Basic feature configuration for Cisco Unified Personal Communicator

.

This chapter includes the information required to deploy Cisco Unified Personal Communicator. For information specific to Cisco Jabber clients, such as Jabber for Windows, see the appropriate client documentation below:

- Cisco Jabber—http://www.cisco.com/web/products/voice/jabber.html

- Cisco Jabber for Windows—http://www.cisco.com/en/US/products/ps12511/index.html

- Cisco Jabber for Mac—http://www.cisco.com/en/US/products/ps11764/index.html

- Android—http://www.cisco.com/en/US/products/ps11678/index.html

- BlackBerry—http://www.cisco.com/en/US/products/ps11763/index.html

- iPad—http://www.cisco.com/en/US/products/ps12430/index.html

- iPhone—http://www.cisco.com/en/US/products/ps11596/index.html

- Nokia—http://www.cisco.com/en/US/products/ps11766/index.html

- Video for TelePresence—http://www.cisco.com/en/us/products/ps11328/index.html

- Web SDK—http://www.cisco.com/en/US/products/ps11765/index.html

If you wish to continue with information specific to Cisco Unified Personal Communicator, proceed with the contents in this chapter:

Note CTI gateway and voicemail configuration has moved from IM and Presence to Cisco Unified Communications Manager. For more information about these features, see the *Cisco Unified Communications Manager Administration Guide, Release 9.0(1)*.

Roadmap for deploying Cisco Unified Personal Communicator

The following table provides a feature-by-feature map of topics that describe the tasks you need to perform to deploy Cisco Unified Personal Communicator:

To Deploy These Features...	Read These Topics...	Perform These Tasks...
Pre-deployment tasks	• Prerequisites for integrating Cisco Unified Personal Communicator, on page 4	• Assign the licensing capabilities on Cisco Unified Communications Manager. • Configure firewalls to pass Cisco Unified Personal Communicator traffic, on page 5
Availability status information and instant messaging	• (Cisco Unified Personal Communicator Release 8.x) required XCP services, on page 6 • (Cisco Unified Personal Communicator Release 8.x) optional XCP services, on page 6	• Verify Cisco XCP Router service is running, on page 6 • Turn on IM and Presence Services to support XMPP clients • (Cisco Unified Personal Communicator Release 8.x) configure settings, on page 22 • (Cisco Unified Personal Communicator Release 8.5) configuring chat history, on page 8

To Deploy These Features...	Read These Topics...	Perform These Tasks...
Advanced instant messaging features, such as group chat and persistent chat rooms	• (Cisco Unified Personal Communicator Release 8.x) optional XCP services, on page 6	• Service parameter configuration for IM Gateway, on page 7 • Configuring persistent chat rooms, on page 7
Place calls from a computer	• Application dialing and directory lookup rules, on page 8 • Transformation of dialed numbers by Cisco Unified Personal Communicator, on page 9 • Cisco Unified Client Services Framework device type, on page 10 • Extension Mobility configuration, on page 10 • (Cisco Unified Personal Communicator Release 8.x) guidelines for configuring softphone device name, on page 11 • TFTP server connection, on page 20	
Place calls from a desk phone	• Desk phone control and CTI connection failures, on page 11	
Video calls and videoconferencing	-	• Configure users for point-to-point video calls and for multipoint videoconferencing, on page 24 • Configure videoconferencing resources and Ad-Hoc conferencing on Cisco Unified Communications Manager, on page 25 • (Cisco Unified Personal Communicator Release 8.x) configure settings, on page 22

To Deploy These Features...	Read These Topics...	Perform These Tasks...
Alternative server to control signing in	-	• Configure CCMCIP profiles for Cisco Unified Personal Communicator release 8.x
Security features	-	• (Cisco Unified Personal Communicator Release 8.x) configure settings, on page 22
High availability features	• High Availability, on page 21	• High Availability IM and Presence deployments configuration
Third-party client applications	• (Cisco Unified Personal Communicator Release 8.x) optional XCP services, on page 6	• Third-Party client configuration on IM and Presence
HTML content display	-	• (Cisco Unified Personal Communicator Release 8.5) Distribute HTML files for display in Cisco Unified Personal Communicator window
Desktop agent	• (Cisco Unified Personal Communicator Release 8.5) Cisco Unified Personal Communicator as desktop agent	• Configure Cisco Unified Personal Communicator as desktop agent • Start Cisco Unified Personal Communicator as desktop agent

Prerequisites for integrating Cisco Unified Personal Communicator

Before you configure Cisco Unified Personal Communicator, ensure that you have done the following:

- Configured the Cisco Unified Communications Manager node for integration with IM and Presence Service.

