Cisco Jabber for Mac Installation and Configuration Guide

First Published: July 06, 2011

Last Modified: February 16, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

Overview of Cisco Jabber for Mac

Overview of Cisco Jabber for Mac

Cisco Jabber for Mac streamlines communications and enhances productivity by unifying availability, instant messaging, voice, voice messaging, desktop sharing, and conferencing capabilities securely into one client on your desktop. Cisco Jabber for Mac delivers secure, clear, and reliable communications, offers flexible deployment models, is built on open standards and integrates with commonly used desktop applications. Communicate and collaborate effectively from anywhere you have an Internet connection.

What's new in Cisco Jabber for Mac

Release 8.6.2

The following features were added to Cisco Jabber for Mac Release 8.6.2:

- Support for OS X Lion (version 10.7.x).
- Support for click-to-IM in addition to click-to-call from embedded tel: or xmpp: links.
- The **Sign In** tab under **Preferences** > **General** has been renamed **General**.

Release 8.6.3

The development effort for this release concentrated on bug fixes. Consult the Limitations and Restrictions and Caveats sections of the Release Notes for details.

Release 8.6.4

The following improvements have been made in Cisco Jabber for Mac Release 8.6.4:

- Desktop share for OS X Lion stability issues resolved, and desktop share reenabled.
- Improved connectivity of phone/voicemail services whenever there's network interface change.
- Improved overall stability of softphone feature.
- Visual enhancements to chat tabs for a consistent look and feel.
- Enhanced phone services icons in hub menu to ensure proper color when selected.
- Space character now permitted in user ID in CUP mode.
- Enhanced CUCM failover and fallback.
- Improved CUP failover, especially during abrupt shutdowns.
- Improved display of contact photos in OS X Lion.
- VPN support expanded to include Cisco VPN release 5.0 and Cisco AnyConnect.

Release 8.6.5

The following improvements have been made in Cisco Jabber for Mac Release 8.6.5:

- Added support for Mac OS 10.8.
- Enhancements to support the MacBook Pro with Retina Display.

This release also includes numerous bug fixes. Consult the Limitations and Restrictions and Caveats sections of the Release Notes for details.

How to use this guide

This guide is designed to help you install, configure, and perform administrative tasks for Cisco Jabber for Mac. The following table will direct you to the sections of this guide that are relevant to your needs:

If you want to:	Consult the following section(s):
Deploy Cisco Jabber for Mac in an on-demand environment using Cisco Collaboration Cloud	Overview of Cisco Jabber for Mac on-demand deployment
Deploy Cisco Jabber for Mac in an on-premises environment using Cisco Unified Presence	Overview of Cisco Jabber for Mac on-premises deployment
Configure or administrate telephony for Cisco Jabber for Mac	For on-demand deployment: see Getting started with Cisco Unified Communications Manager for Click to Call. For on-premises deployment: Deploy Cisco Jabber for Mac on-premises, on page 7
Configure or administrate voicemail for Cisco Jabber for Mac	For on-demand deployment: see Specifying Visual Voicemail settings. For on-premises deployment: Deploy Cisco Jabber for Mac on-premises, on page 7

Configure or administrate meetings for Cisco Jabber for Mac	For on-demand deployment: see Understanding additional services. For on-premises deployment: Deploy Cisco Jabber for Mac on-premises, on page 7
Distribute the Cisco Jabber for Mac client	For on-demand deployment: see Overview of Cisco Jabber for Mac on-demand deployment. For on-premises deployment: see Distribute the Cisco Jabber for Mac client, on page 45

Deploy certificates for Cisco Jabber for Mac

Cisco Jabber for Mac features a new security enhancement that provides users with a warning dialog in the event that a certificate cannot be validated (due to self-signage, incorrect name or date, or other reasons). As long as the certificate is valid and trusted, the dialog will not appear.

Cisco provides users with the opportunity to "Continue" connecting from the warning dialogs when Cisco Jabber for Mac is deployed into networks with self-signed certificates. Users also have the option to mark the self-signed certificate as "Always Trust," which places the certificate in the user's Keychain and eliminates the warning dialog on subsequent launches.

Users may become frustrated when presented with several warning dialogs when first launching the product, since Cisco Jabber for Mac connects to many servers. In order to resolve this issue and improve the user experience, Cisco recommends that administrators acquire proper certificates that are issued from a trusted Certificate Authority. When Cisco Jabber for Mac is presented with a valid certificate, it will connect normally without prompting the user (unless the user has chosen the option to see certificates before Cisco Jabber for Mac connects).

Alternatively, you can provide self-signed certificates that the user can install on his or her local machine. The user will not encounter the dialog box if the certificates are already in place when Cisco Jabber for Mac launches.

Perform the following steps to deploy self-signed certificates to users:

Procedure

Step 1 Download the "tomcat-trust" certificate from the Cisco Unified OS administration interface, under **Security** > **Certificate Management**.

Step 2 Download the corresponding certificates from the Cisco Unified Presence and Unity servers, where applicable.

Step 3 Concatenate the certificates into a single file with the extension **.pem** (for example, "companyABCcertificates.pem").

Step 4 Send the file to your Cisco Jabber for Mac users and ask them to double-click it. Doing so launches the Keychain Access application and imports the certificates.

Note:

The operating system requires that the user enter the Mac OS X administration password for each certificate that is being imported.

CHAPTER 2

Deploy Cisco Jabber for Mac on-demand

Overview of Cisco Jabber for Mac on-demand deployment

You can deploy Cisco Jabber for Mac in an on-demand (or "cloud") environment by using the Cisco WebEx Connect Administration Tool. To learn how to use this tool, consult the Cisco WebEx Connect Administration Guide:

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

You may also download a PDF of the guide.

Recommended installation

To perform this type of deployment from start to finish, Cisco recommends that you follow the steps below in the order specified:

1. Configure organization information. See Understanding the Configuration Tab.
2. Create and provision users. See Overview of User Management.
3. Configure IM and availability. See Cisco WebEx Connect federation with other instant messaging providers.
4. Configure telephony services. See Getting started with Cisco Unified Communications Manager for Click to Call.
5. Configure voicemail. See Specifying Visual Voicemail settings.
6. Configure meetings. See Understanding additional services.

Note This is a list of high-level tasks that may not include every aspect of your configuration. Consult the individual links for more information.

Distribute the client

You can obtain the Cisco Jabber for Mac client from either of the following download links:

http://downloadbts.webexconnect.com/jabber/mac/uc-client-mac.zip

http://download.webexconnect.com/jabber/mac/uc-client-mac.zip

CHAPTER 3

Deploy Cisco Jabber for Mac on-premises

This chapter describes how to deploy Cisco Jabber for Mac in an on-premises environment, using Cisco Unified Presence.

Overview of Cisco Jabber for Mac on-premises deployment

You can deploy Cisco Jabber for Mac in an on-premises environment by leveraging the following key Cisco technologies:

- Cisco Unified Presence
- Cisco Unified Communications Manager
- Cisco Unity Connection
- Cisco Unity
- Cisco MeetingPlace

Note This guide has been prepared to align with Cisco Unified Presence release 8.6(1). The system administration interface and menu choices described in the procedures that follow may vary with other versions of Cisco Unified Presence. For example, references to Cisco Unified Personal Communicator have been updated to Cisco Jabber in Cisco Unified Presence release 8.6(3).

Recommended installation

To perform this type of deployment, Cisco recommends that you configure your system in the following order:

1. Configure directory (LDAP) services
2. Configure firewall
3. Create and provision users
4. Configure IM and availability
5. Configure optional features (federated IM, telephony, voicemail, meetings)
6. Distribute the client

Note This is a list of high-level tasks that may not include every aspect of your configuration. Consult the On-premises deployment checklist for a more detailed example of a typical deployment.

You should also be aware that you will occasionally switch from entering information in the Cisco Unified Presence Administration Tool to entering information in the Cisco Unified Communications Manager Administration Tool.

