



CHAPTER 3

Configuring Recommended Servers for Cisco Unified Personal Communicator

December 2008

- [How to Configure Voice-Mail Servers, page 3-1](#)
- [How to Configure Conferencing Servers, page 3-12](#)
- [Configuring Videoconferencing Resources, page 3-19](#)



Note

Make sure you first complete the tasks in [Chapter 2, “Configuring Required Servers for Cisco Unified Personal Communicator.”](#) After you complete the tasks in this chapter, Cisco Unified Personal Communicator has full feature support for voice mail, web conferencing, and videoconferencing.

How to Configure Voice-Mail Servers

- [Configuring Cisco Unity Connection Servers, page 3-2](#)
- [Configuring Cisco Unity Servers, page 3-4](#)
- [Specifying Voice-Mail Server Names and Addresses in Cisco Unified Presence Administration, page 3-6](#)
- [Configuring Secure Messaging in Cisco Unified Presence Administration, page 3-7](#)
- [Specifying Mailstore Server Names and Addresses in Cisco Unified Presence Administration, page 3-9](#)
- [Creating Voice-Mail Profiles in Cisco Unified Presence Administration, page 3-11](#)

Configuring Cisco Unity Connection Servers

Cisco Unity Connection provides Cisco Unified Personal Communicator users with the ability to view, play, sort, and delete voice-mail messages from within the Cisco Unified Personal Communicator application.

Before You Begin

- Install and configure Cisco Unified Communications Manager. For details, see the installation and upgrade guides, and maintain and operate guides at the following URL:
http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html
- Install and configure a supported release of Cisco Unity Connection.
 - For details about the server installation:
http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html
 - For details about supported Cisco Unity Connection releases, see the Cisco Unified Personal Communicator release notes:
http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html
- Integrate Cisco Unified Communications Manager and Cisco Unity Connection. Both servers must be installed and running to configure voice-mail ports. For details about the voice-mail configuration, see the *Cisco Unified Communications Manager Administration Guide*:
http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

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 left pane.
 - b. Click **Class of Service**.
 - c. Click 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** for port 7993 and TLS, under Features.
 - e. For all other ports and protocols, perform the following steps:
 - Check **Allow Users to Access VoiceMail Using an IMAP Client** under Licensed Features.
 - Select **Allow Users to Access Message Bodies**.
 - Check **Allow Users to Use Unified Client to Access Voice Mail** under Features.
 - f. Click **Save**.
- Step 2** Configure the user:
- If the users are existing Cisco Unity Connection users, add them to the Cisco Unified Communications Manager database and to Cisco Unified Presence. Proceed to Step 4.
 - If the user is a new Cisco Unified Personal Communicator user, add the user to Cisco Unified Communications Manager database, Cisco Unity Connection, and to Cisco Unified Presence.

See the administration guides for Cisco Unified Communications Manager and Cisco Unified Presence at the following URLs:

- http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
- http://www.cisco.com/en/US/products/ps6837/prod_maintenance_guides_list.html

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

The user ID in Cisco Unity Connection does *not* need to match the user ID in Cisco Unified Presence or in Cisco Unified Personal Communicator. Cisco Unified Personal Communicator has an independent voicemail ID, which is set in the application Preference window.

For details about setting up the account, see the *Cisco Unity Connection User Moves, Adds, and Changes Guide*:

http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html

Step 4 (Optional) Enable secure messaging as follows:

- a. Expand **Class of Service** in the left pane, and then click **Class of Service**.
- b. Select an option from Require Secure Messaging in the Message Options section to enable secure messages.

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

- a. Expand **Users** in the left pane.
- b. Click **Users**.
- c. Click the alias of a user.
- d. Select **Edit > Message Settings**.
- e. Check **Mark Secure** in Unidentified Callers Message Security.

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

For details, see the *Cisco Unity Connection User Moves, Adds, and Changes Guide*:

http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html

Step 7 Perform the voice-mail configuration in Cisco Unified Presence Administration.