- Configured the IM and Presence Service node.

- Configured licensing details on Cisco Unified Communications Manager for IM and Presence Service. After a user is licensed, the user can use Cisco Unified Personal Communicator.

- Assigned all of your Cisco Unified Personal Communicator users to IM and Presence Service nodes in the system topology.

- (Optional) Configured Cisco Unity Connection and Cisco Unified MeetingPlace or Cisco WebEx so that Cisco Unified Personal Communicator can use visual voicemail and meeting features.

Note   Before you deploy Cisco Unified Personal Communicator Release 8.x to your users' computers, ensure that no other applications are installed that depend on Cisco Unified Client Services Framework. For a list of these applications, see the *Release Notes for Cisco Unified Personal Communicator* at http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html.

Related Topics

Cisco Unified Communications Manager configuration for integration with IM and Presence Service

IM and Presence server configuration for deployment in network

Configure firewalls to pass Cisco Unified Personal Communicator traffic

Internet traffic moves through a firewall based on service identification numbers that are known as ports. Certain ports must be open for Cisco Unified Personal Communicator to work. Network administrators typically open a minimal number of network ports, allowing the traffic for approved applications to enter and leave the network while blocking other network traffic.

Before You Begin

Read information about the network ports used by Cisco Unified Personal Communicator in the Release Notes for Cisco Unified Personal Communicator.

Procedure

Step 1   Identify whether users have a software firewall installed on their computers, or if there is a hardware firewall in the network between IM and Presence and Cisco Unified Personal Communicator.

Step 2   Configure the firewall to pass Cisco Unified Personal Communicator traffic.
Failure to perform this step results in missing, incorrect, or intermittent display of availability status in Cisco Unified Personal Communicator.

Related Topic

Release Notes for Cisco Unified Personal Communicator:

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

Verify Cisco XCP Router service is running

Procedure

Step 1   Choose **Tools** > **Control Center - Network Services** in Cisco Unified IM and Presence Serviceability in IM and Presence.

Step 2   Choose the node from the Server list box.

Step 3   Click **Go**.

Step 4   Locate the Cisco XCP Router service in the IM and Presence Services section.

Step 5   Verify that the Status column reads "Running."

Related Topics

Cisco XCP Router restart

(Cisco Unified Personal Communicator Release 8.x) about configuring XCP services for Cisco Unified Personal Communicator

(Cisco Unified Personal Communicator Release 8.x) required XCP services

You must ensure that the following IM and Presence XCP services are running on all IM and Presence nodes in all clusters:

• Cisco XCP Authentication Service

• Cisco XCP Connection Manager

(Cisco Unified Personal Communicator Release 8.x) optional XCP services

Depending on what features you want to make available, ensure that the following IM and Presence XCP services are running on all IM and Presence nodes in all clusters:

• Cisco XCP Text Conference Manager, for group chat and persistent chat rooms.

• Cisco XCP Web Connection Manager, to manage connections for web-based client applications, that connect to IM and Presence using HTTP.

• Cisco XCP SIP Federation Connection Manager, to support federation services with third-party applications that use SIP.

- Cisco XCP XMPP Federation Connection Manager, to support federation services with third-party applications that use XMPP.

- Cisco XCP Counter Aggregator, if you want system administrators to be able to view statistical data on XMPP components.

- Cisco XCP Message Archiver, for automatic archiving of all instant messages.

- Cisco XCP Directory Service, if you want to enable third-party XMPP client applications to do LDAP searches.

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

Related Topics

Turn on IM and Presence Services to support XMPP clients
Turn on Cisco XCP Text Conference Manager
Chat configuration on IM and Presence
Turn on IM and Presence services

Chat configuration

Service parameter configuration for IM Gateway

Users of SIP IM clients must be able to exchange bi-directional IMs with users of XMPP IM clients. Turn on the SIP-to-XMPP connection on the IM and Presence IM Gateway for IM interoperability between SIP and XMPP clients.

You must also ensure that the Cisco XCP SIP Federation Connection Manager service is running.

Related Topics

Turn on IM and Presence services
Authorization policy configuration on IM and Presence

Configuring persistent chat rooms

To configure persistent chat rooms, you must first configure persistent chat servers. To configure persistent chat servers, you must set up a PostgreSQL database. For more information about how to configure an external database in IM and Presence see the *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* at the following URL:

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

You must also ensure that the Cisco XCP Text Conference Manager service is running.