On-premises deployment checklist

The following checklist describes a typical on-premises deployment of Cisco Jabber for Mac for your reference. Your organization's deployment may vary.

1. Configure Cisco Unified Presence settings
2. Start essential services, on page 10
3. Configure firewall(s)
4. Deploy certificates for Cisco Jabber for Mac
5. Configure LDAP Servers
6. Configure a Secure Connection Between Cisco Unified Presence and the LDAP Directory
7. Create LDAP profiles and add users
8. Configure the LDAP attribute map
9. Configure LDAP Synchronization for User Provisioning
10. Configure LDAP Authentication
11. Enable Instant Messaging Policy, on page 21
12. Fetch Contact Pictures from a Web Server
13. Option: Configure federated IM
14. Option: Configure telephony
15. Option: Configure voicemail

16 Option: Configure meetings

17 Distribute the Cisco Jabber for Mac client

Before you deploy

Configure Cisco Unified Presence settings

Note You must perform this task in Cisco Unified Presence.

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **Settings**.

Step 2 Enter information into the fields:

Field	Setting
CSF certificate directory (relative to CSF install directory)	This field applies only if the Client Services Framework (CSF) requires you to import security certificates to authenticate with LDAP, web conferencing, and CCMCIP. For most deployments, you do not need to import security certificates. You only need to import security certificates for CSF to trust in the following scenarios: • You use a signed certificate for Cisco Unified Communications Manager Tomcat instead of the default self-signed certificate. • You want CSF to connect to the LDAP server via LDAPS. • You use a signed certificate for Cisco Unity Connection Tomcat instead of the default self-signed certificate. If you must specify a value, specify the directory that contains the security certificates as an absolute path. If you do not specify a directory, CSF looks for the certificates in the default directory and trusts any certificates in that location. Default Setting: Not set

Credentials source for voicemail service	If user credentials for the voicemail service are shared with another service, select the appropriate service from this list box. The user credentials automatically synchronize from the service that you select. Default Setting: Not set **Troubleshooting Tips** If this value is set to Not set, users must enter their credentials manually using the Preferences menu from the client.
Credentials source for web conferencing service	If user credentials for the meeting service are shared with another service, select the appropriate service from this list box. The user credentials automatically synchronize from the service that you select. Default Setting: Not set **Troubleshooting Tips** If this value is set to Not set, users must enter their credentials manually using the Preferences menu from the client.
Maximum message size	Enter the allowed size limit for instant messages, in bytes.
Allow cut & paste in instant messages	Check this check box to allow users to cut and paste in their instant messages (IMs). Default Setting: On

Step 3 Select **Save**.

Start essential services

Note You must perform this task in Cisco Unified Communications Manager.

To deploy Cisco Jabber, start the following Cisco Unified Presence Extensible Communication Platform (XCP) services on all Cisco Unified Presence nodes in all clusters:

- Cisco Unified Presence XCP Authentication Service
- Cisco Unified Presence XCP Connection Manager

You may also start the following optional Cisco Unified Presence XCP services on all Cisco Unified Presence nodes in all clusters, depending on what features you want to make available:

- Cisco Unified Presence XCP Text Conference Manager, for group chat.
- Cisco Unified Presence XCP SIP Federation Connection Manager, to support federation services with third-party applications that use SIP.
- Cisco Unified Presence XCP XMPP Federation Connection Manager, to support federation services with third-party applications that use XMPP.
- Cisco Unified Presence XCP Counter Aggregator, if you want system administrators to be able to view statistical data on XMPP components.
- Cisco Unified Presence XCP Message Archiver, for automatic archiving of all instant messages.

Note Read the documentation relating to any feature that you are implementing before you turn on the relevant services. Additional configuration might be required.

Procedure

Step 1 Select **Cisco Unified Serviceability** > **Tools** > **Control Center - Network Services**.

Step 2 Select the desired Cisco Unified Presence server from the **Server** list box.

Step 3 Select **Go**.

Step 4 Confirm the Cisco UP XCP Router service is running.

Step 5 If the Cisco UP XCP Router service is not running, do the following:

a) Select the radio button next to the **Cisco UP XCP Router** service in the **CUP Services** section.
b) Select **OK**.

Step 6 Select **Cisco Unified Serviceability** > **Tools** > **Service Activation**.

Step 7 Select the desired Cisco Unified Presence server from the **Server** list box.

Step 8 Select **Go**.

Step 9 Select **Cisco UP XCP Directory Service**.

Step 10 Select **Save**.

Firewall requirements for Cisco Jabber for Mac

Internet traffic moves through a firewall based on service identification numbers that are known as ports. Ports are an organizational concept used categorize and prioritize traffic. The primary purpose of a firewall is to recognize the traffic that moves through it and to allow or deny the traffic based on its port number. Firewalls must be configured to allow traffic on certain ports for Cisco Jabber to work properly. Network administrators typically block all unnecessary traffic on their networks. This involves only opening those ports that are required by enterprise-specific applications and closing all others.

There are two types of firewalls that may be encountered in the enterprise environment, software and hardware firewalls. Software firewalls exist as a component of most modern computer operating systems. They are intended to provide a basic level of security at the individual user level. When users run Cisco Jabber for the first time, they may be asked to **Accept** or **Unblock** the application. This is the operating system software

firewall asking if the application should be allowed to run. Users should be notified of this and provided information on how to properly respond. If users experience problems with availability, phone mode switching, or instant messages, the firewall might be denying connections despite the previous allowed setting. Restart Cisco Jabber. If this does not resolve the issue, return to the Firewall settings, remove Cisco Jabber, and add it again to the list of applications that allow incoming connections.

Hardware firewalls are network devices that provide protection from unwanted traffic at an enterprise level. Hardware firewalls must be configured to allow the ports carrying traffic for Cisco Jabber. The following table lists the ports used by Cisco Jabber. These ports must be open on all firewalls for Cisco Jabber to function properly.

Port	Protocol	Description
Inbound		
16384-32766	UDP	Receives Real-Time Transport Protocol (RTP) media streams for audio. These ports are configured in Cisco Unified Communications Manager.
Outbound		
69	UDP	Connects to the Trivial File Transfer Protocol (TFTP) server to download the TFTP file.
80	TCP HTTP	Connects to services such as Cisco Unified MeetingPlace or Cisco WebEx for meetings, Cisco Unity or Cisco Unity Connection for voicemail features.
143	IMAP (TCP / TLS)	Connects to Cisco Unity or Cisco Unity Connection to retrieve and manage the list of voice messages for the user, and the voice messages themselves.
389	TCP	Connects to the LDAP server for contact searches.
443	TCP HTTPS	Connects to services such as Cisco Unified MeetingPlace or Cisco WebEx for meetings, Cisco Unity or Cisco Unity Connection for voicemail features.
636	LDAPS	Connects to the secure LDAP server for contact searches. **Note** Cisco Jabber for Mac does not support port 3269 (Active Directory Global Catalog over LDAPS).

993	IMAP (SSL)	Connects to Cisco Unity or Cisco Unity Connection to retrieve and manage the list of voice messages for the user, and the voice messages themselves.
2748	TCP	Connects to the CTI gateway, which is the CTIManager component of Cisco Unified Communications Manager.
5060	UDP / TCP	Provides Session Initiation Protocol (SIP) call signaling.
5061	TCP	Provides secure SIP call signaling.
5222	TCP (XMPP)	Connects to the Cisco Unified Presence server for availability status and instant messaging features.
7993	IMAP (TLS)	Connects to Cisco Unity Connection to retrieve and manage the list of secure voice messages for the user, and the secure voice messages themselves.
8191	TCP	Connects to the local port to provide Simple Object Access Protocol (SOAP) web services.
8443	TCP	Connects to the Cisco Unified Communications Manager IP Phone (CCMCIP) server to get a list of currently-assigned devices.
16384-32766	UDP	UDP Sends RTP media streams for audio.
44442	HTTP	The client listens for events from Cisco Unified Client Services Framework.