Troubleshooting Tips

- Cisco Unified Personal Communicator users must enter their Cisco Unity Connection credentials, that is, their username and web application password, in the Cisco Unified Personal Communicator Preferences window.
- If the server can be contacted and the user credentials are correct, but voice-mail messages are not downloaded, do the following:
 - Check the configuration of port 7993.
 - Make sure Cisco Unified Personal Communicator is listening on port 7993.
 - Check the firewall configuration. Use Telnet from a remote computer to the computer running Cisco Unified Personal Communicator, and make sure you can connect.

For details, see the Cisco Unified Personal Communicator troubleshooting guide at the following URL:

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

Related Topics

- [Specifying Voice-Mail Server Names and Addresses in Cisco Unified Presence Administration, page 3-6](#)
- [Configuring Secure Messaging in Cisco Unified Presence Administration, page 3-7](#)
- [Creating Voice-Mail Profiles in Cisco Unified Presence Administration, page 3-11](#)

Configuring Cisco Unity Servers

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

When Cisco Unified Personal Communicator users want to listen to their voice mails, they use Cisco Unified Personal Communicator to retrieve them from the mailstore server through IMAP.

Cisco Unified Personal Communicator supports both the Cisco Unity unified messaging and the Cisco Unity voice messaging configurations. With unified messaging, the Exchange server e-mail account supports both voice mail and e-mail. With voice messaging, the Exchange server e-mail account contains only voice-mail messages.

Before You Begin

- Install and configure Cisco Unified Communications Manager. For details, see the installation and upgrade guides, and maintain and operate guides at the following URL:
http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html
- Install and configure a supported release of Cisco Unity.
 - For details about the server installation with Microsoft Exchange, see the following URL:
http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html
 - For details about supported Cisco Unity releases, see the Cisco Unified Personal Communicator release notes at the following URL:
http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html
- Integrate Cisco Unified Communications Manager and Cisco Unity. Both servers must be installed and running to configure voice-mail ports. For details about the voice-mail configuration, see the *Cisco Unified Communications Manager Administration Guide* at the following URL:
http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
- 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. For details, see the security guide:
http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html

Procedure

-
- Step 1** Configure the Microsoft Exchange server to use the IMAP virtual server.

For Exchange 2003, perform the following steps:

- a. Select **Start > All Programs > Microsoft Exchange > System Manager**.
- b. In the left pane of the System Manager, expand **Servers**.
- c. Select the server name.
- d. Select **Protocols > IMAP**.
- e. Right-click, and select **Start Server**.

For Exchange 2007, perform the following steps:

- a. Select **Start > Run**, enter **services.msc**, and click **OK**.
- b. Select the Microsoft Exchange IMAP4 service, and click **Start**. This service is not started by default.

Step 2 Configure the port and encryption type.**For Exchange 2003, perform the following steps:**

- a. Right-click IMAP Virtual Server, and select **Properties**.
- b. Click **Authentication** from the Access tab.
 - Verify that **Requires SSL/TLS Encryption** is not checked to use TCP and SSL connection.
 - Verify that **Requires SSL/TLS Encryption** is checked to use SSL only.
- c. Click **OK**.

For Exchange 2007, perform the following steps:

- a. Specify the authentication settings for the Client Access Server that is running the IMAP4 service through the Exchange Power Shell.
Select **Start > Programs > Microsoft Exchange Server 2007 > Exchange Management Shell**.
Exchange 2007 uses SSL by default.
- b. 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 and to Cisco Unified Presence.
- If the user is a new user, add the user to the Cisco Unified Communications Manager database, Cisco Unity (which adds the user to Exchange and to Active Directory), and to Cisco Unified Presence.

See the administration guides for Cisco Unified Communications Manager and Cisco Unified Presence at the following URLs:

- http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
- http://www.cisco.com/en/US/products/ps6837/prod_maintenance_guides_list.html

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 > Subscribers > Features** to make the change on a subscriber template.

The change you make here is not applied to currently existing 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. Click **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. Click **Save**.

Step 7 Perform the voice-mail and mailstore configuration in Cisco Unified Presence Administration.

Troubleshooting Tip

Cisco Unified Personal Communicator users must enter their Cisco Unity credentials in the Cisco Unified Personal Communicator Preferences window.