When a Cisco Unified Personal Communicator user joins a persistent chat room, IM and Presence sends instant message history information to the Cisco Unified Personal Communicator user. The number of messages in instant message history that IM and Presence sends is specified in the Number of messages that display per room option, which you specify when you configure conferencing and persistent chat. If the Archive all room messages option is enabled for persistent chat, Cisco Unified Personal Communicator queries IM and Presence for additional history, and the number of messages displayed by Cisco Unified Personal Communicator might exceed the value in the Number of messages to display per room setting on the IM and Presence node.

Related Topics

Turn on IM and Presence services

Configure persistent chat room settings

(Cisco Unified Personal Communicator Release 8.5) disabling chat

You can configure the IM and Presence Service to disable the chat feature on Cisco Unified Personal Communicator. For information about how to disable chat, see Turn on or off instant messaging for IM and Presence cluster.

Related Topic

Turn on or off instant messaging for IM and Presence cluster

(Cisco Unified Personal Communicator Release 8.5) configuring chat history

You can configure the IM and Presence service to prevent Cisco Unified Personal Communicator from keeping a log of the chat history on the client computer. The ability to prevent the chat history is introduced in Cisco Unified Personal Communicator Release 8.5 and is not configurable on earlier versions of Cisco Unified Personal Communicator or IM and Presence. For information about how to configure the chat history on IM and Presence, see Allow clients to log instant message history.

Related Topic

Allow clients to log instant message history

Cisco Unified Personal Communicator configuration on Cisco Unified Communications Manager

Application dialing and directory lookup rules

Based on the dial plan for your company and the information stored in the LDAP directory (telephone number for the user), you might need to define application dialing rules and directory lookup rules on Cisco Unified Communications Manager. IM and Presence then queries Cisco Unified Communications Manager to obtain these dialing rules for the Cisco Unified Personal Communicator.

These rules define how Cisco Unified Personal Communicator can reformat the inbound call ID to be used as a directory lookup key and how to transform a phone number retrieved from the LDAP directory for outbound dialing.

When you are configuring application dial rules, note the following:

- Cisco Unified Communications Manager Release 7.1 supports application dial rules that contain the plus character in dialed numbers.

The following table defines the application dialing rules and directory lookup rules, and provides examples and the menu path for each.

Table 1: Dialing rule definitions

Rule	Definition	Configuration Example	Menu path
Application dial rules	Application dial rules automatically strip numbers from, or add numbers to, phone numbers that the user dials. Application dialing rules are used to manipulate numbers that are dialed from Cisco Unified Personal Communicator.	You can configure a dialing rule in Cisco Unified CM Administration that automatically adds the digit 9 at the start of a 7-digit phone number to provide access to an outside line.	**Call Routing** > **Dial Rules** > **Application Dial Rules**
Directory lookup rules	Directory lookup rules transform caller identification numbers into numbers that can be looked up in the directory from Cisco Unified Personal Communicator. Each rule specifies which numbers to transform based on the initial digits and the length of the number.	You can create a directory lookup rule in Cisco Unified CM Administration that automatically removes the area code and two prefix digits from a 10-digit telephone. This rule transforms 4089023139 into 23139.	**Call Routing** > **Dial Rules** > **Directory Lookup Dial Rules**

Related Topics

Transformation of dialed numbers by Cisco Unified Personal Communicator

Before Cisco Unified Personal Communicator places a call through contact information, the application removes everything from the phone number to be dialed, except for letters and digits. The application transforms the letters to digits and applies the dialing rules from IM and Presence. The letter-to-digit mapping is locale-specific and corresponds to the letters found on a standard telephone keypad for that locale. For example, for an US English locale, 1-800-GOTMILK transforms to 18004686455.

Users cannot view or modify transformed numbers before Cisco Unified Personal Communicator places the numbers. If there is a problem with the dialed number because of incorrect conversions, you must correct the dialing rules.

Related Topics

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

Cisco Unified Client Services Framework device type

Cisco Unified Personal Communicator requires a new Cisco Unified Communications Manager device type called Cisco Unified Client Services Framework. Depending on which release of Cisco Unified Communications Manager is installed in your Cisco Unified Communications system, you might need to patch Cisco Unified Communications Manager with a Cisco Options Package (COP) file.

You must run the COP file if your Cisco Unified Communications Manager does not have the Cisco Unified Client Services Framework device type. You run the COP file on the Cisco Unified Communications Manager database publisher node. After you apply the COP file, you must restart the Cisco Unified Communications Manager database publisher node, and all other nodes.