Configure IM and Availability

Configure LDAP Servers

Note You must perform this task in Cisco Unified Presence.

Before You Begin

- Configure the LDAP attribute map.
- Obtain the hostnames or IP addresses of the LDAP directories.

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **LDAP Server**.

Step 2 Select **Add New**.

Step 3 Enter the LDAP server name.

Step 4 Enter an IP address or an FQDN (Fully Qualified Domain Name) of the LDAP server.

Step 5 Specify the port number used by the LDAP server. The defaults are:

- TCP—389
- TLS—636

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

Step 6 Select **TCP** or **TLS** for the protocol type.

Step 7 Select **Save**.

Configure a Secure Connection Between Cisco Unified Presence and the LDAP Directory

Before You Begin

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

Procedure

Step 1 Select **Cisco Unified OS Administration** > **Security** > **Certificate Management**.

Step 2 Select **Upload Certificate**.

Step 3 Select **directory-trust** from the **Certificate Name** menu.

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

Step 5 Select **Upload File**.

Step 6 Restart the Tomcat service from the CLI using this command:

```
utils service restart Cisco Tomcat
```

Create LDAP Profiles and Add Users

Before You Begin

Cisco Jabber connects to an LDAP server on a per-search basis. If the connection to the primary server fails, Cisco Jabber attempts the first backup LDAP server, and if it is not available, it then attempts to connect to the second backup server. Cisco Jabber also periodically attempts to return to the primary LDAP server. If an LDAP query is in process when the system fails over, the next available server completes this LDAP query.

You can see LDAP server information in the **Server Health** window in Cisco Jabber (**Help** > **Show System Diagnostics**). If Cisco Jabber cannot connect to any of the LDAP servers, it reports the failure in the **System Diagnostics** window.

- Specify the LDAP server names and addresses.
- You must create the LDAP profile before you can add Cisco Jabber for Mac licensed users to the profile.

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **LDAP Profile**.

Step 2 Select **Add New**.

Step 3 Enter information into the fields.

Field	Setting
Name	Enter the profile name limited to 128 characters.
Description	(Optional) Enter a description limited to 128 characters.
Bind Distinguished Name	(Optional) Enter the administrator-level account information limited to 128 characters. This is the distinguished name with which you bind for authenticated bind. The syntax for this field depends on the type of LDAP server that you deploy. For details, see the LDAP server documentation.

Anonymous Bind	(Optional) Uncheck this option to use the user credentials to sign in to this LDAP server. For non-anonymous bind operations, Cisco Jabber receives one set of credentials. If configured, these credentials must be valid on the backup LDAP servers. **Note** If you check Anonymous Bind, users can sign in anonymously to the LDAP server with read-only access. Anonymous access might be possible on your directory server, but Cisco does not recommend it. Instead, create a user with read-only privileges on the same directory where the users to be searched are located. Specify the directory number and password in Cisco Unified Presence for Cisco Jabber to use.
Password	(Optional) Enter the LDAP bind password limited to 128 characters. This is the password for the administrator-level account that you provided in the Bind Distinguished Name string to allow users to access this LDAP server.
Confirm Password	Reenter the same password as the password you entered in the Password field. (Optional) After configuring Cisco Unified Presence for authenticated bind with the LDAP server, configure the LDAP server for anonymous permissions and anonymous login so that all directory information (name, number, mail, fax, home number, and so forth) is passed to the Cisco Jabber client.
Search Context	(Optional) Enter the location where you configured all the LDAP users. This location is a container or directory. The name is limited to 256 characters. Only use a single OU/LDAP search context. **Note** If you integrate with Microsoft Active Directory: • Set O and OU (OU must contain users; for example, ou=users, dc=cisco, dc=com). For example, cn=users, DC=EFT-LA,DC=cisco, DC=com • The search base should include all users of Cisco Jabber.
Recursive Search	(Optional) Check to perform a recursive search of the directory starting at the search base.
Primary LDAP Server and Backup LDAP Server	Select the primary LDAP server and optional backup servers.

Make this the Default LDAP Profile for the System	(Optional) Check to add any new users to the system into this default profile. If you turn on this setting, Cisco Unified Presence adds any users that it synchronizes from Cisco Unified Communications Manager to this default profile. Cisco Unified Presence only adds users to this default profile after you select the default profile (and you turn on the Sync Agent). Cisco Unified Presence does not change any existing profile configuration. Therefore, Cisco recommends that you select and configure the default profile before you turn on the Sync Agent.
Add Users to Profile	Select the button to open the **Find and List Users** window. Select **Find** to populate the search results fields. Alternatively, search for a specific users and select **Find**. To add users to this profile, select the users, and select **Add Selected**.

Step 4 Select **Save**.

Configure the LDAP Attribute Map

Note You must perform this task in Cisco Unified Presence.

Before You Begin

You must configure the LDAP attribute map on Cisco Unified Presence where you enter LDAP attributes for your environment and map them to the given Cisco Jabber for Mac attributes.

If you want to use LDAP to store your employee profile photos, you must either use a third-party extension to upload the photo files to the LDAP server, or extend the LDAP directory server schema by other means to create an attribute that the LDAP server can associate with an image. For Cisco Jabber for Mac to display the profile photo, in the LDAP attribute map, you must map the Cisco Jabber for Mac "Photo" value to the appropriate LDAP attribute. By default, Cisco Jabber for Mac uses the jpegPhoto LDAP attribute to display the user photo, which is present in the Windows 2003 and 2007 Active Directory schema. Note that Windows 2000 Active Directory uses the thumbnailPhoto attribute.

Note

- Contact photos may be cropped when they are displayed in Cisco Jabber for Mac.
- The UPC UserID setting in the LDAP attribute map must match the Cisco Unified Communications Manager user ID. This mapping allows a user to add a contact from LDAP to the Contact list in Cisco Jabber for Mac. This field associates the LDAP user with the associated user on Cisco Unified Communications Manager and Cisco Unified Presence.
- You can map an LDAP field to only one Cisco Jabber field.

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **Settings**.

Step 2 Select a supported LDAP server from **Directory Server Type**.
The LDAP server populates the LDAP attribute map with Cisco Jabber user fields and LDAP user fields.

Step 3 If necessary, make modifications to the LDAP field to match your specific LDAP directory.
The values are common to all LDAP server hosts. Note the following LDAP directory product mappings:

Product	LastName Mapping	UserID Mapping
Microsoft Active Directory	SN	sAMAccountName
iPlanet, Sun ONE or OpenLDAP	SN	uid

Step 4 Select **Save**.

Troubleshooting Tips

- If you want to stop using the current attribute mappings and use the factory default settings, select **Restore Defaults**.

Indexed Active Directory Attributes

The following Active Directory attributes must be indexed:

- sAMAccountName
- displayName
- mail
- msRTCSIP-PrimaryUserAddress

Any attributes that are used for contact resolution must also be indexed. For example, you might need to index the following attributes:

- telephoneNumber
- Any other directory phone number attributes that are be used to find contacts, depending on the value of the DisableSecondaryNumberLookups key
- ipPhone, if this attribute is used in your environment

Configure LDAP Authentication

Note You must perform this task in Cisco Unified Communications Manager.

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

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

Before You Begin

Enable LDAP synchronization on Cisco Unified Communications Manager.

Procedure

Step 1 Select **Cisco Unified Communications Manager Administration** > **System** > **LDAP** > **LDAP Authentication**.

Step 2 Check **Use LDAP Authentication for End Users**.

Step 3 Configure the LDAP authentication settings.

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

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

Step 5 Click **Save**.

Troubleshooting Tips

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

Configure LDAP Synchronization for User Provisioning

Note You must perform this task in Cisco Unified Communications Manager.

LDAP synchronization uses the Cisco Directory Synchronization (DirSync) tool on Cisco Unified Communications Manager to synchronize information (either manually or periodically) from a corporate LDAP directory. When you enable the DirSync service, Cisco Unified Communications Manager automatically provisions users from the corporate directory. Cisco Unified Communications Manager still uses its local database, but disables its facility to allow you to create user accounts. You use the LDAP directory interface to create and manage user accounts.