Related Topics

- [Specifying Voice-Mail Server Names and Addresses in Cisco Unified Presence Administration, page 3-6](#)
- [Configuring Secure Messaging in Cisco Unified Presence Administration, page 3-7](#)
- [Specifying Mailstore Server Names and Addresses in Cisco Unified Presence Administration, page 3-9](#)
- [Creating Voice-Mail Profiles in Cisco Unified Presence Administration, page 3-11](#)

Specifying Voice-Mail Server Names and Addresses in Cisco Unified Presence Administration

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

Before You Begin

- Make sure that you configure a supported server as described in the following sections:
 - [Configuring Cisco Unity Connection Servers, page 3-2](#)
 - [Configuring Cisco Unity Servers, page 3-4](#)
- For Cisco Unity Connection, obtain the hostname or IP address of the voice-mail server. You might need to specify more than one hostname to provide services for the number of users in your environment.

- For Cisco Unity, obtain the hostname or IP address of the Cisco Unity server. You might need to specify more than one hostname to provide services for the number of users in your environment.
- For Cisco Unity, obtain the hostnames or IP addresses of the peer Microsoft Exchange server or servers.

Procedure

- Step 1** Select the following menu in Cisco Unified Presence Administration:
 Release 7.0: **Application > Cisco Unified Personal Communicator > Voicemail Server**
 Release 6.x: **Application > Cisco Unified Personal Communicator > Unity Server**
- Step 2** Click **Add New** in the Find and List window to add a new server.
- Step 3** Enter information into the fields, as shown in the following table:

Field	Setting
Release 7.0 Only	
Server Type	Select Unity or Unity Connection .
Name	Enter the Cisco Unity Connection or Cisco Unity server name.
Hostname/IP Address	Enter the hostname or the IP address of the server.
Web Service Port, Web Service Protocol	Enter 443 in Web Service Port. Select HTTPS in Web Service Protocol.
Release 6.x Only	
Name	Enter the Cisco Unity Connection or Microsoft Exchange server name.
Hostname/IP Address	Enter the IP address of the Exchange server.

- Step 4** Click **Save**.
- Step 5** Click **Add New**, and repeat this procedure for each voice-mail server in your environment.

Related Topics

- [Configuring Secure Messaging in Cisco Unified Presence Administration, page 3-7](#)
- [Specifying Mailstore Server Names and Addresses in Cisco Unified Presence Administration, page 3-9](#)
- [Creating Voice-Mail Profiles in Cisco Unified Presence Administration, page 3-11](#)

Configuring Secure Messaging in Cisco Unified Presence Administration

To enable users to retrieve and play secure voice-mail messages from Cisco Unified Personal Communicator, you must do the following:

- Configure secure messaging in Cisco Unified Presence Administration Release 7.0
- Configure Cisco Unity to encrypt messages

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 voice-mail messages through a special IMAP port, port 7993. This port requires Transport Layer Security (TLS). Cisco Unified Personal Communicator uses this port to access, download, and play the secure message.

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 Unified Personal Communicator 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 Unified Personal Communicator plays the message.
4. If the message is encrypted, the following happens:
 - a. Cisco Unified Personal Communicator extracts the encrypted session keys from the .wav file for the message.
 - b. Cisco Unified Personal Communicator 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 Unified Personal Communicator uses the key to decrypt the message, and plays the messages to the user.
 - e. If the Cisco Unity server cannot decrypt the session key, Cisco Unified Personal Communicator plays a decoy message to the user.

Before You Begin

Install and configure secure message features on the voice-mail servers, as follows:

- For Cisco Unity Connection, see the information in this guide on how to configure Cisco Unity Connection servers. See also the product online help, the system administration guide, and the user moves, adds, and changes guide at the following URL:
http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html
- For Cisco Unity, see the information in this guide on how to configure Cisco Unity servers. See also the product online help or the security guide for Cisco Unity with Microsoft Exchange at the following URL:
http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html

Restrictions

Secure message features are not available in releases of Cisco Unified Presence Administration earlier than Release 7.0.