For information about which releases of Cisco Unified Communications Manager require you to run the COP file to install the Cisco Unified Client Services Framework device type, see the *Release Notes for Cisco Unified Personal Communicator* at the following URL:

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

Extension Mobility configuration

The Extension Mobility feature dynamically configures a phone according to the user that is currently logged into the phone. When a user logs in to the phone, the phone adopts the default device profile information for that user, including line numbers, speed dials, services links, and other user-specific phone properties.

By using Extension Mobility, a Cisco Unified Personal Communicator user can associate the application with one or more desk phones that have the same directory number on the primary line as the default desk phone of the user on Cisco Unified Communications Manager.

You can configure Extension Mobility on Cisco Unified CM Administration by choosing **Device** > **Phone**menu, and accessing the Directory Number configuration window.

When you configure Extension Mobility, note the following:

- When you create the device user profile (**Device** > **Device Settings** > **Device Profile**), enable CTI control, and ensure that the line is controllable by CTI.

- When you add the Cisco Unified IP Phone to Cisco Unified Communications Manager (**Device** > **Phone**), make sure that is controllable by CTI.

Related Topics

(Cisco Unified Personal Communicator Release 8.x) guidelines for configuring softphone device name

When you create a softphone device for each Cisco Unified Personal Communicator Release 8.0 user, you choose the Cisco Unified Client Services Framework device type.

You must also specify a device name. 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.

Desk phone control and CTI connection failures

The CTI gateway provides desk phone control (phone-association mode) to Cisco Unified Personal Communicator users. You must specify CTI gateway server names, addresses, ports, and protocol types on Cisco Unified Presence so that the information required to reach the CTI gateway server can be downloaded when the user logs in to Cisco Unified Personal Communicator.

If the CTI connection to Cisco Unified Communications Manager is lost while Cisco Unified Personal Communicator is operating in desk phone mode, the application tries to reestablish the connection to the primary and then to the backup nodes. Connection attempts continue on a round-robin basis, beginning again with the primary node. Successive attempts to reconnect to a node occur at intervals of 4, 8, 16, 32, and 60 seconds (maximum) until a connection is re-established.

Table 2: CTI Connection Status and Expected Recovery Behavior

Scenario	Expected Recovery Behavior
CTI connection fails and no calls are present	- Cisco Unified Personal Communicator attempts to reconnect to the next available CTI server. - Until a connection is established, the Cisco Unified Personal Communicator user cannot initiate any new calls through the application. No new incoming call notifications are provided through the application. - The user has manual control of the desk phone for making and receiving calls. - When Cisco Unified Personal Communicator reconnects to one of the CTI servers, Cisco Unified Personal Communicator users again have the ability to control and monitor new calls through the application.

Scenario	Expected Recovery Behavior
CTI connection fails with one or more calls present	• Cisco Unified Personal Communicator attempts to reconnect to the next available CTI server. • Existing calls are unaffected, but the user no longer has control through Cisco Unified Personal Communicator and does not receive any updates or changes in the call state. Any existing Cisco Unified Personal Communicator session window closes. • The user has manual control of the physical phone for making and receiving calls. • When Cisco Unified Personal Communicator reconnects to one of the CTI servers, it opens a new session window for each call and shows the current state. • Cisco Unified Personal Communicator remains connected to the current node (whether primary or backup) until the user relaunches Cisco Unified Personal Communicator or when a connection failure causes it to reconnect.

Related Topics

Configure CTI Gateway server names and addresses

You do not need to perform this procedure if you previously configured Cisco Unified Communications Manager with an IP address through the **Cisco Unified CM Administration** > **System** > **Server** menu. IM and Presence dynamically creates a TCP-based CTI gateway host profile for that address, and automatically populates the CTI gateway fields on IM and Presence.

Before You Begin

- Make sure that you have completed this configuration on Cisco Unified Communications Manager:

    ◦ Configured the phone devices for CTI device control.

    ◦ Added the Cisco Unified Personal Communicator users to a CTI-enabled user group.

- Obtained the hostnames or IP addresses of the CTI gateway.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Application** > **Cisco Jabber** > **CTI Gateway Server**.

Step 2 Click **Add New**.

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 the FQDN (Fully Qualified Domain Name) of Cisco Unified Communications Manager that is running the CTI service.
Port	Enter 2748.

