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 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.

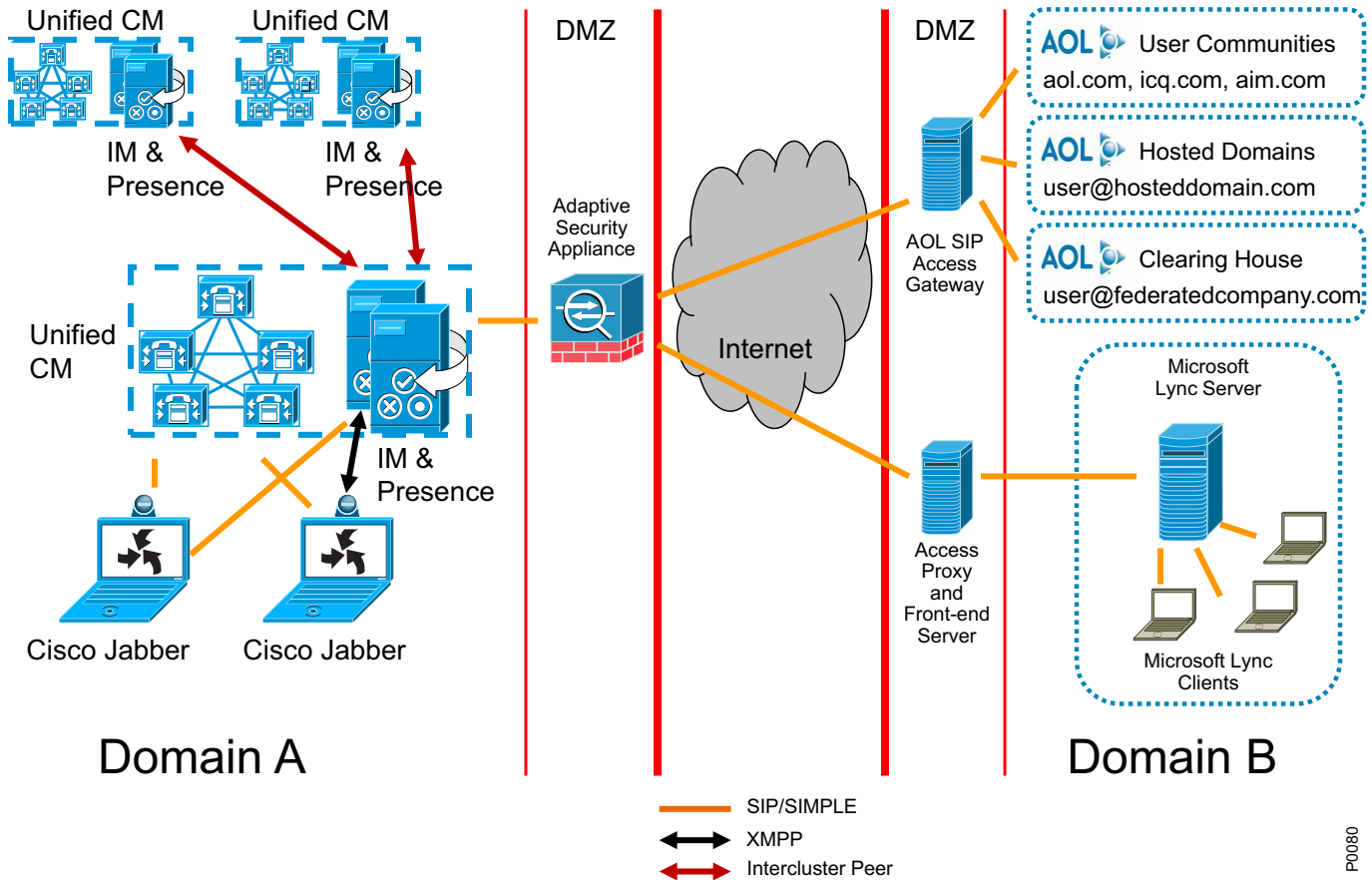
**Figure 20-9** IM and Presence XMPP Federation (Inter-Domain)

P0079

Cisco IM and Presence also provides configuration through SIP to allow for inter-domain federation with Microsoft and AOL, as depicted in [Figure 20-10](#). Cisco IM and Presence 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 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 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 20-10 IM and Presence SIP Federation (Inter-Domain)**

P0080

Table 20-3 lists the state mappings between Cisco IM and Presence and Microsoft Lync Server.

**Table 20-3 Mapping of Presence States**

Cisco Status	Cisco Color	Status to Microsoft Lync Server	Status to AOL
Out of office	RED	Away	Away
Do not disturb	RED	Busy	Away
Busy	RED	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 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 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 for the external domain.

The Cisco IM and Presence 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.

Additional configuration and deployment considerations regarding a federated deployment can be found in the latest version of the *Integration Guide for Configuring Cisco IM and Presence for Interdomain Federation*, available at

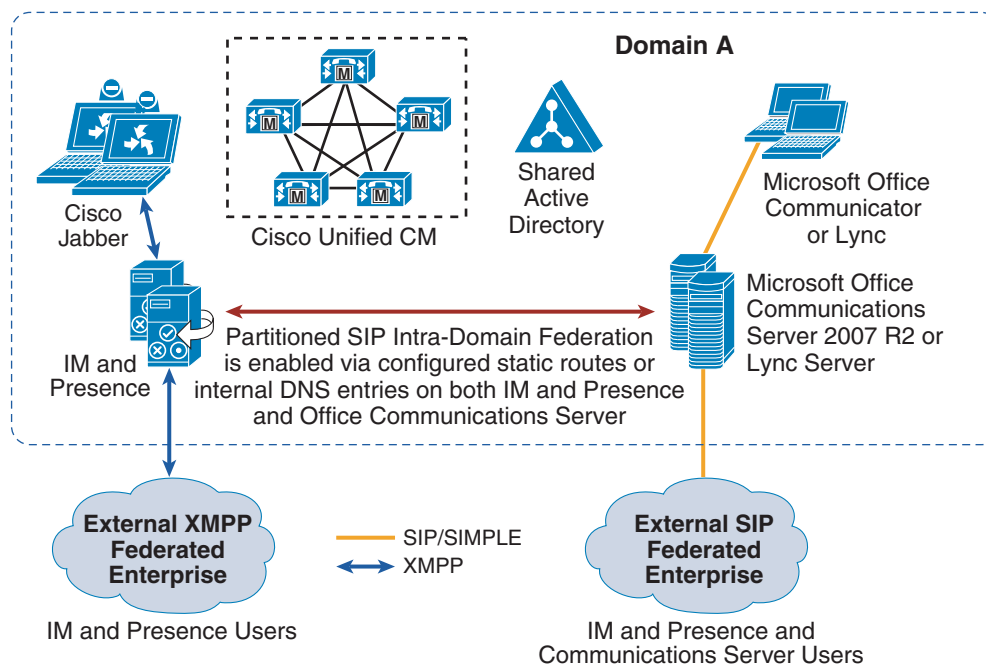
[http://www.cisco.com/en/US/products/ps6837/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html)

An intra-domain partitioned federated deployment, shown in Figure 20-11, is a secondary option that allows for Cisco IM and Presence 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 or on the Microsoft Lync Server.

