CHAPTER 1

Configuring Basic Features for Cisco Unified Personal Communicator

June 4, 2013

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 want to continue with information specific to Cisco Unified Personal Communicator, proceed with the contents in this chapter;

REVIEW DRAFT—CISCO CONFIDENTIAL

REVIEW DRAFT—CISCO CONFIDENTIAL

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, page 1-7	• Assign the licensing capabilities on Cisco Unified Communications Manager. See the *Installation Guide for Cisco Unified Presence Release 8.6* for more information. • Configuring Firewalls to Pass Cisco Unified Personal Communicator Traffic, page 1-8
Availability status information and instant messaging	• (Cisco Unified Personal Communicator Release 8.x) Required XCP Services, page 1-9 • (Cisco Unified Personal Communicator Release 8.x) Optional XCP Services, page 1-9	• Verifying That the Cisco UP XCP Router Service Is Running, page 1-8 • Turning On Cisco Unified Presence Services to Support XMPP Clients, page 10-4 • (Cisco Unified Personal Communicator Release 8.x) Configuring Settings, page 1-22 • (Cisco Unified Personal Communicator Release 8.5) Configuring Chat History, page 1-11
Advanced instant messaging features, such as group chat and persistent chat rooms	• (Cisco Unified Personal Communicator Release 8.x) Optional XCP Services, page 1-9	• Configuring the Service Parameters for the IM Gateway, page 1-10 • (Cisco Unified Personal Communicator Release 8.x) Configuring Persistent Chat Rooms, page 1-10

REVIEW DRAFT—CISCO CONFIDENTIAL

To Deploy These Features...	Read These Topics...	Perform These Tasks...
Place calls from a computer	• Application Dialing and Directory Lookup Rules, page 1-11 • Transformation of Dialed Numbers by Cisco Unified Personal Communicator, page 1-12 • Cisco Unified Client Services Framework Device Type, page 1-13 • Extension Mobility Configuration, page 1-13 • (Cisco Unified Personal Communicator Release 8.x) Guidelines for Configuring the Softphone Device Name, page 1-14 • (Cisco Unified Personal Communicator Release 7.1) Guidelines for Configuring the Softphone Device Name, page 1-14 • TFTP Server Connection, page 1-20	• Creating a Softphone Device for Each Cisco Unified Personal Communicator User, page 1-15 • Associating Users with Softphone Devices, page 1-17 • Adding Users to User Groups, page 1-18 • Associating a New Device with a User, page 1-18 • Associating a New Device with a User, page 1-18 • Associating a New Device with a User, page 1-18 • Resetting a Device, page 1-19 • Configuring the Proxy Listener and TFTP Addresses, page 1-21 • (Cisco Unified Personal Communicator Release 8.x) Configuring Settings, page 1-22
Place calls from a desk phone	• Desk Phone Control and the CTI Connection Failures, page 1-26 • (Cisco Unified Personal Communicator Release 7.x) Desk Phone Control and LDAP TelephoneNumber Field, page 1-27	• Configuring CTI Gateway Server Names and Addresses, page 1-28 • Creating CTI Gateway Profiles, page 1-29

REVIEW DRAFT — CISCO CONFIDENTIAL

To Deploy These Features...	Read These Topics...	Perform These Tasks...
Video calls and videoconferencing	—	• Configuring Users for Point-to-Point Video Calls and for Multipoint Videoconferencing, page 1-30 • Configuring Videoconferencing Resources and Ad-Hoc Conferencing on Cisco Unified Communications Manager, page 1-31 • (Cisco Unified Personal Communicator Release 8.x) Connecting a Cisco Unified IP Phone to the Network and Your Computer, page 1-34 • (Cisco Unified Personal Communicator Release 8.x) Enabling Video for a Cisco Unified IP Phone, page 1-35 • (Cisco Unified Personal Communicator Release 8.x) Configuring Settings, page 1-22
Voicemail	• Secure Voicemail Messaging on Cisco Unity Connection, page 13-2 • Secure Voicemail Messaging on Cisco Unity, page 13-2 • Secure Voicemail Messaging Configuration, page 13-3	• Configuring Cisco Unity Connection Servers, page 13-4 • Configuring Cisco Unity Servers, page 13-6 • Configuring Voicemail Server Names and Addresses on Cisco Unified Presence, page 13-9 • Configuring Mailstore Server Names and Addresses on Cisco Unified Presence, page 13-9 • Creating Voicemail Profiles on Cisco Unified Presence, page 13-11 • (Cisco Unified Personal Communicator Release 8.x) Configuring Settings, page 1-22