Step 4 Click **Save**.
Troubleshooting Tip

You can see the CTI gateway information in the Server Health window in Cisco Unified Personal Communicator (**Help** > **Show Server Health**on Windows operating system and **Help** > **Show System Diagnostics** on Mac OS).

What to Do Next

Create CTI Gateway profiles, on page 13

Related Topics

User and device configuration on Cisco Unified Communications Manager
Desk phone control and CTI connection failures, on page 11

Create CTI Gateway profiles

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

Before You Begin

- You must create the CTI gateway profile before you can add Cisco Unified Personal Communicator licensed users to the application profile.

- You must first specify CTI gateway server names and addresses in **Application** > **Cisco Jabber** > **CTI Gateway Server** before you can choose the servers as primary or backup nodes in this procedure.

- IM and Presence dynamically creates a TCP-based CTI gateway profile based on the hostname of Cisco Unified Communications Manager. Before using this profile, verify that IM and Presence and Cisco Unified Personal Communicator clients can ping Cisco Unified Communications Manager by the DNS name. If they cannot contact the node, you need to add the IP address of Cisco Unified Communications Manager in Cisco Unified CM IM and Presence Administration (**Application** > **Cisco Jabber** > **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 CM Administration** > **System** > **Server** menu, IM and Presence dynamically creates a TCP-based CTI gateway profile based on that address. The fields in IM and Presence Administration

(**Application** > **Cisco Jabber** > **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   Choose **Application** > **Cisco Jabber** > **CTI Gateway Profile**.

Step 2   Click **Add New**.

Step 3   Enter information into the fields.

Field	Setting
Name	Enter the profile name.
Description	(Optional) Enter a profile description.
Primary CTI Gateway Server and Backup CTI Gateway Server	Choose a primary server and backup servers.
Make this the Default CTI Gateway Profile for the System	Check so that any new users that are added to the system are automatically placed into this default profile.
	Users who are already synchronized to IM and Presence from Cisco Unified Communications Manager are not added to the default profile. However, after the default profile is created, any users synchronized after that are added to the default profile.

Step 4   Click **Add Users to Profile**.

Step 5   Use the Find and List Users window to find and choose users.

Step 6   Click **Add Selected** to add users to the profile

Step 7   Click **Save** in the main CTI Gateway Profile window.

Related Topics

Cisco Unified Personal Communicator configuration on Cisco Unified Communications Manager

Create softphone device for each Cisco Unified Personal Communicator user

To enable Cisco Unified Personal Communicator softphone features, you must create a new softphone device for each user. This topic describes how to create a softphone device for one user. To create softphone 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 Cisco Unified Personal Communicator licensing requirements module, including the information about adjunct licensing.

- Read the guidelines on configuring the device name.
  Restrictions

The auto-registration features in Cisco Unified Communications Manager are not supported with Cisco Unified Personal Communicator.

Procedure

Step 1 Choose **Cisco Unified CM Administration** > **Device** > **Phone**.

Step 2 Click **Add New**.

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

Step 4 Click **Next**.

Step 5 Configure the following information:

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

b) Enter a descriptive name for the phone in the Description field. For example, enter Richard–softphone.

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

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

e) Configure all the required fields for your environment.

f) Choose the user ID from Owner User ID menu.

g) Choose the device name of the Cisco Unified IP Phone to associate with Cisco Unified Personal Communicator from Primary Phone.

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

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

Field	Setting
Presence Group	Choose **Standard Presence Group**.

Field	Setting
Device Security Profile	Choose **Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile**.
SIP Profile	Choose **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.
Digest User	Choose the user ID. This is the same user ID as the one you chosen for Owner User ID.

Step 6   Click **Save**.

Step 7   Click 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 the Cisco Unified Personal Communicator.

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 Cisco Unified Personal Communicator 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   Click **Save**.

Make sure that the status shown at the top of the window indicates a successful save and that the resulting status is Ready.

Troubleshooting Tips

• The directory number that is configured for Cisco Unified Personal Communicator and the Cisco Unified IP Phone must be identical. A directory number is configured with a partition, and you assign a directory number to Cisco Unified Personal Communicator and the Cisco Unified IP Phone. This configuration causes the Cisco Unified Personal Communicator to share the line with the Cisco Unified IP Phone for this user.

• 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.

• From Cisco Unified Communications Manager Release 6.x, make sure that an association exists between the user and the line that is configured for that user so that the correct availability status in Cisco Unified Personal Communicator is displayed. Choose **Device** > **Phone**, and view the association information for the device. Make sure that the user is associated with the line on the Directory Number configuration window. Make sure that you associate the line and user for all the phones used by the user for that directory number.