**Note**

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

**Figure 20-11 Cisco IM and Presence Intra-Domain Federation**



292388

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 inter-domain federation support for Microsoft. Rich presence and group chat functionality are not supported with the partitioned intra-domain presence federation.

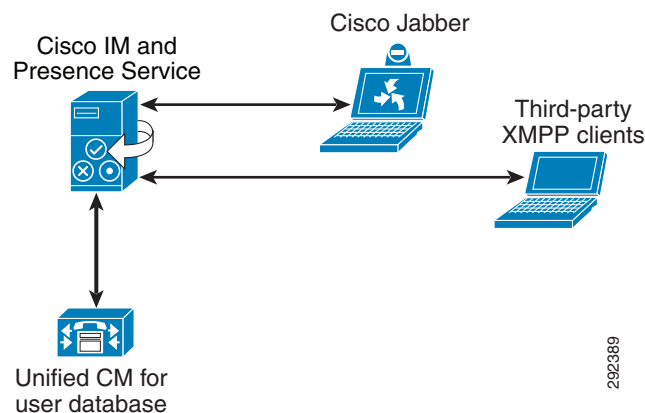
Inter-domain federation and partitioned intra-domain federation can be supported simultaneously with the following qualifications:

- XMPP federation may be enabled on the Cisco IM and Presence deployment but is available only to Cisco IM and Presence licensed users.
- SIP federation may be enabled either on Cisco IM and Presence 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 administration must be configured with static routes to the Microsoft environment for the external domain. Alternatively, Cisco IM and Presence could manage the SIP federation, while Microsoft Lync or Office Communications Server could manage the XMPP federation.

## Instant Messaging Only Deployment

Cisco IM and Presence allows for an enterprise-class instant messaging only solution, which provides full presence and instant messaging support as defined in the section on [On-Premises Cisco IM and Presence Enterprise Instant Messaging, page 20-27](#), to be deployed in cases where a full Unified Communications deployment is not yet provided. A Cisco IM and Presence cluster deployed in an instant messaging only environment supports up to three servers in a cluster (see [Figure 20-12](#)). Instant messaging only users on Cisco IM and Presence are still provisioned from Unified CM through the AXL/SOAP interface by means of LDAP synchronization or manual provisioning. Cisco Jabber and third-party XMPP clients are the supported clients in a Cisco IM and Presence instant messaging only deployment, and all other design guidelines for Cisco IM and Presence apply.

**Figure 20-12** *Instant Messaging Only User Mode Deployment*



292389

## On-Premises Cisco IM and Presence Migration

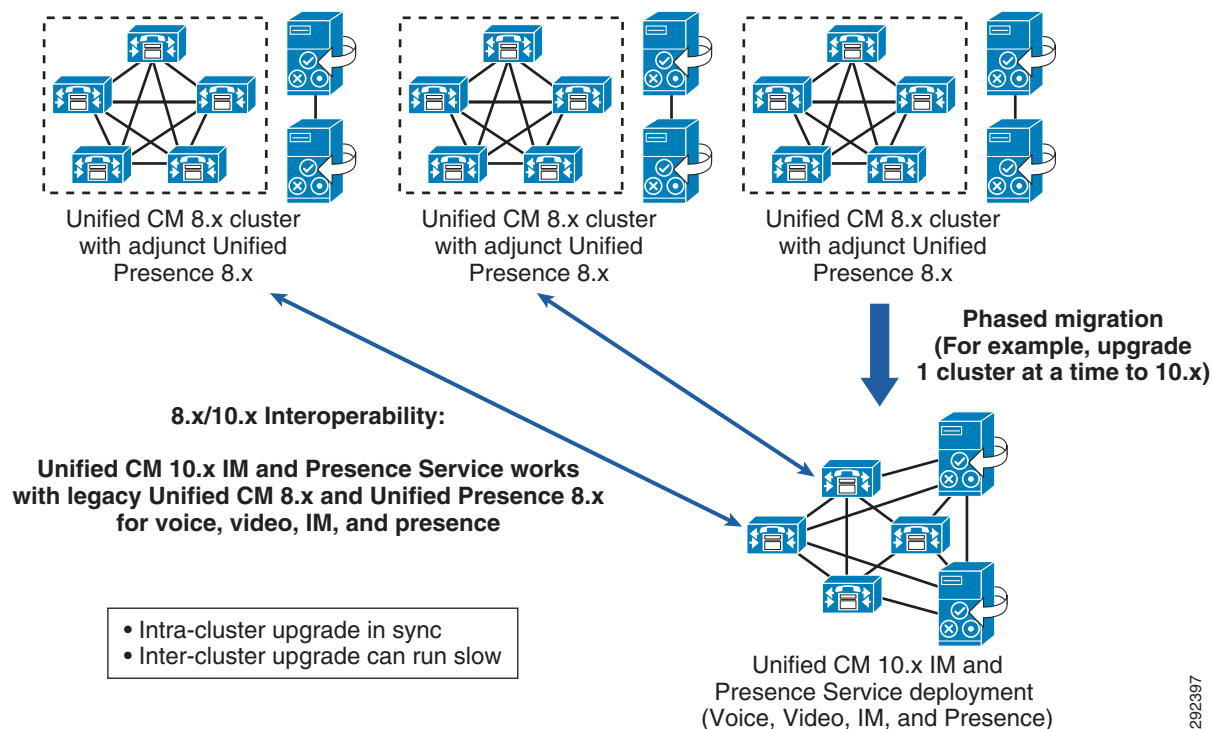
Cisco IM and Presence 10.x supports only virtualized server instances. Earlier versions of Cisco IM and Presence must migrate from Cisco MCS physical server hardware to Cisco Unified Computing System (UCS) virtualized hardware in order to deploy IM and Presence 10.x.

Migration from earlier releases of Cisco Unified Presence to Cisco IM and Presence is supported in the following cases (see [Figure 20-13](#)):

- Direct migration from Cisco Unified Communications Manager (Unified CM) 7.x or 8.x to Cisco Unified Communications 9.x IM and Presence — provides the ability to deploy Unified CM with voice, video, IM, and presence.
- Direct migration from Unified CM 7.x or 8.x and Cisco Unified Presence 8.x to Cisco Unified Communications 9.x IM and Presence — provides the ability to deploy Unified CM with voice, video, IM, and presence.

Earlier versions of Unified CM and Cisco Unified Presence require a multi-step upgrade migration.