- Make sure that you install the LDAP server before you attempt the LDAP-specific configuration on Cisco Unified Communications Manager.
- LDAP synchronization does not apply to application users on Cisco Unified Communications Manager.
- Activate and start the Cisco DirSync service on Cisco Unified Communications Manager.

Note You must manually provision application users in the Cisco Unified Communications Manager Administration interface.

Procedure

Step 1 Select **Cisco Unified Communications Manager Administration** > **System** > **LDAP** > **LDAP System**.

Step 2 Select **Add New**.

Step 3 Configure the LDAP server type and attribute.

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

Step 5 Click **Save**.

Step 6 Select **Cisco Unified Communications Manager Administration** > **System** > **LDAP** > **LDAP Directory**.

Step 7 Select **Add New**.

Step 8 Configure the following items:

- LDAP directory account settings
- User attributes to be synchronized
- Synchronization schedule
- LDAP server hostname or IP address, and port number

Step 9 Check **Use SSL** if you want to use Secure Socket Layer (SSL) to communicate with the LDAP directory.

Step 10 Click **Save**.

Troubleshooting Tips

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

Enable Instant Messaging Policy

Note You must perform this task in Cisco Unified Presence.

This procedure describes how to turn on or off IM capabilities for all IM client applications in a Cisco Unified Presence cluster. IM capabilities are turned on by default on Cisco Unified Presence.

Caution When you turn off IM capabilities on Cisco Unified Presence, all group chat functionality (ad hoc and persistent chat) will not work on Cisco Unified Presence. Cisco recommends that you do not turn on the Cisco UP XCP Text Conference service or configure an external database for persistent chat on Cisco Unified Presence.

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Messaging** > **Settings**.

Step 2 Configure the IM settings as follows:

If You Want To…	Do This…
Turn on IM capabilities for client applications in the Cisco Unified Presence cluster. If you turn on this setting, local users of client applications can send and receive IMs. If you turn off this setting, local users of client applications cannot send and receive IMs. Users can only use the IM application for availability and phone operations.	Check **Enable instant messaging**.
Allow users of client applications to log IM history on Cisco Unified Presence. You can prevent or allow users to log IM history locally on their computer. On the client side, the application must support this functionality; it must enforce the prevention of IM logging.	Check **Allow clients to log instant message history (on supported clients only)**.

Step 3 Select **Save**.

Step 4 Restart the Cisco UP XCP Router service.

Turn IM History Logging On or Off

Note You must perform this task in Cisco Unified Presence.

You can prevent or allow users to log IM history locally on their computer. On the client side, the application must support this functionality; it must enforce the prevention of IM logging.

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Messaging** > **Settings**.

Step 2 Configure the IM history log as follows:

If You Want To…	Do This…
Allow users of client applications to log IM history on Cisco Unified Presence.	Check **Allow clients to log instant message history (on supported clients only)**.
Prevent users of client applications from logging IM history on Cisco Unified Presence.	Uncheck **Allow clients to log instant message history (on supported clients only)**.

Step 3 Select **Save**.

Fetch Contact Pictures from a Web Server

You can configure a parameterized URL string in the Photo field in the LDAP attribute map so that Cisco Jabber can fetch pictures from a web server instead of from the LDAP server. The URL string must contain an LDAP attribute with a query value containing a piece of data that uniquely identifies the photo of the user. Cisco recommends that you use the User ID attribute. However, you can use any LDAP attribute whose query value contains a piece of data that uniquely identifies the photo of the user.

Cisco recommends that you use *%%<userID>%%* as the substitution string, for example:

- http://mycompany.example.com/photo/std/%%uid%%.jpg
- http://mycompany.example.com/photo/std/%%sAMAccountName%%.jpg

You must include the double percent symbols in this string, and they must enclose the name of the LDAP attribute to substitute. Cisco Jabber removes the percent symbols and replaces the parameter inside with the results of an LDAP query for the user whose photo it resolves.

For example, if a query result contains the attribute “uid” with a value of “johndoe,” then a template such as http://mycompany.com/photos/%%uid%%.jpg creates the URL http://mycompany.com/photos/johndoe.jpg. Cisco Jabber attempts to fetch the photo.

This substitution technique works only if Cisco Jabber can use the results of the query and can insert it into the template you specify above to construct a working URL that fetches a JPG photo. If the web server that hosts the photos in a company requires a POST (for example, the name of the user is not in the URL) or uses some other cookie name for the photo instead of the username, this technique does not work.

Note

- The URL length is limited to 50 characters.
- Cisco Jabber does not support authentication for this query; the photo must be retrievable from the web server without credentials.

Configure IM Policy Settings

This procedure contains information on configuring general IM policy settings.

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Presence** > **Settings**.

Step 2 Perform the following configuration:

If You Want To . . .	Do This
Turn on automatic authorization so that Cisco Unified Presence automatically authorizes all availability subscription requests it receives from Cisco Jabber for Mac users in the local enterprise.	Check **Allow users to view the availability of other users without being prompted for approval.**
Turn off automatic authorization so that Cisco Unified Presence sends all availability subscriptions to the client where the user is prompted to authorize or reject the subscription.	Uncheck **Allow users to view the availability of other users without being prompted for approval.**

Step 3 Select **Cisco Unified Presence Administration** > **Messaging** > **Settings**.

Step 4 Perform the following configuration:

If You Want To . . .	Do This
Globally disable instant messaging services.	Uncheck **Enable instant messaging**.
Globally enable offline instant messaging.	Uncheck **Suppress Offline Instant Messaging**.
Globally display client instant messaging history.	Check **Allow clients to log instant message history (on supported clients only)**.

Step 5 Select **Save**.

Step 6 Restart the Cisco UP XCP Router service.

Optional configurations

Third-party XMPP client support

Requirements for supporting third-party XMPP clients

Support for Third-Party XMPP Clients

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

License Requirements for Third-Party Clients

For each user of an XMPP client application, you require a Cisco Unified Presence user feature license. The Cisco Unified Presence user feature license consumes one Cisco Unified Communications Manager Device License Unit (DLU). On Cisco Unified Communications Manager, you will need to upload the user DLU, and assign Cisco Unified Presence capabilities to the user.

XMPP Client Integration on Cisco Unified Communications Manager

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

- Configure the licensing requirements. Upload the user DLU, and then assign Cisco Unified Presence capabilities for the user.
- Configure the users and devices. Associate a device with each user, and associate each user with a line appearance.

LDAP Integration for XMPP Contact Search

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

Domain Name for XMPP Clients

The domain name on the XMPP client, specifically the XMPP connection attempt domain name, must match the domain on Cisco Unified Presence. To verify the domain value on Cisco Unified Presence, select **Cisco Unified Presence Administration** > **System** > **Cluster Topology**, select **Settings** in the right pane, and verify the Domain Name value.

DNS Configuration for XMPP Clients

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

Configure a secure connection between Cisco Unified Presence and XMPP clients

To configure a secure connection between your Cisco Unified Presence server and third-party XMPP clients:

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **System** > **Security** > **Settings.**

Step 2 To establish a secure TLS connection between Cisco Unified Presence and XMPP client applications in a cluster, select **Enable XMPP Client To CUP Secure Mode**.
Cisco recommends that you do not turn off this secure mode unless the XMPP client application can protect the client login credentials in non-secure mode. If you do turn off the secure mode, verify that you can secure the XMPP client-to-server communication in some other way.

Step 3 To establish a secure TLS connection between Cisco Unified Presence and XMPP-based API client applications in a cluster, select **Enable Web Client To CUP Secure Mode**.
If you turn on this setting, upload the certificates or signing certificates for the web client in the `cup-xmpp-trust` repository on Cisco Unified Presence.