What to Do Next

Related Topics

Associate users with softphone devices

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 Choose **Cisco Unified CM Administration** > **System** > **LDAP** > **LDAP Directory**.

Step 2 Search for the LDAP directory in the Find and List LDAP Directories window.

Step 3 Choose the LDAP configuration name for the LDAP directory.

Step 4 Click **Perform Full Sync Now**.

Step 5 Choose **Cisco Unified CM Administration** > **Device** > **Phone**.

Step 6 Search for the device for the user in the Find and List Phones window.

Step 7 Choose the name of the device.

Step 8 Choose the directory number for the device in the Association Information section that displays on the left side of the window.

Step 9 Click **Associate End Users** at the bottom of the window.

Step 10 Search for the user in the Find and List Users window.

Step 11 Choose the user, then click **Add Selected**.

Step 12 Click **Save** on the Directory Number Configuration window.

What to Do Next

Add users to access control groups

Procedure

Step 1 Choose **Cisco Unified CM Administration** > **User Management** > **End User**.

Step 2 Search for the user in the Find and List Users window.

Step 3 Choose the user.

Step 4 Click **Add to Access Control Group** in the Permissions Information section.

Step 5 Use the Find and List Access Control Groups window to find and choose the following access control groups:

- Standard CCM End Users

- Standard CTI Enabled

If the phone of the user is a Cisco Unified IP Phone 9900 or 8900 series model, choose the following access control group also:

- Standard CTI Allow Control of Phones supporting Connected Xfer and conf access control group

If the phone of the user is a Cisco Unified IP Phone 6900 series model, choose the following access control group also:

- Standard CTI Allow Control of Phones supporting Rollover Mode

Step 6 Click **Add Selected**.

Step 7 Click **Save** on the End User Configuration window.

What to Do Next

-

Associate new device with a user

Procedure

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

What to Do Next

Reset device

Procedure

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

Specify softphone device for user with multiple associated softphone devices

If Cisco Unified Personal Communicator user has more than one associated softphone device in Cisco Unified Communications Manager, you can specify which device to use on startup by excluding all other devices. To do this, you must set the value of the following registry key value to be a comma-separated list of device names, as follows:

Registry Key	Sample Value
ExcludedDevices	csfjohndoe,csfjanedoe

The registry key is located in HKEY_CURRENT_USER\Software\Cisco Systems, Inc.\Client Services Framework\AdminData.

About Cisco Unified Personal Communicator configuration on IM and Presence

TFTP server connection

Cisco Unified Personal Communicator connects to the primary Trivial File Transfer Protocol (TFTP) server (whose address is retrieved from IM and Presence) at startup. When the connection is established, Cisco Unified Personal Communicator downloads the <softphone-device-name>.cnf.xml configuration file from Cisco Unified Communications Manager for each user.

The configuration file contains the list of Cisco Unified Communications Manager primary and failover server addresses and the transport protocol for Cisco Unified Personal Communicator to use in softphone mode to connect to Cisco Unified Communications Manager.

After Cisco Unified Personal Communicator downloads the file successfully, the configuration information is made available to other Cisco Unified Personal Communicator subsystems, and Cisco Unified Personal Communicator disconnects from the TFTP server.

Each time Cisco Unified Personal Communicator tries to download the configuration file, the application attempts to contact the primary TFTP server. If the primary TFTP server does not respond, Cisco Unified Personal Communicator fails over to the backup TFTP servers, if any exist. Cisco Unified Personal Communicator fails over to the backup TFTP servers in the order specified in Cisco Unified CM IM and Presence Administration.

If all TFTP server connections fail, Cisco Unified Personal Communicator tries to load the last valid downloaded configuration from the following locations:

Platform	Location
Windows XP	drive:\Documents and Settings\username\Local Settings\Application Data\Cisco\Unified Communications\Client Services Framework\Config
Windows Vista	

- For Mac OS: ~/Library/Caches/com.cisco.AriesX/<username>/Phone/

If the loading of the local file is successful, Cisco Unified Personal Communicator updates the Server Health window with a warning notification (yellow indicator). If the file transfer fails and the file does not exist, Cisco Unified Personal Communicator updates the Server Health window with a failure notification and switches to Disabled mode.

The following Cisco Unified Communications Manager failover restrictions apply to Cisco Unified Personal Communicator:

- Auto-registration is not supported.