**Figure 20-13** Large Enterprise Migration with Backward Compatibility



292397

# On-Premises Cisco IM and Presence Enterprise Instant Messaging

Cisco IM and Presence 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 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 SIP clients and XMPP clients is provided by IM internal gateway functionality.

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 handles storage for each of these instant messaging features in different locations. Offline instant messaging is stored locally in the Cisco IM and Presence IDS database. Ad-hoc group chat is stored locally in memory on Cisco IM and Presence. Persistent group chat requires an external database to store chat rooms and conversations. The external databases supported are PostgreSQL (see <http://www.postgresql.org/>) and Oracle (see <http://www.oracle.com>).

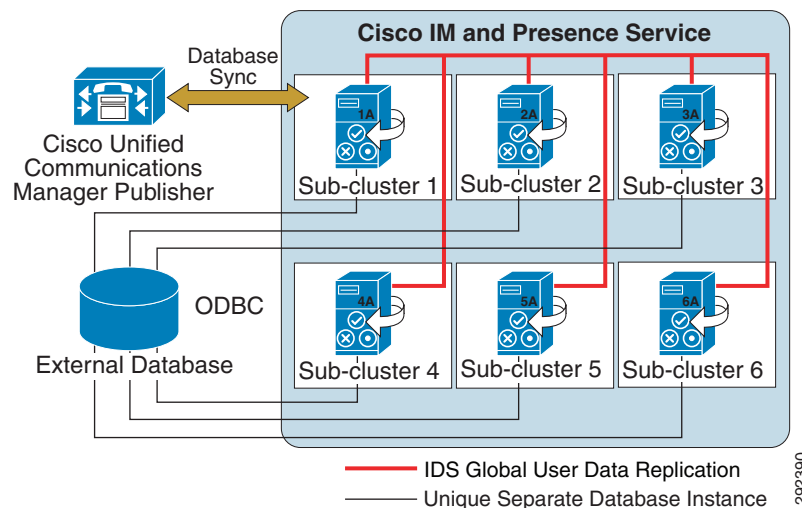


## Note

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

Cisco IM and Presence 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 is deployed with persistent group chat. (See [Figure 20-14](#).) The database instances can share the same hardware but are not required to do so.

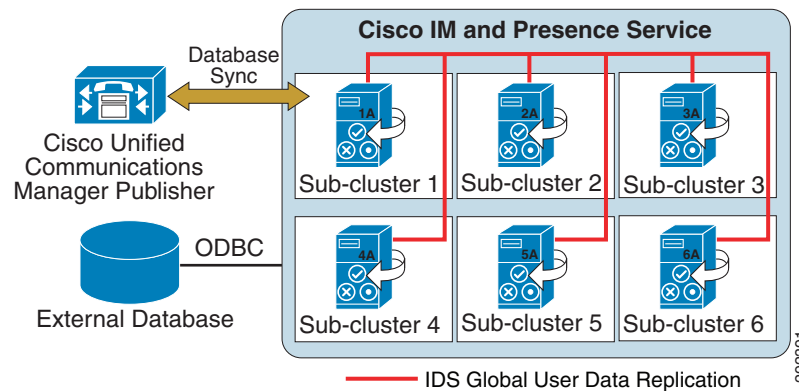
**Figure 20-14 Cisco IM and Presence Persistent Chat**



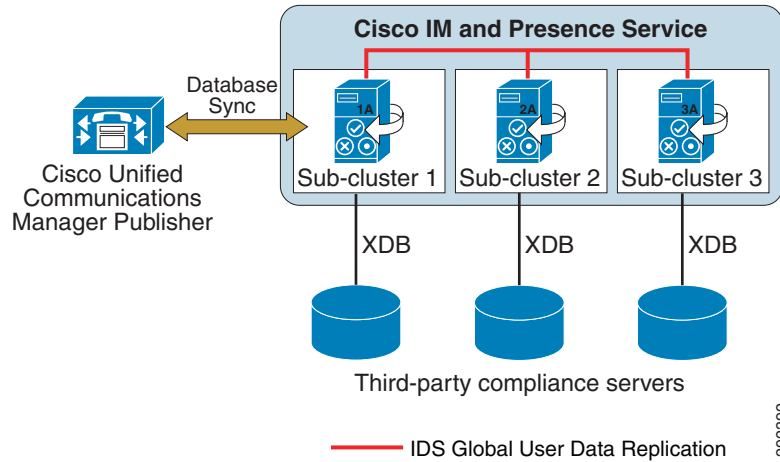
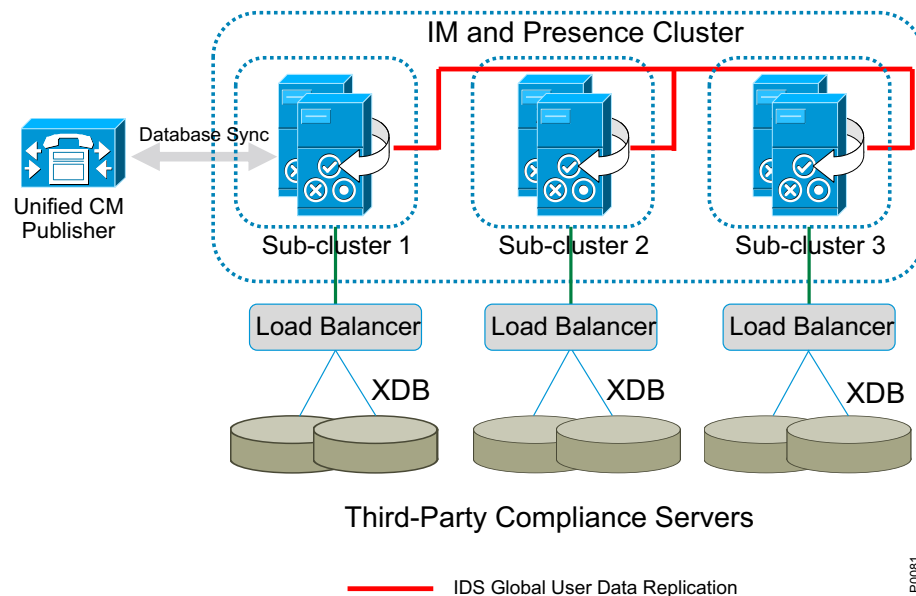
## On-Premises Cisco IM and Presence Message Archiving and Compliance

As part of the XCP architecture, Cisco IM and Presence 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 native compliance. Cisco IM and Presence native compliance and message archival requires an external database (PostgreSQL or Oracle) instance per cluster, as shown in [Figure 20-15](#). The same database can be shared with multiple clusters; however, a large number of users in an intercluster deployment might require multiple database servers.