Procedure

- Step 1** Select **Application > Cisco Unified Personal Communicator > Voicemail Server**.
- Step 2** Find and select your server.
- Step 3** Perform one of the following actions, depending on what type of secure messaging you want to configure:

Secure Messaging Type	Action
SOAP	Make sure that the web service port and protocol are configured. You configure the web service port and protocol when you specify the voice-mail server name and address.
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.

Related Topics

- [Configuring Cisco Unity Connection Servers, page 3-2](#)
- [Configuring Cisco Unity Servers, page 3-4](#)
- [Specifying Voice-Mail Server Names and Addresses in Cisco Unified Presence Administration, page 3-6](#)
- [Specifying Mailstore Server Names and Addresses in Cisco Unified Presence Administration, page 3-9](#)
- [Creating Voice-Mail Profiles in Cisco Unified Presence Administration, page 3-11](#)

Specifying Mailstore Server Names and Addresses in Cisco Unified Presence Administration

You must configure Cisco Unified Presence Release 7.0 with mailstore information so that Cisco Unified Personal Communicator can connect to the mailstore. Cisco Unified Personal Communicator 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.

Before You Begin

- Obtain the hostname or IP address of the mailstore server.
- If you upgrade from Release 6.x to Release 7.0, Cisco Unified Presence automatically imports the IMAP settings into the Mailstore Configuration page. In Release 6.x, these settings are on the **Application > Cisco Unified Personal Communicator > Unity Server** page.

Restrictions

- You must provision mailstore servers before you can add the servers to the voice-mail profiles.

Procedure

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

Step 2 Click **Add New** to add a new server.

Step 3 Enter information into the fields, as follows.

Field	Setting
Name	Enter the server name.
Description	(Optional) Enter a server description.
Hostname/IP Address	Enter the hostname or the IP address of the mailstore server.
Port, Protocol Type	Specify the IMAP port number configured for the server and the corresponding protocol to use when Cisco Unified Personal Communicator contacts this server. Cisco Unity Connection: <ul style="list-style-type: none"> SSL = 993 TCP = 143 TLS = 143 or 7993 Cisco Unity with Exchange: <ul style="list-style-type: none"> SSL = 993 TCP = 143 TLS = 143

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

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

Step 4 Click **Save**.

Related Topics

- [Creating Voice-Mail Profiles in Cisco Unified Presence Administration, page 3-11](#)

Creating Voice-Mail Profiles in Cisco Unified Presence Administration

Before You Begin

- You must create voice-mail profiles before you can add Cisco Unified Personal Communicator licensed users to profiles.
- Specify voice-mail server names and addresses.
- Specify mailstore server names and addresses.

Restrictions

Voice-mail server failover and mailstore server failover are not supported in Cisco Unified Personal Communicator Release 7.0(1). Do not specify backup servers in the Voicemail Profile in Cisco Unified Presence Administration.

Procedure

- Step 1** Select the following menu in Cisco Unified Presence Administration:
Release 7.0: **Application > Cisco Unified Personal Communicator > Voicemail Profile**
Release 6.x: **Application > Cisco Unified Personal Communicator > Unity Profile**
- Step 2** Click **Add New** in the Find and List window.
- Step 3** Enter information into the fields, as follows.



Note

The fields in the window might be in a different order than listed in the table depending on the release Cisco Unified Presence.

Field	Setting
Name	Enter the profile name.
Description	(Optional) Enter a profile description.
Voice Messaging Pilot	(Optional) The voice-mail pilot number is the directory number that a user dials to access their voice messages. Cisco Unified Communications Manager automatically dials the voice-messaging number when a user presses the Messages button on their phone. Each pilot number can belong to a different voice-messaging system. Select one of the following options: <ul style="list-style-type: none"> • <i>Number</i>—Select the voice-mail 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 voice mail.
Primary Voicemail Server	Select a primary server. Select one of the mailstore servers you specified. In Release 6.x, this field is called Primary Unity Server.
Backup Voicemail Server	(Optional) Enter the name of your backup voicemail server. If you do not want a backup voicemail server, select None . In Release 6.x, this field is called Backup Unity Server.