- Cisco Unified Personal Communicator fails over to a configured TFTP server when it tries to download the configuration file. The application also tries to download the file from the backup TFTP servers.

- AutoUpdate and upgrades through TFTP are not supported for Cisco Unified Personal Communicator software.

Related Topics

Configure TFTP addresses, on page 21

High Availability

High availability in a subcluster means that if a node in the subcluster fails, the Instant Message and Availability services from that node can fail over to the second node in the subcluster. High Availability is supported for the following releases of Cisco Unified Personal Communicator:

- Cisco Unified Personal Communicator Release 8.5 with IM and Presence Release 8.5

- Cisco Unified Personal Communicator Release 8.6 with IM and Presence Release 8.6

To configure high availability for Cisco Unified Personal Communicator clients, you configure high availability on the IM and Presence node. For more information, refer to High Availability IM and Presence deployments configuration.

The impact of failover on Cisco Unified Personal Communicator is described in Impact of failover to IM and Presence clients and services.

Cisco Unified Personal Communicator configuration on IM and Presence

Configure TFTP addresses

Before You Begin

- Read the TFTP server connection topic.

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

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Application** > **Legacy Clients** > **Settings**.

Step 2 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 3 Click **Save**.
Troubleshooting Tip

You can see the TFTP server addresses in the Server Health window in Cisco Unified Personal Communicator (**Help** > **Show Server Health**on Windows operating system and **Help** > **Show System Diagnostics** on Mac OS).

Related Topics

(Cisco Unified Personal Communicator Release 8.x) configure settings

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Application** > **Legacy Clients** > **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. For example, C:\CSFcerts. If you use a relative path, the path is relative to the CSF installation directory C:\Program Files\Common Files\Cisco Systems\Client Services Framework. If you do not specify a directory, CSF looks for the certificates in the following directory and trusts any certificates in that location: **Windows XP:** drive:\Documents and Settings\username\Local Settings\Application Data\Cisco\Unified Communications\Client Services Framework\certificates **Windows Vista/Windows 7:** drive:\Users\username\AppData\Local\Cisco\Unified Communications\Client Services Framework\certificates Default Setting: Not set

Step 3   Click **Save**.

Related Topics

LDAP directory integration with Cisco Unified Personal Communicator
LDAP directory integration for contact searches on XMPP clients

Video calls and Videoconferencing configuration

Configure users for point-to-point video calls and for multipoint videoconferencing

Procedure

Step 1 (For multipoint videoconferencing) If you want Cisco Unified Personal Communicator softphone users to have merged conference calls (three or more parties) with audio and video support, you must first configure videoconferencing resources.

Step 2 Distribute cameras that are supported for use with Cisco Unified Personal Communicator. For a list of these cameras, see the *Release Notes for Cisco Unified Personal Communicator*:
http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html

The camera driver installer is not provided with some models of Cisco VT Camera. In this case, you must distribute the installer.

a) For new installations:

- If users are to perform the installation, distribute the camera, the camera driver installer (if a driver is necessary), and the user guide.

- If users already have a supported camera, do not distribute the driver.

Step 3 Provide users with the appropriate documentation to complete the installation.

What to Do Next

For details about supported cameras, video codecs, and audio codecs, see the Release Notes for Cisco Unified Personal Communicator:

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

Provide users with this documentation:

- Cisco Unified Personal Communicator user documentation:

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

- Cisco VT Camera Quick Start Guide (for use with Windows-based computers)

  http://www.cisco.com/en/US/products/sw/voicesw/ps5662/prod_installation_guides_list.html

Related Topics

Configure videoconferencing resources and Ad-Hoc conferencing on Cisco Unified Communications Manager

Using Cisco Unified CM Administration, you can enable merged conference calls (three or more parties) with audio and video support for Cisco Unified Personal Communicator 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.

- Obtain the MAC address of the videoconference bridge.

Procedure

Step 1   Perform the following configuration on Cisco Unified MeetingPlace Application Server Administration Center:

Task	Menu Path
Enter the IP address of your Cisco Unified Communications Manager in the **Primary TFTP server** fields.	**System Configuration** > **Call Configuration** > **Ad-Hoc** > **Cisco Unified Communications Manager Configuration**
Enter the MAC address of your Cisco Unified Communications Manager in the **Application server MAC address** field.	