**Figure 20-15** Cisco IM and Presence Native Compliance and Message Archiving



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. Cisco IM and Presence 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. All Cisco IM and Presence servers in the cluster are subject to compliance. [Figure 20-16](#) shows a deployment with a compliance server for each server in the IM and Presence cluster; whereas [Figure 20-17](#) shows a mapping of a single compliance server to multiple IM and Presence servers, or multiple compliance servers to a single IM and Presence server. The various deployment options allow for greater flexibility in compliance policy routing and cluster deployment.

**Figure 20-16 Cisco IM and Presence Third-Party Compliance****Figure 20-17 Full High Availability Cluster-Wide Compliance****Note**

Once the administrator selects the cluster-wide compliance and moves away from the 1:1 compliance mapping, it is not possible to revert back to 1:1 compliance mapping. Therefore, it is important to map out an appropriate third-party compliance server deployment when selecting 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.

## Instant Messaging 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. These calculations presume single-byte character data encoding; therefore, additional storage may be needed if internationalized character sets are used.

Cisco IM and Presence 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 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.

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 20-4](#) lists some examples of storage requirements for Cisco Collaboration Clients.

**Table 20-4** 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	1500	10	200	100	2.7 GB	3.0 GB
Medium	2500	15	200	250	10.2 GB	10.9 GB
High	2500	25	200	500	26.3 GB	27.5 GB

## On-Premises Cisco IM and Presence Calendar Integration

Cisco IM and Presence has the ability to retrieve calendar state and aggregate it into a presence status via the calendar module interface with Microsoft Exchange 2003, 2007, or 2010 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 with the calendar module interface of Microsoft Exchange 2003, 2007, or 2010.

Microsoft Exchange integration is supported with Microsoft Active Directory 2003 and Active Directory 2008 as well as Windows Server 2003 and Windows Server 2008. Microsoft Exchange 2003 or 2007 makes the calendar data available from the server through Outlook Web Access (OWA), which is built upon extensions to the WebDAV protocol (RFC 2518). Microsoft Exchange 2007 or 2010 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 (see [Table 20-5](#)).

**Note**

EWS and WebDAV cannot be configured on the same server.

**Table 20-5**      *Aggregated Presence State Based on Calendar State*

Cisco IM and Presence State	Calendar State
Available	Free / Tentative
Idle/Busy	Busy
Away	Out of Office <sup>1</sup>

1. Out of Office is specific for status set for a meeting only and does not reflect the Out Of Office status configured via the Out Of Office Assistant.

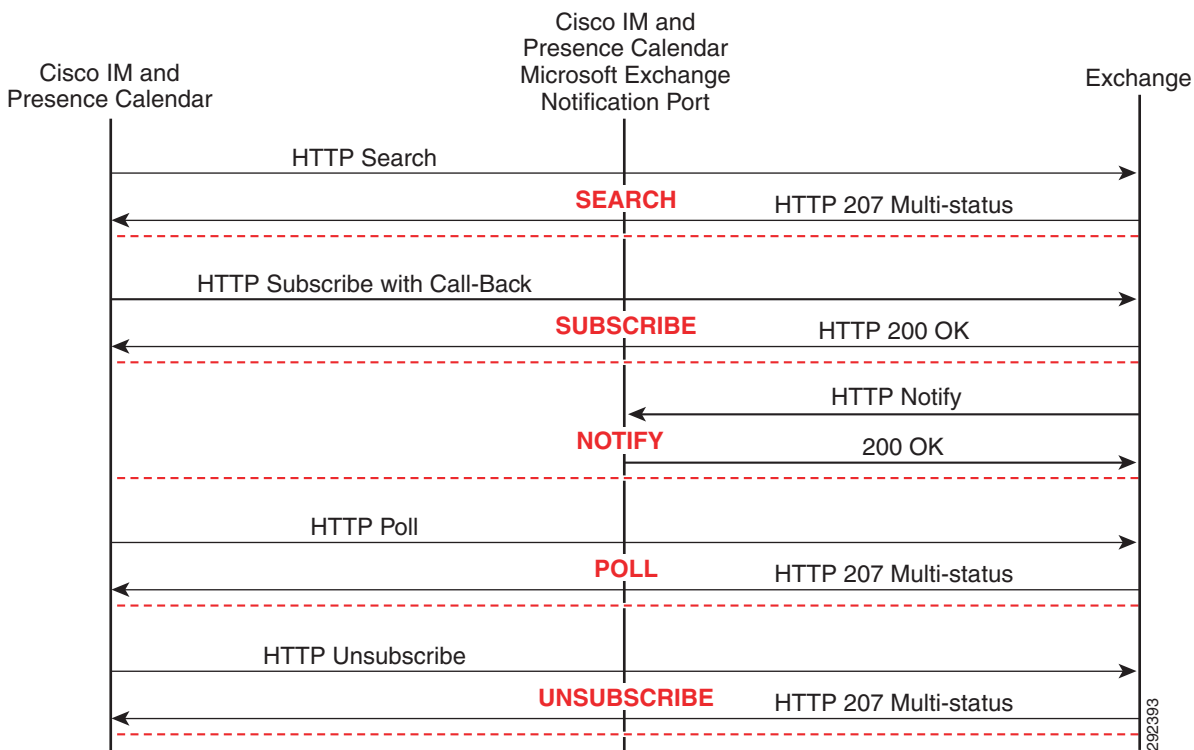
The exchange ID that is used to retrieve calendar information is taken from the email ID of the LDAP structure for that user. If the email ID does not exist or if LDAP is not being used, then the Cisco IM and Presence user ID is mapped as the exchange ID.

Information is gathered via a subscription for calendar state from the Cisco IM and Presence Service to the Microsoft Exchange server. [Figure 20-18](#) depicts this communication.

## Outlook Web Access Calendar Integration

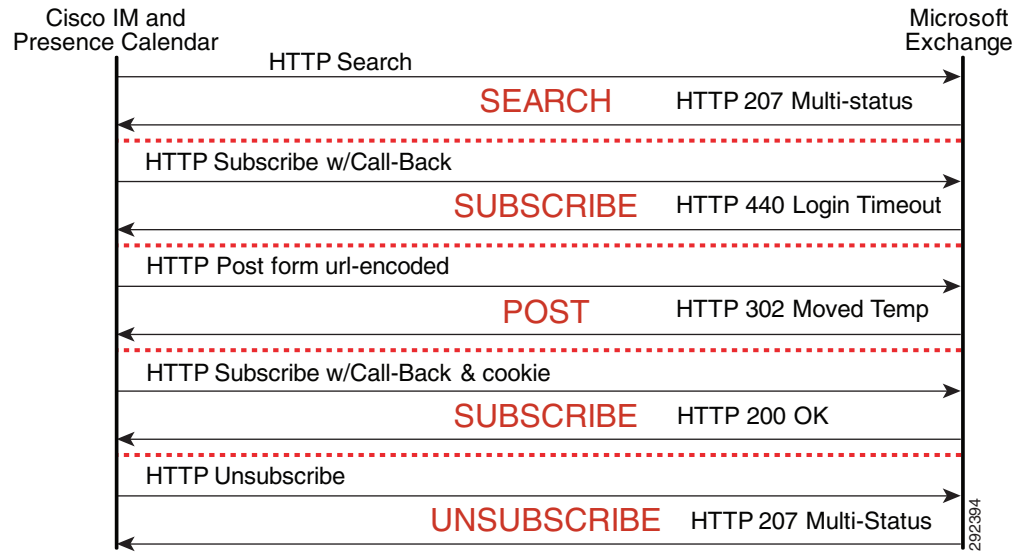
This feature requires a service parameter that is the port address for the UDP HTTP (Microsoft Exchange Notification Port) listen port. This port is where Microsoft Exchange sends any notifications (indicated by the NOTIFY message) indicating a change to a particular subscription identifier for calendar events. (See [Figure 20-18](#).)