Field	Setting
Add Users to Profile	Click this button, then use the Find and List Users window to find and select users. Click Add Selected to add users to the profile.
Release 7.0 Only	
Primary Mailstore	Select the primary mailstore server. Select one of the mailstore servers you specified.
Backup Mailstore	(Optional) 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	(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 4 Click **Save**.

Step 5 Click **Add New**, and repeat this procedure for each voice-mail profile you want to create.

Related Topics

- [How to Change Application Profiles, page 2-31](#)
- [Specifying Voice-Mail Server Names and Addresses in Cisco Unified Presence Administration, page 3-6](#)
- [Specifying Mailstore Server Names and Addresses in Cisco Unified Presence Administration, page 3-9.](#)
- [Changing Application Profiles for a Single User, page 2-32](#)

How to Configure Conferencing Servers

- [Configuring Cisco Unified MeetingPlace Express and Cisco Unified MeetingPlace Express VT Servers, page 3-12](#)
- [Configuring Cisco Unified MeetingPlace Servers, page 3-15](#)
- [Specifying Conferencing Server Names and Addresses in Cisco Unified Presence Administration, page 3-17\)](#)
- [Creating Conferencing Profiles in Cisco Unified Presence Administration, page 3-18](#)

Configuring Cisco Unified MeetingPlace Express and Cisco Unified MeetingPlace Express VT Servers

Cisco Unified MeetingPlace Express or Cisco Unified MeetingPlace ExpressVT provide Cisco Unified Personal Communicator users with the ability to escalate to web meetings from within an existing audio or video communication session. With Cisco Unified MeetingPlace Express VT, users can move from point-to-point to multiparty voice and video calls.

Before You Begin

- Install a supported release of the web conferencing server (Cisco Unified MeetingPlace Express or Cisco Unified MeetingPlace Express VT). For details about the server installation:
http://www.cisco.com/en/US/products/ps6533/prod_installation_guides_list.html
For details about supported Cisco Unified MeetingPlace Express releases, see the release notes:
http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html
- Integrate the web conferencing server with Cisco Unified Communications Manager. Configure call control features:
http://www.cisco.com/en/US/products/ps6533/products_installation_and_configuration_guides_list.html
- Determine the number of Cisco Unified MeetingPlace Express (or Cisco Unified MeetingPlace Express VT) user licenses that are needed to provide enough web ports for meetings initiated through Cisco Unified Personal Communicator.

Procedure

Step 1 Integrate the web conference server with Cisco Unified Personal Communicator:

For Cisco Unified MeetingPlace Express VT ad hoc conferencing functionality:

- a. Install the following licenses through the Cisco Unified MeetingPlace Express Administration Center:
 - adhocsystemsoftware
 - webconf
 - maxadhoc

This provides enough web ports for Cisco Unified Personal Communicator users. Cisco Unified Personal Communicator requires support for more than six voice, six video, and six web ports.

- b. Configure Cisco Unified MeetingPlace Express VT for ad hoc conferencing by following the instructions in the configuration and maintenance guide:
http://www.cisco.com/en/US/products/ps6533/prod_maintenance_guides_list.html

For Cisco Unified MeetingPlace Express reservationless functionality:

- a. Install the following licenses:
 - systemsoftware
 - webconf
 - maxweb

This provides enough web ports for both the full web meetings that are initiated from Cisco Unified MeetingPlace Express, and the web meetings that are initiated from Cisco Unified Personal Communicator.

- b. For Cisco Unified MeetingPlace Express-specific information about integrating with Cisco Unified Personal Communicator, managing certificates, creating user profiles, and configuring call-control, see the configuration and maintenance guide:
http://www.cisco.com/en/US/products/ps6533/prod_maintenance_guides_list.html

- Step 2** If not already enabled, enable the Secure Sockets Layer (SSL) encryption technology on the web conference server by obtaining and uploading the required certificates from a trusted certificate authority (CA).

The certificate is required for secure communications between Cisco Unified Personal Communicator and the web conference server. Without SSL, clear text passwords are sent from Cisco Unified Personal Communicator to the web conferencing server and from the log-in browser to the web conferencing server.