Step 4 Select **Save.**

Enable support for third-party XMPP clients

To enable support for third-party XMPP clients, perform the following steps for each node of your Cisco Unified Presence cluster:

Procedure

Step 1 Select **Cisco Unified Serviceability** > **Tools** > **Service Activation**.

Step 2 Select the Cisco Unified Presence server from the **Server** menu.

Step 3 Turn on the following services:

- Cisco UP XCP Connection Manager - Turn on this service if you are integrating third-party XMPP clients on Cisco Unified Presence.
- Cisco UP XCP Authentication Service - Turn on this service if you are integrating third-party XMPP clients, or XMPP-based API clients, on Cisco Unified Presence.
- Cisco UP XCP Web Connection Manager - Turn on this service if you are integrating XMPP-based API clients on Cisco Unified Presence.

For XMPP clients to function correctly, make sure you turn on the Cisco UP XCP Router on all nodes in your cluster.

Step 4 Click **Save**.

Telephony

Configure CCMCIP profiles for client applications

The CCMCIP service runs on Cisco Unified Communications Manager and retrieves a list of devices associated with each user. CCMCIP profiles are required before the client application can retrieve the list of user devices from Cisco Unified Communications Manager. You can create a profile to control client applications when the application allows a user to use a desk phone for phone calls. The profile can also facilitate discovery of devices when the client applications allow users to use a desk phone for phone calls, or to use a computer for phone calls.

You can then associate selected users with the new profile.

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **CCMCIP Profile**.

Step 2 Select **Add New**.

Step 3 Enter the profile name and description.

Step 4 Enter information into the fields:

Field	Setting
Primary CCMCIP Host	Enter the address of the server for the CCMCIP service to use to retrieve the list of associated devices when users sign in to Cisco Jabber. Enter the address in one of the following forms: • IP address • Host name • Fully-qualified domain name (FQDN) This value must match exactly the IP address, host name, or FQDN of the CCMCIP server.

Field	Setting
Backup CCMCIP Host	Enter the address of the backup server for the CCMCIP service to use if the primary CCMCIP server fails. Enter the address in one of the following forms: • IP address • Host name • FQDN This value must match exactly the IP address, host name, or FQDN of the backup CCMCIP server.
Server Certificate Verification	Specify how the CCMCIP server associated with this profile supports TLS connections. This setting is for TLS verification of the CCMCIP servers listed for this CCMCIP profile. Select from the following options: • Self Signed or Keystore—Cisco Unified Presence accepts the certificate if the certificate is self-signed, or the signing Certificate Authority certificate is in the local trust store. A keystore is a file that stores authentication and encryption keys. • Any Certificate—Cisco Unified Presence accepts all valid certificates. • Keystore Only—Cisco Unified Presence accepts only certificates that are defined in the keystore. You must import the certificate or its Certificate Authority signing certificate into the local trust store. Default Setting: Self Signed or Keystore
Make this the default CCMCIP Profile for the system	(Optional) Check this option if you want new users to be automatically added to the default profile. Users who are already synchronized to Cisco Unified Presence from Cisco Unified Communications Manager are not added to the default profile. However, any users who are synchronized after the default profile is created are added to the default profile.

Step 5 Select **Add Users to Profile**.

Step 6 Use the **Find and List Users** window to find and select users, and select **Add Selected** to add users to the profile.

Step 7 Select **Save**.

Configure CTI gateway profiles

Note You must perform this task in Cisco Unified Presence.

You must create CTI gateway profiles in Cisco Unified Presence Administration and assign primary and backup servers for redundancy.

Before You Begin

- The CTI gateway profile must be created before you can add licensed users of the client application to the application profile.
- The CTI gateway server names and addresses must be specified in **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **CTI Gateway Server** before you can select the servers as primary or backup servers in this procedure.
- Cisco Unified Presence dynamically creates a TCP-based CTI gateway profile based on the hostname of Cisco Unified Communications Manager. Before using this profile, verify that Cisco Unified Presence and the application clients can ping Cisco Unified Communications Manager by the DNS name. If they cannot contact the server, you need to add the IP address of Cisco Unified Communications Manager in **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **CTI Gateway Server**. You do not need to delete the host profiles that are created automatically.
- If you previously configured Cisco Unified Communications Manager with an IP address through the **Cisco Unified Communications Manager Administration** > **System** > **Server** menu, Cisco Unified Presence dynamically creates a TCP-based CTI gateway profile based on that address. The fields in **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **CTI Gateway Profile** are automatically populated, and you need only add users to the default CTI TCP profile that is created (see Step 3).

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **CTI Gateway Profile**.

Step 2 Search for the CTI gateway profile in the **Find and List CTI Gateway Profiles** window.
If the CTI gateway profile is found, no further action is required.

Step 3 If the CTI gateway profile is *not* found, select **Add New**.

Step 4 Enter information into the fields.

Field	Setting
Name	Enter the profile name.
Description	Enter a profile description.
Primary CTI Gateway Server and **Backup CTI Gateway Server**	Select a primary server and backup servers.

Field	Setting
Make this the Default CTI Gateway Profile for the System	Check this option if you want any new users that are added to the system to be placed automatically into this default profile. Users who are already synchronized to Cisco Unified Presence from Cisco Unified Communications Manager are not added to the default profile. However, once the default profile is created, any users synchronized after that are added to the default profile.

Step 5 Select **Add Users to Profile**.

Step 6 Use the **Find and List Users** window to find and select users.

Step 7 Select **Add Selected** to add users to the profile.

Step 8 Select **Save** in the main **CTI Gateway Profile** window.

Desk Phone Control Mode

Configuration of Cisco Unified Presence to enable use of desk phone for calls

If you want Cisco Jabber to be able to control a desk phone, the following must be true:

- The desk phone registers to Cisco Unified Communications Manager.
- The Cisco Unified Communications Manager server has a CTI server.
- Cisco Unified Presence must be configured to enable Cisco Jabber to connect to a CTI server to control the phone.

This section describes how to configure Cisco Unified Presence to enable Cisco Jabber to connect to a CTI server.

Enable control of desk phone from CTI

Note You must perform this task in Cisco Unified Communications Manager.

Procedure

Step 1 Select **Cisco Unified Communications Manager Administration** > **Device** > **Phone**.

Step 2 Search for the desk phone in the **Find and List Phones** window.

Step 3 Select the device name of the desk phone.

Step 4 Check **Allow Control of Device from CTI** to enable CTI to control and monitor this device.

Step 5 Select **Save**.

Using the computer as a phone

Enable control of computer as a phone from CTI

To enable control of the computer as a phone device from the computer telephony interface (CTI) in Cisco Jabber:

Procedure

Step 1 Select **User Management** > **End User** in Cisco Unified Communications Manager Administration.

Step 2 Select the user you want to add.

Step 3 Select **Add to User Group** in the Permissions Information group in the **End User Configuration** window.

Step 4 Search for "Standard CTI" in the **Find and List User Groups** window.

Step 5 Select **Standard CTI Enabled** user group.
If the phone of the user is a Cisco Unified IP Phone 6900, 8900 or 9900 series model, select the **Standard CTI Allow Control of Phones supporting Connected Xfer and conf** user group also.

Step 6 Select **Add Selected**.

Step 7 Select **Save** in the **End User Configuration** window.

Create a Cisco Unified Client Services Framework device for each user

Note You must perform this task in Cisco Unified Communications Manager.

To enable users to use phone features on their computers, you must create a new Cisco Unified Client Services Framework device for each user. This topic describes how to create this device for one user. To create these devices for many users, you can use the Bulk Administration Tool (BAT).

BAT performs bulk updates to the Cisco Unified Communications Manager database. For more information about BAT, see the *Cisco Unified Communications Manager Bulk Administration Guide* at the following URL:

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

Before You Begin

- Read the licensing requirements information, including the information on adjunct licensing.
- Read the guidelines on configuring the device name.
- **Restriction:** The auto-registration features in Cisco Unified Communications Manager are not supported with this application.