**Figure 20-18 Outlook Web Access Communication Between Cisco IM and Presence and Microsoft Exchange**



The SEARCH transaction is used to search a user's calendar relevant to a given interval, and is invoked when the user has set a preference to include the calendar information in the presence status. The results of the search are converted into a list of free/busy state transitions. The SUBSCRIBE message indicates the subscription for notifications to changes in the free/busy state of the user in the folder /exchange/userX/Calendar. The POLL method is used to acknowledge that the client has either received or responded to a particular event, while the UNSUBSCRIBE message is used to terminate a previous subscription or subscriptions.

Cisco IM and Presence Outlook Web Access integration supports enabling of Forms Based Authentication, which performs an additional HTTP POST transaction request containing the actual URL of the Exchange Server encoded as part of the header, as shown in [Figure 20-19](#).

**Figure 20-19 Forms Based Authentication with Cisco IM and Presence Calendar****Note**

Cisco IM and Presence 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 will honor the REDIRECT message to the exchange server that is hosting the user for which Cisco IM and Presence 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, as well as Cisco Unified Communications Manager, must have the appropriate locales installed for the users to select their locale.
- Cisco IM and Presence 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 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

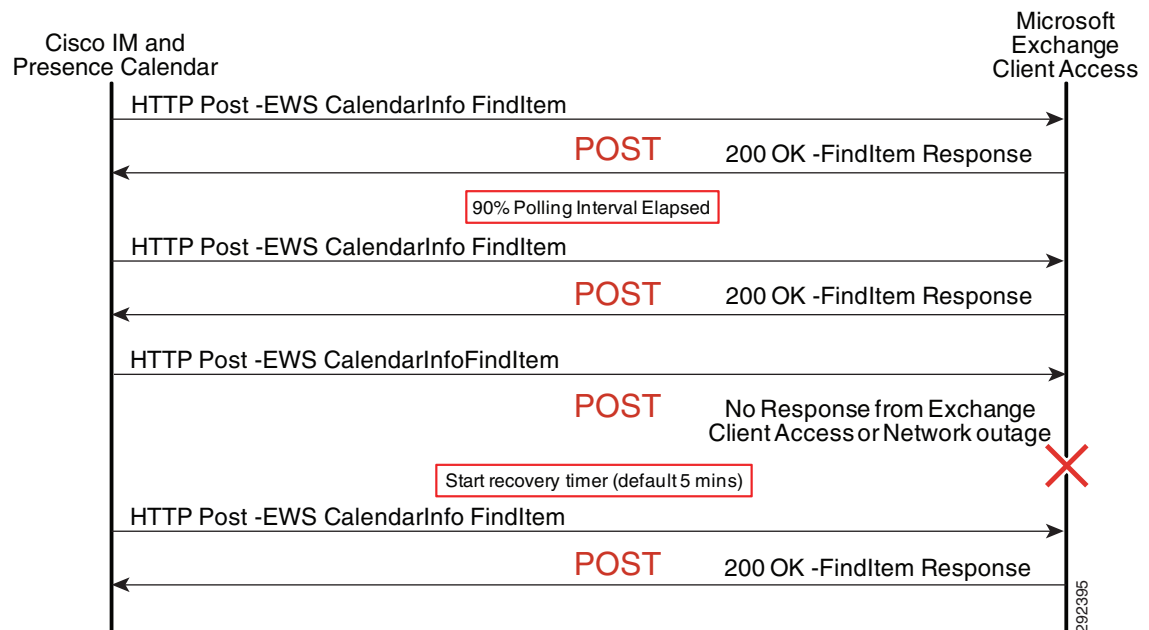
Cisco IM and Presence can be configured to allow for Microsoft Exchange Web Services to collect calendar state information to be aggregated into an overall presence view of the user. If the users mailbox is located on the configured Exchange server, Cisco IM and Presence will communicate directly with the Exchange server; whereas, if the users mailbox is located on a different Exchange server than the one configured, Cisco IM and Presence 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 calendar integration is supported with a single Microsoft Exchange forest only.

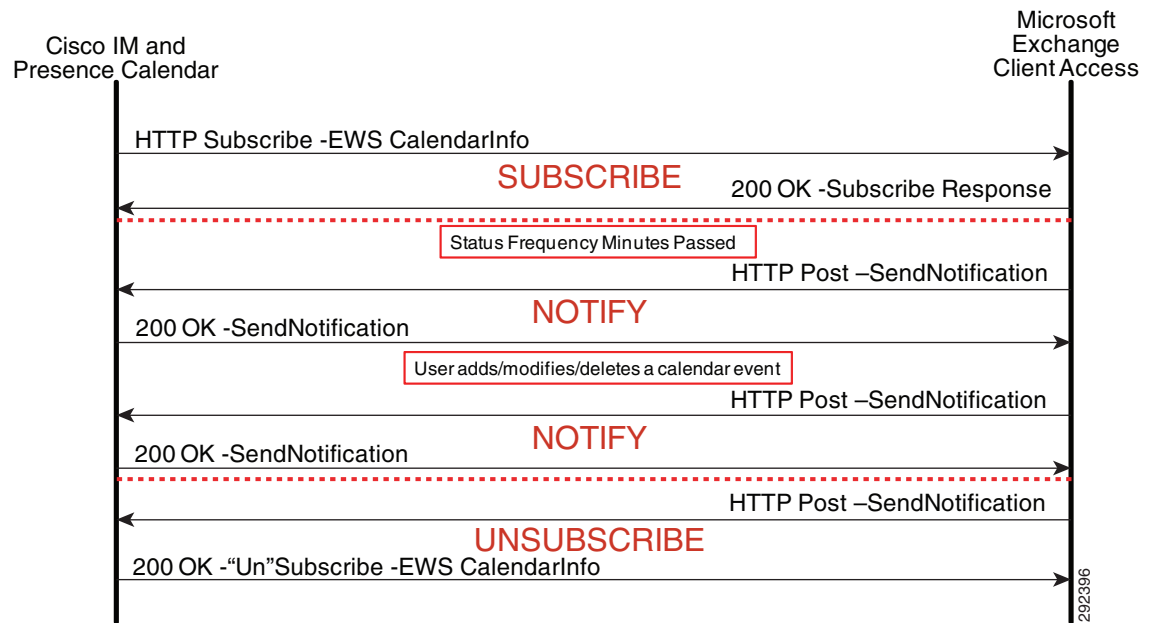
Cisco IM and Presence Exchange Web Services calendar integration supports both a polling of calendar information as shown in [Figure 20-20](#) as well as a subscription/notification for calendar information as shown in [Figure 20-21](#). Various configuration parameters control the rate of polling intervals, 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