- Step 3** Set up a user profile on the web conference server for each Cisco Unified Personal Communicator user who might initiate web meetings from a Cisco Unified Personal Communicator conversation.
- You do not need to create a user profile for Cisco Unified Personal Communicator users who attend web meetings. They join the web meeting as guests, and a password is not needed.
 - Make sure to set the **Method of Attending** to **I'll Call In** for users who might initiate web meetings; otherwise, the web conference system will try to contact the user who clicked the **Escalate to Web Conference** button in Cisco Unified Personal Communicator. Make sure to ask users not to change this setting.

**Tip**

As an alternative, you can configure the Administrative XML Layer Simple Object Access Protocol (AXL SOAP) authentication on Cisco Unified Communications Manager to simplify the web conference user profile administration. With this configuration, the Cisco Unified Personal Communicator meeting initiator needs a Cisco Unified Communications Manager profile instead of a web conference user profile. With AXL authentication, when the initiator requests a meeting for the first time through Cisco Unified Personal Communicator, a web conference profile is automatically created for the initiator.

- Step 4** Assist users with the Presenter Add-In installation so that desktops, documents, or computer applications can be shared. For details:

http://www.cisco.com/en/US/products/ps6533/products_user_guide_list.html

- Step 5** Change the network configuration so that inbound calls from the public switched telephone network (PSTN) to Cisco Unified Personal Communicator support RFC2833.

- For inbound calls, Cisco Unified Personal Communicator requires RFC2833 support if these calls require dual tone multifrequency (DTMF) digit collection. Inbound calls to the client will not be answered with key press markup language (KPML) support.

A typical inbound call scenario is when the web conference server calls the user as a conference is being set up. In this situation, if the inbound call from the PSTN supports RFC2833, the Cisco Unified Personal Communicator user can join the meeting by using the session dial pad.

- For outbound calls, Cisco Unified Personal Communicator supports both KPML and RFC2833 digit collection.

- Step 6** Perform the Cisco Unified MeetingPlace Express server-specific configuration in Cisco Unified Presence Administration.

For details about supported and unsupported Cisco Unified MeetingPlace Express meeting controls, see the release notes:

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

For a description of the characteristics of a web conference that you add to a Cisco Unified Personal Communicator conversation, see the user guide for Cisco Unified Personal Communicator:

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

Troubleshooting Tips

Cisco Unified Personal Communicator users must enter their Cisco Unified MeetingPlace Express credentials in the Cisco Unified Personal Communicator Preferences window.

Related Topics

- [Specifying Conferencing Server Names and Addresses in Cisco Unified Presence Administration, page 3-17](#)
- [Creating Conferencing Profiles in Cisco Unified Presence Administration, page 3-18](#)

Configuring Cisco Unified MeetingPlace Servers

Cisco Unified MeetingPlace provides a more extensive feature set (such as scheduled and reservationless rich-media conferencing) and allows more concurrent users than Cisco Unified MeetingPlace Express or Cisco Unified MeetingPlace Express VT. With Cisco Unified MeetingPlace, a Cisco Unified Personal Communicator user can escalate to a web conferencing session or to a video conferencing session from within an existing audio session.

Before You Begin

- Install a supported release of the web conferencing server. For details about the server installation:
http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html

For details about supported Cisco Unified MeetingPlace releases, see the Cisco Unified Personal Communicator release notes:

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

- Integrate the web conferencing server with Cisco Unified Communications Manager. Configure call control features:

Release 7.0:

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_installation_and_configuration_guides_list.html

Release 6.x:

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_implementation_design_guides_list.html

- Determine the number of web and audio conferencing user licenses that provide enough web ports for meetings initiated through Cisco Unified MeetingPlace and through Cisco Unified Personal Communicator:

Release 7.0:

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html

Release 6.x:

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_implementation_design_guides_list.html

Procedure

Step 1 Install web and audio conferencing user licenses.

Step 2 If not already enabled, enable the Secure Sockets Layer (SSL) encryption technology on the web conference server. You must obtain and upload the required certificates from a trusted certificate authority (CA).

The certificate is required for secure communications between Cisco Unified Personal Communicator and the web conference server. Without SSL, clear text passwords are sent from Cisco Unified Personal Communicator to the web conferencing server and from the log-in browser to the web conferencing server.