Step 2   Perform the following configuration on Cisco Unified Communications Manager:

Task	Menu Path
Configure the videoconference bridge.	**Cisco Unified CM Administration** > **Media Resources** > **Conference Bridge**
Create a media resource group list.	**Cisco Unified CM Administration** > **Media Resources** > **Media Resource Group List**
Add the videoconference bridge to the media resource group list.	
Create a media resource group.	**Cisco Unified CM Administration** > **Media Resources** > **Media Resource Group**
Add a media resource to the media resource group.	
Assign devices to the media resource group list. Search for the device in the Find and List Phones window. Choose the device, then choose the list from the Media Resource Group List drop-down list.	**Cisco Unified CM Administration** > **Device** > **Phone**

Step 3 (Optional) To enable any participant to add more participants to the conference, perform the following steps:

a) Choose **Cisco Unified CM Administration** > **System** > **Service Parameters** in Cisco Unified CM Administration.

b) Choose your Cisco Unified Communications Manager node from the Server drop-down list.

c) Choose **Cisco CallManager (Active)** from the Service drop-down list.

d) To enable any participant to add more participants the conference, set Advanced Ad Hoc Conference Enabled to **True** in the Clusterwide Parameter (Feature - Conference) section.

e) To specify a minimum number of video-capable participants for ad-hoc conferences, enter the minimum number in the **Minimum Video Capable Participants To Allocate Video Conference** field in the Clusterwide Parameters (Feature - Conference) section.
  When an ad-hoc conference starts, the conference uses an audio bridge or a video bridge, depending on the value in this setting. For example, if you set this setting to 2, a minimum of two participants in the conference must have video-enabled devices. If this at least two participants do not have video-enabled devices, then the conference becomes an audio-only conference. The participants cannot change the conference to video after this happens.

f) Click **Save**.

Step 4 Associate the phone with the new media resource group list:

a) Choose **Cisco Unified CM Administration** > **Device** > **Phone**.

b) Under Search Options, search for the directory number of the phone, and when it is found, choose the device name.

c) In the Phone Configuration window in the Device Information section, find the Media Resource Group List, and choose the media resource group list that you just configured.

d) Choose **Enabled** for Video Capabilities in the Product Specific Configuration Layout section.

e) Click **Save**.

f) Click **Reset**.

Related Topics

Configure bandwidth capability for Cisco Unified Personal Communicator

Cisco Unified Personal Communicator uses a Cisco Unified Communications Manager device type called Cisco Unified Client Services Framework. The bandwidth capability of the Cisco Unified Client Services Framework device that is associated with an installation of Cisco Unified Personal Communicator, is one of several factors that determine the video capability of the Cisco Unified Personal Communicator for the user.

To configure the bandwidth capability of Cisco Unified Client Services Framework devices, use the region settings of the device pool that the Cisco Unified Client Services Framework device is in. The following settings affect the bandwidth capability of the device:

• Audio Codec

• Video Call Bandwidth

For more information about region and device pool configuration in Cisco Unified Communications Manager, see 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

(Cisco Unified Personal Communicator Release 8.x) Cisco Unified IP phones configuration for video

The Cisco Unified Client Services Framework (CSF) device type is always video-enabled, so you do not need to configure devices of this type. However, you must explicitly configure Cisco Unified IP Phones to enable video.

If you want Cisco Unified Personal Communicator to be able to send and receive video, you must select the following devices as controlled devices for the user:

- The Cisco Unified Client Services Framework device

- Any desk phone devices

Note   When you use your Cisco Unified IP Phone for phone calls, you can only use video on your computer if the Cisco Unified IP Phone uses Skinny Client Control Protocol (SCCP).

(Cisco Unified Personal Communicator Release 8.x) connect Cisco Unified IP phone to network and your computer

Procedure

Step 1   Connect the SW port on the Cisco Unified IP Phone to the network.

Step 2   Connect the PC port on the Cisco Unified IP Phone to the controlling PC with an Ethernet cable.

What to Do Next

(Cisco Unified Personal Communicator Release 8.x) Enable video for Cisco Unified IP phone, on page 28

(Cisco Unified Personal Communicator Release 8.x) Enable video for Cisco Unified IP phone

Procedure

Step 1   Choose **Device** > **Phone** in Cisco Unified CM Administration.

Step 2   Find the device that you want to configure.

Step 3   Click on the Device Name.

Step 4   Scroll to the **Product Specific Configuration Layout** section.

Step 5   Choose **Enabled** from the **PC Port** drop-down list.

Step 6   Choose **Enabled** from the **Video Capabilities** drop-down list.

Step 7   Click **Save**.
When video is enabled on the phone, a video icon is displayed in the lower-right corner of the LCD screen.