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

**Figure 20-20 Exchange Web Services Polling with Cisco IM and Presence Calendar**



**Figure 20-21 Exchange Web Services Subscription/Notification with Cisco IM and Presence Calendar**



Exchange Web Services Auto Discover is also supported by Cisco IM and Presence 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 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 Mobility Integration

Cisco IM and Presence 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 via AXL/SOAP and SIP.

An application user must be configured on Cisco IM and Presence and Cisco Unified CM before Cisco Unified CM can establish an administrative session with Cisco IM and Presence. Cisco Jabber Mobile IM end-user logins will generate a Cisco Unified CM SOAP request to Cisco IM and Presence 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 Third-Party Open API

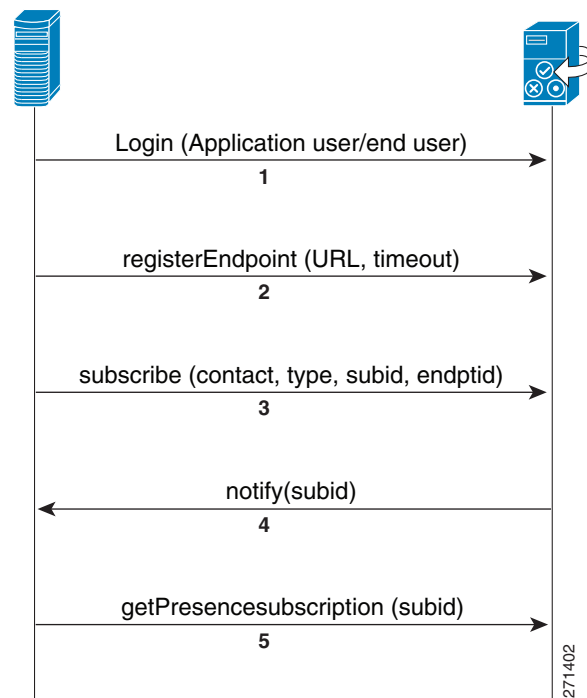
Cisco IM and Presence has the ability to integrate with third-party applications through HTTP in addition to SIP/SIMPLE and XMPP. The HTTP interface has a configuration interface as well as a presence interface via Representational State Transfer (REST). The Third-Party Open API provides two mechanisms 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 <http://developer.cisco.com/web/cdc>

### Real-Time Eventing Model

The real-time eventing model uses an application user on Cisco IM and Presence 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 20-22](#) highlights the Third-Party Open API real-time eventing model interaction with Cisco IM and Presence.

**Figure 20-22 Third-Party Open API Real-Time Eventing Model**



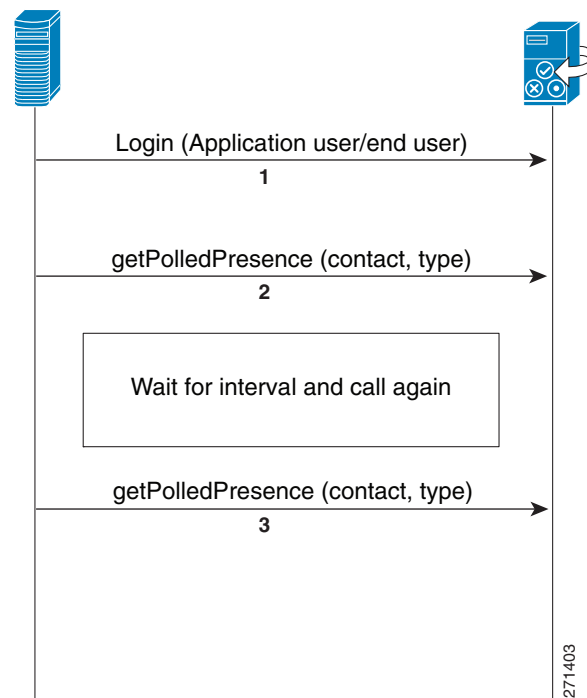
The call flow in [Figure 20-22](#) illustrates the following sequence of events:

1. The application initiates a SOAP login request to Cisco IM and Presence via the super-user application user (APIUser), and Cisco IM and Presence 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 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 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 20-23](#) highlights the Third-Party Open API polling model interaction with Cisco IM and Presence.

**Figure 20-23** Third-Party Open API Polling Model



The call flow in [Figure 20-23](#) illustrates the following sequence of events:

1. The application initiates a SOAP login request to Cisco IM and Presence via the super-user application user (APIUser), and Cisco IM and Presence 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. The client XMPP interface is treated as a normal XMPP client within Cisco IM and Presence; 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. 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:

- 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 deployment.
- To improve performance, balance the Third-Party Open API users across all servers in the Cisco IM and Presence cluster.

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

<http://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:

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

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

- 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 marks Layer 3 IP packets via Differentiated Services Code Point (DSCP). Cisco IM and Presence marks all call signaling 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 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.
- Use the User Assignment Mode for Presence Server enterprise parameter default of **balanced** for best overall cluster performance.

- Cisco IM and Presence requires an external database instance for each server in the cluster for persistent chat, and one database instance per cluster for message archiving. Native compliance supports mapping of all or a sub-set of servers in an IM and Presence cluster to one external compliance database. Third-party compliance supports flexible deployments where there can be multiple compliance servers per IM and Presence server, multiple IM and Presence servers per compliance server, or some combination. The external databases supported are PostgreSQL and Oracle, and all IM and Presence servers in the cluster are subject to compliance.
- Cisco IM and Presence supports a total of 45,000 users per cluster for full Unified Communications mode or 75,000 users for IM-only 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, refer to *Port Usage Information for Cisco IM and Presence*, available at

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

## Third-Party Presence Server Integration

Cisco IM and Presence 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:

<http://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 with Microsoft Lync.

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

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

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

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

- Communications between Cisco IM and Presence 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 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 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 platform.