For details about setting up SSL, see the web conferencing configuration guide (Release 6.x) or the configuration guide (Release 7.0):

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_installation_and_configuration_guides_list.html

Step 3 Set up a user authentication method on the web conference server.

The following authentication methods are supported for use with Cisco Unified Personal Communicator:

- MeetingPlace
- HTTP Basic Authentication (Domain)
- LDAP
- LDAP, then MeetingPlace

For details about configuring the authentication methods, see the web conferencing configuration guide (Release 6.x) or the configuration guide (Release 7.0):

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_installation_and_configuration_guides_list.html

Step 4 Set up a user profile on the Cisco Unified MeetingPlace server for each Cisco Unified Personal Communicator user who might initiate web meetings from a Cisco Unified Personal Communicator conversation.

Step 5 Perform the conferencing server configuration in Cisco Unified Presence Administration.

Troubleshooting Tips

- Cisco Unified Personal Communicator users must enter their Cisco Unified MeetingPlace credentials in the Cisco Unified Personal Communicator Preferences window. Make sure you provide the password that is consistent with the configured authentication method. For example, if you configured MeetingPlace as the authentication method, provide the user with the MeetingPlace password. If you configured LDAP as the authentication method, provide the user with the LDAP password.
- You do not need to create Cisco Unified MeetingPlace user profiles for all Cisco Unified Personal Communicator users. Cisco Unified Personal Communicator users who do not have Cisco Unified MeetingPlace profiles can attend web conferences initiated by other Cisco Unified Personal Communicator users as guests, and passwords are not needed. However, some authentication methods, for example, HTTP Basic Authentication, do not allow Cisco Unified Personal Communicator users to log in to Cisco Unified MeetingPlace as guests.

For details about the authentication methods, see the web conferencing configuration guide (Release 6.x) or the configuration guide (Release 7.0):

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_installation_and_configuration_guides_list.html

- If you configure multiple web servers with different authentication methods and mismatched credentials, users might have problems when they try to log in to web conferences.

Related Topics

- [Specifying Conferencing Server Names and Addresses in Cisco Unified Presence Administration, page 3-17](#)
- [Creating Conferencing Profiles in Cisco Unified Presence Administration, page 3-18](#)

Specifying Conferencing Server Names and Addresses in Cisco Unified Presence Administration

You must specify conferencing server names, addresses, ports, and protocol types in Cisco Unified Presence Administration so that Cisco Unified Personal Communicator can interact with them.

Before You Begin

- Make sure you configure a supported conferencing server as described in these sections:
 - [Configuring Cisco Unified MeetingPlace Express and Cisco Unified MeetingPlace Express VT Servers, page 3-12.](#)
 - [Configuring Cisco Unified MeetingPlace Servers, page 3-15](#)
- Obtain the hostname or IP address of the conferencing server.

Procedure

- Step 1** Select the following menu in Cisco Unified Presence Administration:
 Release 7.0: **Application > Cisco Unified Personal Communicator > Conferencing Server**
 Release 6.x: **Application > Cisco Unified Personal Communicator > MeetingPlace Server**
- Step 2** Click **Add New** in the Find and List window to add a new server.
- Step 3** Enter information into the fields.

Field	Setting
Name	Enter the server name.
Description	(Optional) Enter a server description.
Hostname/IP Address	Enter an IP address or a fully qualified domain name of the server.

Field	Setting
Port	Specify the port number configured for the server. Enter 80 for HTTP or 443 for HTTPS.
Protocol	Specify the protocol to use when contacting this server: <ul style="list-style-type: none"> • HTTP: Selects Hypertext Transfer Protocol as the standard method for transferring data between the server, Cisco Unified Personal Communicator, and the browser. Select this option if the Cisco Unified MeetingPlace or the Cisco Unified MeetingPlace Express <i>does not have</i> SSL enabled. • HTTPS: selects Hypertext Transfer Protocol over SSL as the method for securely transferring data between the server, Cisco Unified Personal Communicator, and the browser. Select this option if the Cisco Unified MeetingPlace or the Cisco Unified MeetingPlace Express server has SSL enabled.