Procedure

Step 1 Select **Cisco Unified Communications Manager Administration** > **Device** > **Phone**.

Step 2 Select **Add New**.

Step 3 Select **Cisco Unified Client Services Framework** from the **Phone Type** menu.

Step 4 Select **Next**.

Step 5 Configure the following information:

a) Specify the device name in the **Device Name** field.

b) Enter a descriptive name for the phone in the **Description** field. For example, enter *Richard-phone-on-computer*.

c) Select **Default** from the **Device Pool** list.

d) Select **Standard Client Services Framework** from the **Phone Button Template** list.

e) Configure all the required fields for your environment.

f) If you want to use an adjunct license with this device, select the user ID from the **Owner User ID** list

g) If you want to use an adjunct license with this device, select the device name of the Cisco Unified IP Phone to associate with the client application from the **Primary Phone** list.

h) Enter information in the **Protocol Specific Information** section, as follows:

Field	Description
Presence Group	Select **Standard Presence Group**.
Device Security Profile	Select **Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile**.
SIP Profile	Select **Standard SIP Profile** to specify the default SIP profile. SIP profiles provide specific SIP information for the phone such as registration and keep-alive timers, media ports, and Do Not Disturb control.

Step 6 Select **Save**.

Step 7 Select the **Add a New DN** link in the **Association Information** section that displays on the left side of the window.

Step 8 Configure the following information:

a) Enter the directory number and route partition for Cisco Jabber.

b) Enter the caller ID in **Display (Internal Caller ID)**, in the **Line 1 on Device** ***Device-Name*** section.

c) In the **Multiple Call/Call Waiting** section, specify the maximum number of calls that can be presented to the application in the **Maximum Number of Calls** field.

d) In the **Multiple Call/Call Waiting** section, specify the trigger after which an incoming call receives a busy signal in the **Busy Trigger** field.

Note The **Busy Trigger** setting works with the **Maximum Number of Calls** setting. For example, if the maximum number of calls is set to six and the busy trigger is set to six, the seventh incoming call receives a busy signal.

Step 9 Select **Save**.

Troubleshooting Tips

- Cisco Unified Communications Manager reminds you that changes to line or directory number settings require a restart. However, a restart is required only when you edit lines on Cisco Unified IP Phones that are running at the time of the modifications.
- The directory number that is configured for the Cisco Unified Client Services Framework device and the Cisco Unified IP Phone must be identical. A directory number is configured with a partition, and you assign a directory number to the Cisco Unified Client Services Framework device and the Cisco Unified IP Phone. This configuration causes the Cisco Unified Client Services Framework device to share the line with the Cisco Unified IP Phone for this user.

Naming guidelines for Cisco Unified Client Services Framework devices

To enable users to use phone features on their computers, you must create a new Cisco Unified Client Services Framework device for each user. When you create a Cisco Unified Client Services Framework device, ensure that the device name conforms to these guidelines:

- Can contain uppercase and lowercase letters, and numerals.
- Contains no more than 15 characters.

No correlation to the username is required, but for convenience you might choose to include a username in the device name. For example, you might use the device name *CSFabaker*.

Associate a new device with a user

This procedure contains information on how to associate a new device with an existing user.

Procedure

	Command or Action	Purpose
Step 1	Select **Cisco Unified Communications Manager Administration** > **User Management** > **End User**.	
Step 2	Search for the user in the **Find and List Users** window.	
Step 3	Select the user.	
Step 4	Select **Device Association** in the **Device Information** section.	
Step 5	Search for the device in the **User Device Association** window.	
Step 6	Select the device.	
Step 7	Select **Save Selected/Changes**.	
Step 8	Select **Back to User** from the menu in the **Related Links** navigation box at the top right of the window.	
Step 9	Select **Go**.	
Step 10	Verify that the device is listed in the **Device Information** section on the **End User Configuration** window.	

Associate a line for a phone device with a user

Note You must perform this task in Cisco Unified Communications Manager.

You must ensure that user IDs are the same between LDAP and Cisco Unified Communications Manager. This is easier to accomplish if you have LDAP synchronization enabled in Cisco Unified Communications Manager.

Procedure

Step 1 Select **Cisco Unified Communications Manager Administration** > **Device** > **Phone**.

Step 2 Search for the device for the user in the **Find and List Phones** window.

Step 3 Select the name of the device.

Step 4 Select the directory number for the device in the **Association Information** section that displays on the left side of the window.

Step 5 Select **Associate End Users** at the bottom of the window.

Step 6 Search for the user in the **Find and List Users** window.

Step 7 Select the user, then select **Add Selected**.

Step 8 Select **Save** on the **Directory Number Configuration** window.

Configure the proxy listener and TFTP addresses

You must perform this task in Cisco Unified Presence.

Before You Begin

- Obtain the hostnames or IP addresses of the TFTP servers.

Note Cisco recommends that Cisco Jabber use TCP to communicate with the proxy server. If you use UDP to communicate with the proxy server, availability information for contacts in the Cisco Jabber contact list might not be available for large contact lists.

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **Settings**.

Step 2 Select the Proxy Listener **Default Cisco SIP Proxy TCP Listener**.

Step 3 Assign the primary (required) and backup (optional) TFTP server addresses in the fields provided. You can enter an IP address or an FQDN (Fully Qualified Domain Name).

Step 4 Select **Save**.

Troubleshooting Tips

You can see the TFTP server addresses in the **Server Health** window in Cisco Jabber (**Help** > **Show System Diagnostics**).

Configuration of security for calls

If your organization has a requirement for encrypted voice traffic on the network, the following configuration must be performed:

1. Configure the Cisco Unified Communications Manager server in secure mode.
2. Configure the Certificate Authority Proxy Function (CAPF) server with secure tokens.
3. Create device security profiles.
4. Apply the device security profiles to the Cisco Unified Client Services Framework devices of your users.

The client application can be configured to authenticate to CAPF with a null string, or a string. If a string is used, the user is prompted to enter their authentication string when they connect to Cisco Unified Communications Manager for the first time.

Administrators must distribute the authentication string to the users.

For more information about how to configure security for calls, see the *Cisco Unified Communications Manager Security Guide*:

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

Configure security for a device

Procedure

Step 1 Select **Cisco Unified Communications Manager Administration** > **Device** > **Phone**.

Step 2 Search for the device in the **Find and List Phones** window.

Step 3 Select the name of the device.

Step 4 Select the security profile you require for the device from the **Device Security Profile** drop-down list. Only the phone security profiles that are configured for the phone type and device protocol display.

Step 5 (Optional) If you select **Cisco Unified Client Services Framework- Standard SIP Secure Profile**, do the following:

a) Enter certification and authentication information in the **Certification Authority Proxy Function (CAPF) Information** section.
b) Select **Generate String**.
c) Email the contents of the **Authentication String** field to the user.

Reset a device

Note You must perform this task in Cisco Unified Communications Manager.

Procedure

Step 1 Select **Cisco Unified Communications Manager Administration** > **Device** > **Phone**.
Step 2 Search for the device for the user in the **Find and List Phones** window.
Step 3 Select the name of the device.
Step 4 Select the directory number for the device in the **Association Information** section that displays on the left side of the window.
Step 5 Select **Reset** on the **Directory Number Configuration** window.
Step 6 Select **Confirm Reset** on the **Device Reset** window.

Voicemail

Configure Cisco Unity Connection servers

Cisco Unity Connection provides users with the ability to view, play, sort, and delete voicemail messages from the application interface.

Before You Begin

- Install and configure a supported release of Cisco Unity Connection.
- Integrate Cisco Unified Communications Manager and Cisco Unity Connection. Both servers must be installed and running to configure voicemail ports.