Cisco Unified Communications Manager OVA Template	Number of Microsoft Office Communicator or Lync Users Supported per Server <sup>1</sup>	Number of Microsoft Office Communicator or Lync Users Supported per Cluster <sup>1</sup>
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

1. These numbers are based on Cisco Unified CM 7.1(3) and later releases.

- 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 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 publisher and subscriber.
- You can configure routing of the SIP messages to Cisco IM and Presence 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

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

## IBM Lotus Sametime for Phone Control and Presence (PCAP)

Cisco provides the following guidelines around how best to integrate IBM Lotus Sametime Server with Cisco Unified Communications, but does not contend configuration, deployment, or best practice procedures for IBM Communications products.

For all setup, configuration, and deployment of IBM Lotus Sametime Server, refer to the documentation at

<http://www.ibm.com/>

Cisco does not provide configuration, deployment, or best practice procedures for IBM communications products, but Cisco does provide the guidelines listed below for integrating IBM Lotus Sametime Server with a Cisco Unified Communications system.

#### **Guidelines for Integrating Cisco IM and Presence with IBM Lotus Sametime Server (Version 7.5.1 and Later)**

Click-to-call and click-to-conference functionality integrated within the IBM Lotus Sametime client is handled via a Cisco Call Control plugin resident on IBM Lotus Sametime Server. The integration into Cisco Unified Communications for click-to-call and click-to-conference functionality is handled via the SIP trunk interface with Unified CM. The integration into Cisco Unified Communications for presence functionality is handled via the SIP/SIMPLE interface with Cisco IM and Presence.

- The Unified CM SIP trunk for click-to-call and click-to-conference functionality must be configured for out-of-dialog REFER processing. Enable the Accept Out-of-Dialog REFER checkbox in the SIP Trunk Security Profile associated with the SIP trunk communicating with IBM Lotus Sametime Server.
- The Cisco Call Control plugin, resident on IBM Lotus Sametime Server, maintains a configured list of Unified CMs utilized in a round-robin manner. This list should be populated with the IP address of Unified CM subscribers that have been configured with the out-of-dialog REFER SIP trunks.

The Unified CM list can also be configured with DNS SRV; however, currently this SRV logic is used for redundancy only and not for load balancing, therefore it is not a recommended setting.

- Deployment topologies using IBM Lotus Sametime Server typically will integrate with multiple Unified CM clusters due to the capacity differences between the two systems. With the Cisco Click-to-Call plugin utilizing a list of Unified CMs in a round-robin fashion, a call initiation can result in a REFER being sent to a cluster different from the user's home cluster. The Unified CM receiving this call setup will process the REFER and generate an INVITE to the appropriate destination to complete the call setup.
- Traffic marking has not been implemented fully with the Cisco Call Control plugin. Therefore, follow the traffic marking guidelines in the *Enterprise QoS Solution Reference Network Design (SRND)*, available at

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

## **In-the-Cloud Service and Architecture**

This section describes the in-the-cloud service and architecture for Cisco IM and Presence. 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

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

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

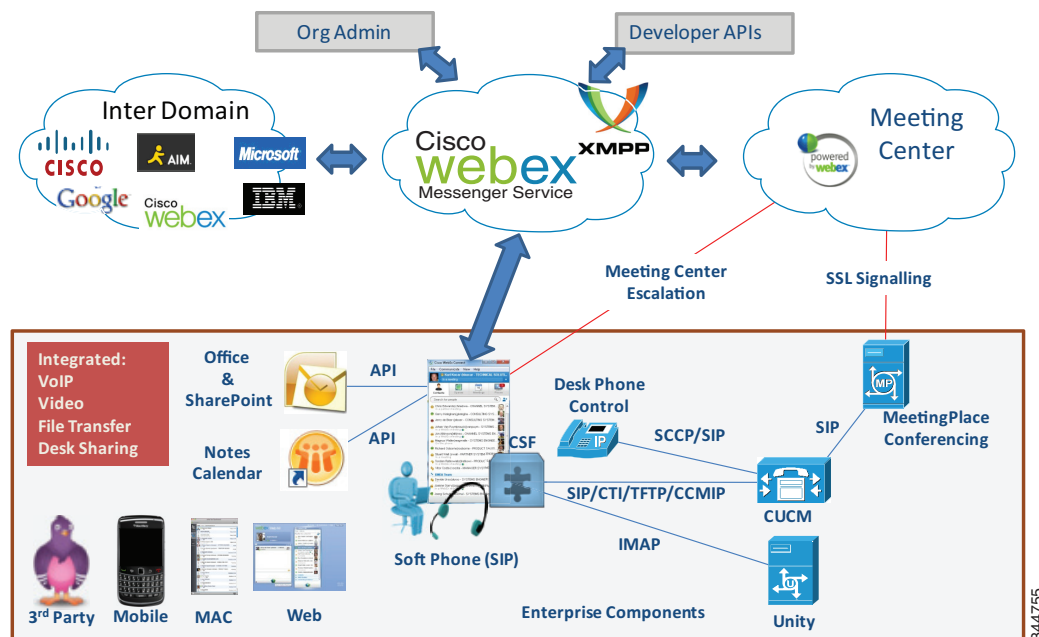
[http://www.cisco.com/en/US/solutions/ns1007/collaboration\\_cloud.html](http://www.cisco.com/en/US/solutions/ns1007/collaboration_cloud.html)

## Deploying Cisco WebEx Messenger Service

A Cisco WebEx Messenger solution deployment consists of the following components, as depicted in Figure 20-24:

- 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 20-24** Deploying Cisco WebEx Messenger Service



## Centralized Management

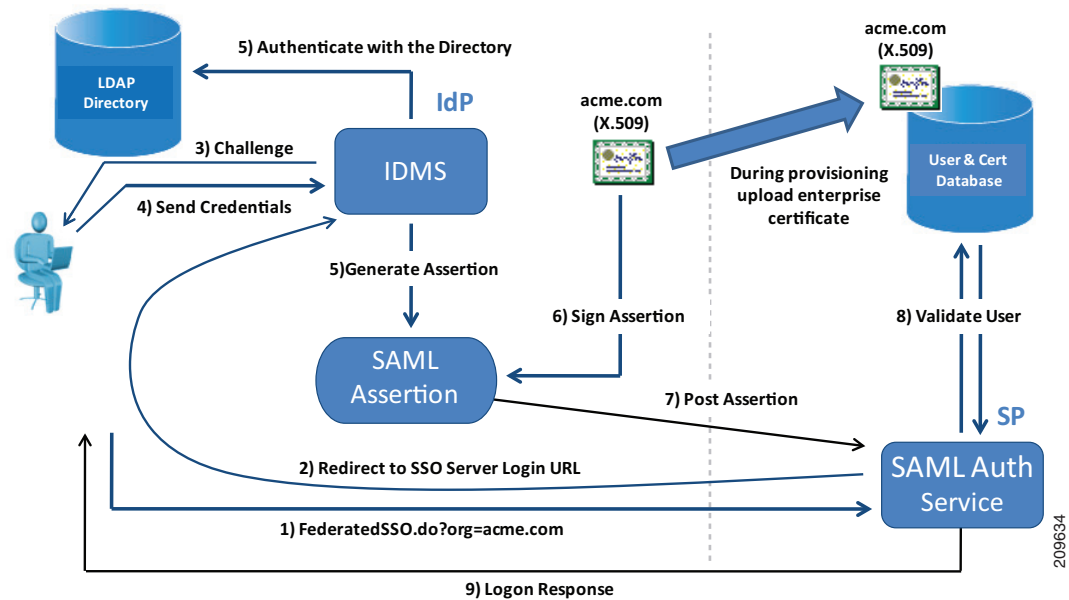
Cisco WebEx Messenger service provides a web-based administrative tool to manage the solution across the organization. Cisco WebEx Messenger service users are configured and managed through the Cisco WebEx Administration Tool, which enables administrators to set up basic security and policy controls 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