Step 4 Click **Save**.

Related Topics

- [Creating Conferencing Profiles in Cisco Unified Presence Administration, page 3-18](#)

Creating Conferencing Profiles in Cisco Unified Presence Administration

You must create conferencing profiles in Cisco Unified Presence Administration and assign each to a primary server.



Note

By contrast, a profile in Cisco Unified MeetingPlace or in Cisco Unified MeetingPlace Express defines the privileges and preferences configured for a specific user in this application.

Before You Begin

- You must create the conferencing profile before you can add Cisco Unified Personal Communicator licensed users to the application profile.
- You must first specify conferencing server names and addresses before you can select them in this procedure.

Restrictions

Conferencing server failover is not supported in Cisco Unified Personal Communicator Release 7.0(1).

Procedure

- Step 1** Select the following menu in Cisco Unified Presence Administration:
- Release 7.0: **Application > Cisco Unified Personal Communicator > Conferencing Profile**
Release 6.x: **Application > Cisco Unified Personal Communicator > MeetingPlace Profile**
- Step 2** Click **Add New** in the Find and List window to add a new profile.

Step 3 Enter information into the fields.

Field	Setting
Name	Enter the profile name.
Description	(Optional) Enter a profile description.
Primary Conferencing Server	Select one of the conferencing servers that you specified as the primary server. This field is called Primary MeetingPlace Server in Release 6.x.
Backup Conferencing Server	Set to None . This field is called Backup MeetingPlace Server in Release 6.x.
Add Users to Profile	Click this button, then use the Find and List Users window to find and select users. Click Add Selected to add users to the profile.
Release 7.0 Only	
Make this the Default Conferencing Profile for the System	(Optional) Check so that any new users who are added to the system are automatically placed 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 4 Click **Save**.

Related Topics

- [Changing Application Profiles for a Single User, page 2-32](#)
- [Specifying Conferencing Server Names and Addresses in Cisco Unified Presence Administration, page 3-17](#)

Configuring Videoconferencing Resources

Through Cisco Unified Communications Manager Administration, you can enable merged conference calls (three or more parties) with audio and video support for Cisco Unified Personal Communicator soft-phone users. Any participant in the conference call can merge other participants into the conference.

Before You Begin

- Install a supported release of the videoconferencing server. For details about the server installation: http://www.cisco.com/en/US/products/hw/video/ps1870/tsd_products_support_series_home.html

For details about supported Cisco Unified Videoconferencing releases, see the Cisco Unified Personal Communicator release notes: http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html
- Obtain the MAC address of the videoconference bridge.

Procedure

- Step 1** Select **Media Resources > Conference Bridge**.
- Step 2** Add the videoconference bridge.
- Step 3** Select **Media Resources > Media Resource Group List**.
- Step 4** Create a media resource group list.
- Step 5** Add the videoconference bridge to the media resource group list.
- Step 6** Select **Media Resources > Media Resource Group**.
- Step 7** Create a media resource group.
- Step 8** Add a media resource to the media resource group.
- Step 9** (Optional) To enable any participant to add more participants the conference, perform the following steps:
- Select **System > Service Parameters**.
 - Select the Cisco Unified Communications Manager server and service.
 - Set Advanced Ad Hoc Conference Enabled to **True** in the Clusterwide Parameter (Feature - Conference) section.
- Step 10** Associate the phone with the new media resource group list:
- Select **Device > Phone** in Cisco Unified Communications Manager Administration.
 - Under Search Options, search for the directory number of the phone, and when it is found, click the device name.
 - In the Phone Configuration window in the Device Information section, find the Media Resource Group List, and select the media resource group list that you just configured.
 - Select **Enabled** for Video Capabilities in the Product Specific Configuration Layout section.
 - Click **Save**.
 - Click **Reset**.

For detailed configuration instructions, use the Cisco Unified Communications Manager Administration online help or the *Cisco Unified Communications Manager Administration Guide*:

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

Related Topics

- [Adding Cisco Unified Personal Communicator as a Phone Type, page 2-5](#)
- [Configuring Users for Point-to-Point Video Calls and for Multipoint Videoconferencing, page 2-34](#)