Procedure

Step 1 Set up a new or existing class of service in Cisco Unity Connection Administration to enable Internet Mail Access Protocol (IMAP) client access to voice messages.

a) Expand **Class of Service** in the section on the left-hand side.
b) Select **Class of Service**.
c) Select the display name of the applicable class of service in the search results table, in the **Search Class of Service** window.
d) Check **Allow Users to Use Unified Client to Access Voice Mail**, under **Features**.
e) Check **Allow Users to Access VoiceMail Using an IMAP Client**, under **Licensed Features**. Then select **Allow Users to Access Message Bodies**.
f) Select **Save**.

Step 2 Configure the user:

- If the users are existing Cisco Unity Connection users, add them to the Cisco Unified Communications Manager database. Proceed to Step 4.
- If the user is a new user, add the user to the Cisco Unified Communications Manager database and proceed to Step 3.

Step 3 Create a Cisco Unity Connection user account on the Cisco Unity Connection server with a voice mailbox for each user.

Note The user ID in Cisco Unity Connection does not need to match the user ID in Cisco Unified Presence or in the client application. The client application has an independent voicemail ID, which is set in the application Options dialog box. However, you might find it useful to have the same user IDs across your Cisco Unified Communications system.

Step 4 (Optional) Enable secure messaging as follows:

a) Expand **Class of Service** in the section on the left-hand side.
b) Select **Class of Service**.
c) Select the display name of the applicable class of service in the search results table, in the **Search Class of Service** window.
d) Select the option you require from the **Require Secure Messaging** drop-down list in the **Message Options** section.

Step 5 (Optional) Specify how to handle unidentified caller message security for your users as follows:

a) Expand **Users** in the section on the left-hand side.
b) Select **Users**.
c) Select the alias of a user.
d) Select **Edit** > **Message Settings**.
e) Check **Mark Secure** in the **Unidentified Callers Message Security** section.

Step 6 If one does not already exist, specify a web application password in Cisco Unity Connection for the applicable user accounts.

Troubleshooting Tips

- Users may need to enter their voicemail credentials in the client application if synchronization with Cisco Unified Presence is not enabled.

- If the server can be contacted and the user credentials are correct, but voicemail messages are not downloaded, do the following:
  - Check the configuration of port 7993.
  - Make sure that Cisco Unity Connection is listening on port 7993.
  - Check the firewall configuration. Use Telnet from a remote computer to the computer running Cisco Jabber, and make sure that you can connect to the firewall. Allow the Cisco Unified Client Services Framework executable file (cucsf.exe) to establish IMAP network connections using TCP, TLS, and SSL at the appropriate server and port. For information about the ports and protocols used by the client application and Cisco Unified Client Services Framework, see the release notes:

    http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html

Configure Cisco Unity servers

Cisco Unity receives calls, plays greetings, and records and encodes voicemail. When a voicemail is received, Cisco Unity adds the .wav file to an email and sends it to the configured email account. Cisco Unity creates a subscriber mailbox on the Microsoft Exchange server for use as its mailstore server for message storage.

When Cisco Jabber users want to listen to their voicemails, they use Cisco Jabber to retrieve them from the mailstore server through IMAP.

Cisco Jabber supports both the Cisco Unity unified messaging and the Cisco Unity voice messaging configurations. With unified messaging, the Exchange server email account supports both voicemail and email. With voice messaging, the Exchange server email account contains only voicemail messages.

Before You Begin

- Install and configure a supported release of Cisco Unity.
- Integrate Cisco Unified Communications Manager and Cisco Unity. Both servers must be installed and running to configure voicemail ports.
- If you plan to use SSL to provide secure transmission with the mailstore server, you must set up Cisco Unity to use SSL during the installation or upgrade (or at any time after the installation or upgrade is complete). You must designate a server to act as your certificate authority, submit a certificate request, issue the certificate, and install it on the Cisco Unity server.

Procedure

Step 1 Configure the Microsoft Exchange server to use the IMAP virtual server:

To Configure This Release...	Do This...
Microsoft Exchange 2003	1 Select **Start** > **All Programs** > **Microsoft Exchange** > **System Manager**. 2 In the section on the left-hand side of the System Manager, expand **Servers**. 3 Select the server name. 4 Select **Protocols** > **IMAP**. 5 Right-click, and select **Start Server**.
Microsoft Exchange 2007	1 Select **Start** > **Run**, enter **services.msc**, and select **OK**. 2 Select the Microsoft Exchange IMAP4 service, and select **Start**. This service is not started by default.

Step 2 Configure the port and encryption type:

To Configure This Server...	Do This...
Microsoft Exchange 2003	1 Right-click IMAP Virtual Server, and select **Properties.** 2 Select **Authentication** from the **Access** tab. 3 To use TCP and SSL, verify that **Requires SSL/TLS Encryption** is *not* checked. To use SSL only, verify that **Requires SSL/TLS Encryption** is checked . 4 Select **OK**.
Microsoft Exchange 2007	1 Select **Start** > **Programs** > **Microsoft Exchange Server 2007** > **Exchange Management Shell**. 2 Specify the authentication settings for the Client Access Server that is running the IMAP4 service through the Exchange Power Shell. **Note** Microsoft Exchange 2007 uses SSL by default. 3 Execute one of the following commands for the appropriate setting: • For plain text login: **set-imapsettings -LoginType PlainTextLogin** • For SSL: **set-imapsettings -LoginType SecureLogin**

Step 3 Configure the user:

- If the user is an existing Cisco Unity user, add the user to the Cisco Unified Communications Manager database
- If the user is a new user, add the user to the Cisco Unified Communications Manager database and Cisco Unity.

Step 4 Create mailboxes for new and existing users. For details, see the documentation for your Exchange server.

Step 5 (Optional) Enable secure messaging as follows:

a) Select **Subscribers** > **Features** to make the change on a subscriber template.
The change you make here is not applied to current subscriber accounts that were created by using this template. The setting applies only to subscriber accounts that are created by using this template after the change has been made.

b) Select an option from the **Message Security When Sending a Message** list to enable secure messages. For example, select **Encrypt All Messages**.
This setting specifies whether messages are encrypted when subscribers send messages to other subscribers.

c) Select **Save**.

d) Repeat these steps for additional subscribers or subscriber templates, as applicable.

Step 6 (Optional) Enable secure messaging for messages from unidentified callers:

a) Select **System** > **Configuration** > **Message Security Settings**.

b) Specify whether messages from unidentified callers are encrypted. Select an option from the list.

c) Select **Save**.

Troubleshooting Tip

Cisco Jabber users must enter their Cisco Unity credentials in the Cisco Jabber **Options** dialog box.

Configure voicemail server names and addresses on Cisco Unified Presence

Note You must perform this task in Cisco Unified Presence.

You must configure voicemail settings so that the Cisco Jabber can interact with the voice message web service (VMWS) on Cisco Unity or Cisco Unity Connection. The VMWS service enables Cisco Jabber to move deleted voicemail messages to the correct location. This service also provides message encryption capabilities to support secure messaging.

Before You Begin

- Configure a supported voicemail server.
- Obtain the hostname or IP address of the voicemail server. You might need to specify more than one hostname to provide services for the number of users in your environment.
- For Cisco Unity, you must also obtain the hostnames or IP addresses of the peer Microsoft Exchange server or servers.
- Perform this procedure for each voicemail server in your environment.

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **Voicemail Server**.

Step 2 Select **Add New**.

Step 3 Select **Unity** or **Unity Connection** from the **Server Type** menu.

Step 4 Enter the Cisco Unity Connection or Cisco Unity server name.

Step 5 Enter the hostname or the IP address of the voicemail server.

Step 6 Enter 443 for the **Web Service Port** value.

Step 7 Select HTTPS in **Web Service Protocol** menu.

Step 8 Select **Save**.

Configure mailstore server names and addresses on Cisco Unified Presence

Note You must perform this task in Cisco Unified Presence.

You must configure Cisco Unified Presence with mailstore information so that Cisco Jabber can connect to the mailstore. Cisco Jabber uses IMAP to download messages.

Cisco Unity creates subscriber mailboxes for message storage on the Microsoft Exchange server. Cisco Unity Connection usually provides a mailstore, and hosts the mailstore on the same server.