<http://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 by allowing users to securely log into Cisco WebEx Messenger service using their corporate login credentials. The user's login credentials are not sent to Cisco, thus protecting the user's corporate login information. Figure 20-25 shows the credential handshake that occurs on user login to Cisco WebEx Messenger.

**Figure 20-25** 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.

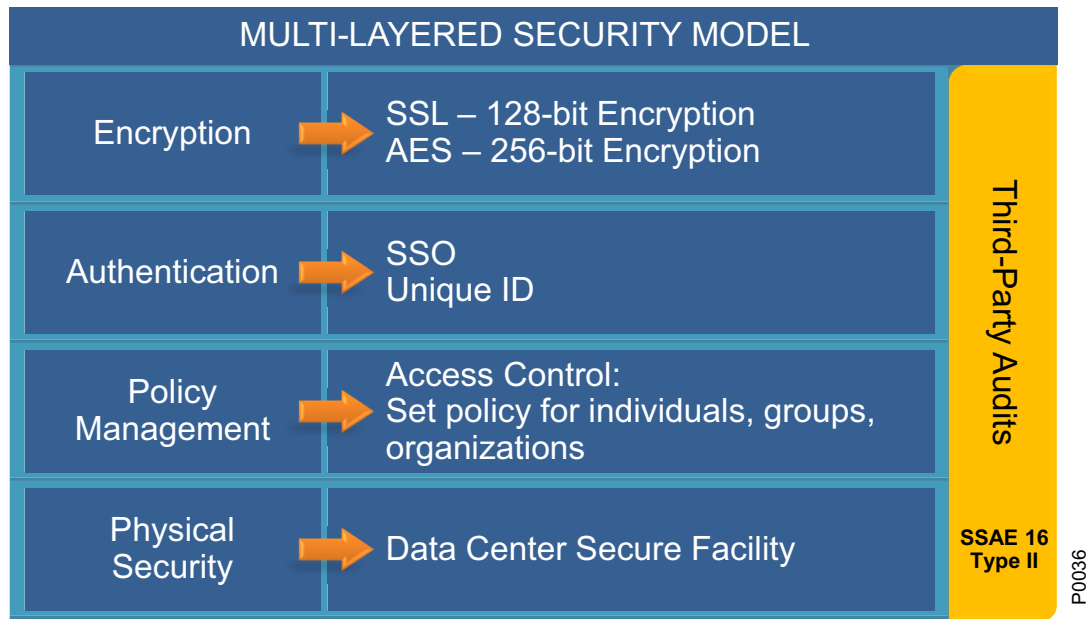
For more information on Single Sign On with WebEx Messenger service, refer to the documentation available at

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

## Security

The Cisco WebEx security model consists of functional layers of security. Figure 20-26 illustrates the separate but interrelated elements that compose each layer.

**Figure 20-26 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

[http://www.cisco.com/en/US/products/ps10528/prod\\_white\\_papers\\_list.html](http://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 though 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

<http://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

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

Cisco Webex Messenger deployment network requirements are available at

<http://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

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

<http://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

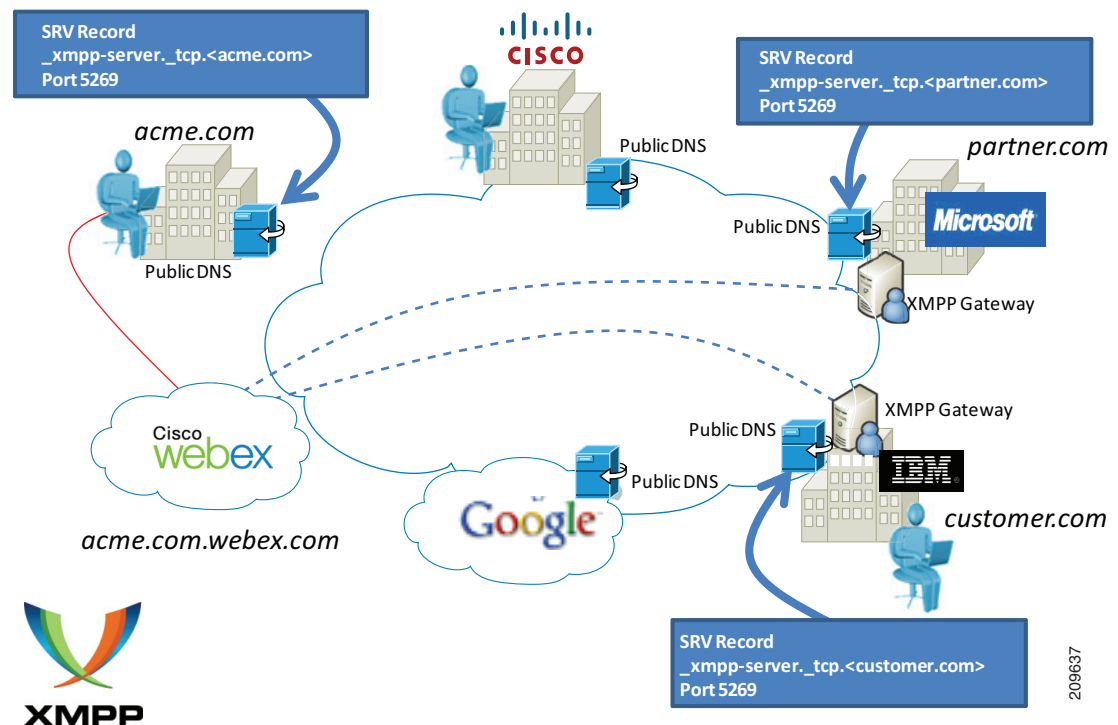
<http://www.webex.com/webexconnect/orgadmin/help/index.htm>

### 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 20-27.) A list of public instant messaging networks based on XMPP is available at

<http://xmpp.org/>

**Figure 20-27 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

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