The following table describes the protocols you can use for voicemail messages, and the security features the protocols implement for voicemail messages:

Protocol	Description
SSL	Uses a secure socket to encrypt usernames, passwords, and voicemail messages.
TCP	Sends usernames, passwords, and voicemail messages in clear text.
TLS	Uses the STARTTLS verb of IMAP to encrypt usernames, passwords, and voicemail messages.

Before You Begin

- Obtain the hostname or IP address of the mailstore server.
- If you upgrade from Cisco Unified Presence Release 6.0(x) to Release 7.0(x), Cisco Unified Presence automatically imports the IMAP settings into the mailstore configuration window.
- Restriction: You must provision mailstore servers before you can add the servers to the voicemail profiles.

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **Mailstore**.

Step 2 Select **Add New**.

Step 3 Enter the mailstore server name.

Step 4 Enter the hostname or the IP address of the mailstore server.

Step 5 Specify the IMAP port number configured for the server and the corresponding protocol to use when Cisco Jabber contacts this server:

Server	Protocols and Port Numbers
Cisco Unity Connection	SSL, 993 TCP, 143 TLS, 143, or 7993
Cisco Unity	SSL, 993 TCP, 143 TLS, 143

Step 6 Select **Save**.

Create voicemail profiles on Cisco Unified Presence

Note You must perform this task in Cisco Unified Presence.

You must create voicemail profiles before you can add Cisco Jabber licensed users to profiles.

Repeat this procedure for each voicemail profile you want to create.

Before You Begin

- Specify voicemail server names and addresses.
- Specify mailstore server names and addresses.

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **Voicemail Profile**.

Step 2 Select **Add New**.

Step 3 Enter the profile name and description.

Step 4 Enter information into the fields:

Field	Description
Voice Messaging Pilot	The voicemail pilot number is the directory number that a user dials to access their voice messages. Each pilot number can belong to a different voice-messaging system. Select one of the following options: • ***Number***—Select the voicemail pilot number for the system. This is the same as the number specified from the **Voice Mail** > **Voice Mail Pilot** menu, in Cisco Unified Communications Manager Administration. • **No Voice Mail**—Select this option if you do not want to send unanswered incoming calls to voicemail.
Primary Voicemail Server	Select a primary server. Select one of the voicemail servers you specified.
Backup Voicemail Server	Enter the name of your backup voicemail server. If you do not want a backup voicemail server, select **None**.
Primary Mailstore	Select the primary mailstore server. Select one of the mailstore servers you specified.
Backup Mailstore	Enter the name of your backup mailstore server. If you do not want a backup voicemail server, select **None**.
Make this the default Voicemail Profile for the system	Check this option if you want new users to be automatically added to the default profile. Users who are already synchronized to Cisco Unified Presence from Cisco Unified Communications Manager are not added to the default profile. However, any users who are synchronized after the default profile is created are added to the default profile.

Step 5 Enter information into the fields:

Field	Description
Inbox Folder	Enter the name of the folder on the mailstore server in which to store new messages. Only change this value if the mailstore server uses a different folder name from the default folder. Default Folder: INBOX

Field	Description
Trash Folder	Enter the name of the folder on the mailstore server in which to store deleted messages. Only change this value if the mailstore server uses a different folder name from the default folder. Default Folder: Deleted Items
Polling Interval	Enter the time (in seconds) that can elapse between polls of the IMAP server for new voice messages, when IDLE is not supported by the mailstore or when a connection failure occurs. Default Value: 60 Permitted Values: 60-900
Allow dual folder mode	This dual folder setting is turned on by default for use with mailstores that support the IMAP UIDPLUS extensions (RFC 2359 and 4315). By default, the Client Services Framework (CSF) will detect if UIDPLUS is not supported and automatically revert to Single Folder mode. Turn off this setting if you know that UIDPLUS is not supported and you want to force the system to use Single Folder mode. Default Setting: On **Tip** The Microsoft Exchange 2007 server does not support UIDPLUS extensions.

Step 6 Select **Add Users to Profile**.

Step 7 Use the **Find and List Users** window to find and select users, and select **Add Selected** to add users to the profile.

Step 8 Select **Save**.

About Secure Voicemail Messaging

Secure voicemail messaging on Cisco Unity Connection

In Cisco Unity Connection, when a user sends a message, class-of-service settings determine the security level of the message. When a user marks a message as private, Cisco Unity Connection automatically marks the message as secure.

Cisco Unity Connection provides audio for secure voicemail messages through a special IMAP port, port 7993. This port requires Transport Layer Security (TLS). Cisco Jabber uses this port to access, download, and play the secure message.

For information on installing and configuring secure message features on Cisco Unity Connection, see the Cisco Unity Connection documentation.

Secure voicemail messaging on Cisco Unity

Cisco Unity uses public key cryptography to send secure messages. Each Cisco Unity server in the network has a public key and a private key. The public key for each server is stored in the Cisco Unity database and is shared through Active Directory with other Cisco Unity servers in the network.

The Cisco Unity server generates new session keys daily. The server uses the session key to encrypt the voice mail, and to control the age of messages. Users cannot play messages that are encrypted with keys that are older than the age policy allows.

Cisco Unity uses Microsoft Exchange to store secure messages. You configure all subscriber mailboxes on these message store servers. Cisco Jabber connects to the message store and performs the following actions:

1. Uses IMAP to download the message from Exchange.
2. Determines if the message is encrypted.
3. If the message is not encrypted, Cisco Jabber plays the message.
4. If the message is encrypted, the following happens:
   a. Cisco Jabber extracts the encrypted session keys from the .wav file for the message.
   b. Cisco Jabber submits the keys to the Cisco Unity server.
   c. The Cisco Unity server tries to decrypt the session keys. The server uses the private key certificates in the Cisco Unity database.
   d. If the Cisco Unity server decrypts the session key, Cisco Jabber uses the key to decrypt the message, and plays the messages to the user.

Secure voicemail on Cisco Unified Presence

The required configuration is different, depending on what type of secure messaging you want to configure:

Secure Messaging Type	Action	Menu Path
SOAP	Make sure that the web service port and protocol are configured. You configure the web service port and protocol when you specify the voicemail server name and address.	**Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **Voicemail Server**
IMAP	Make sure that the IMAP port and protocol are configured. You configure the IMAP port and protocol when you specify the mailstore server name and address.	**Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **Mailstore**

Note Cisco Unity requires SOAP configuration for secure messaging. Cisco Unity Connection does not require SOAP configuration for secure messaging.

Meetings

Configure the Cisco Unified MeetingPlace web server

To configure the Cisco Unified MeetingPlace Web Server for integration with Cisco Jabber:

Procedure

Step 1 If required, enable a secure connection between Cisco Jabber and the Cisco Unified MeetingPlace Application Server.
You must obtain and upload the required certificates from a trusted certificate authority (CA).

Step 2 Create a user profile on the Cisco Unified MeetingPlace Application Server for each Cisco Jabber user who wants to use the web conferencing feature.

Step 3 Configure a conferencing server entry on Cisco Unified Presence. Use the IP address of the Cisco Unified MeetingPlace Web Server as the conferencing server.

Step 4 Use the conferencing server to create a conferencing profile. Check **Make this the default Conferencing Profile for the system** for the conferencing profile.

Step 5 Create a conferencing profile on Cisco Unified Presence, and assign the Cisco Jabber web conferencing users to the conferencing profile.

Distribute the Cisco Jabber for Mac client

Visit the Cisco Software Center to download the Cisco Jabber for Mac client.

Upgrading in the Mac OS X environment is performed automatically by the application, with permission from the user.

Important notice about emergency calls

Using your computer as a phone may not provide the most timely or accurate location data for an emergency call. Calls may be misdirected to the wrong emergency response center or the emergency response center may make errors when determining your location. **Use your computer as a phone only as a last resort during an emergency.** Cisco will not be liable for resulting errors or delays.