REVIEW DRAFT — CISCO CONFIDENTIAL

To Deploy These Features...	Read These Topics...	Perform These Tasks...
Conference calls	• How to Configure Conferencing Servers for Cisco Unified Personal Communicator, page 13-12	• (Cisco Unified Personal Communicator Release 7.1) Configuring Cisco Unified MeetingPlace Express and Cisco Unified MeetingPlace Express VT Servers, page 13-13 • Configuring Cisco Unified MeetingPlace Servers, page 13-16 • (Cisco Unified Personal Communicator Release 8.x) Configuring the Cisco Unified MeetingPlace Web Server, page 13-18 • Configuring Conferencing Server Names and Addresses on Cisco Unified Presence, page 13-19) • Creating Conferencing Profiles on Cisco Unified Presence, page 13-21
Audio quality features	—	• (Cisco Unified Personal Communicator Release 8.x) Creating Audio Profiles on Cisco Unified Presence, page 13-23
Alternative server to control signing in	—	• Configuring CCMCIP Profiles for Cisco Unified Personal Communicator Release 8.x, page 13-24
Security features	—	• (Cisco Unified Personal Communicator Release 8.x) Configuring Settings, page 1-22
High availability features	• High Availability, page 1-21	• How To Configure High Availability Cisco Unified Presence Deployments, page 4-25
Third-party client applications	• (Cisco Unified Personal Communicator Release 8.x) Optional XCP Services, page 1-9	• About Configuring Third-Party Clients on Cisco Unified Presence, page 13-26

REVIEW DRAFT—CISCO CONFIDENTIAL

To Deploy These Features...	Read These Topics...	Perform These Tasks...
HTML content display	—	• (Cisco Unified Personal Communicator Release 8.5) Distributing HTML Files for Display in the Cisco Unified Personal Communicator Window, page 13-29
Desktop agent	• (Cisco Unified Personal Communicator Release 8.5) How to Use Cisco Unified Personal Communicator as a Desktop Agent, page 13-26	• Before You Start Cisco Unified Personal Communicator as a Desktop Agent, page 13-27 • Starting Cisco Unified Personal Communicator as a Desktop Agent, page 13-28

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 server for integration with Cisco Unified Presence
- Configured the Cisco Unified Presence server
- Configured the licensing details for Cisco Unified Personal Communicator
- Assigned all of your Cisco Unified Personal Communicator users to Cisco Unified Presence nodes in the system topology
- (Recommended) Configured the LDAP server
- (Optional) Configured the Cisco Unity and Cisco Unified MeetingPlace or Cisco WebEx on Cisco Unified Presence 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 the computers of your users, ensure that there are no other applications installed on the computers of your users 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

- Configuring Cisco Unified Communications Manager for Integration with Cisco Unified Presence, page 3-1
- Configuring a Cisco Unified Presence Server for Deployment in the Network, page 4-1
- Cisco Unified Personal Communicator License Requirements, page 2-1
- Integrating the LDAP Directory, page 13-1

Adding Licensing Capabilities for Users

For information about how to assign user capabilities, see the *Installation Guide for Cisco Unified Presence Release 8.6*.

Configuring 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 Cisco Unified 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

Verifying That the Cisco UP XCP Router Service Is Running

Procedure

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

Step 2   Select the server from the Server list box.

Step 3   Select **Go**.

Step 4   Locate the Cisco UP XCP Router service in the Cisco Unified Presence Services section.

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

REVIEW DRAFT—CISCO CONFIDENTIAL

Related Topic

(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 Cisco Unified Presence XCP services are running on all Cisco Unified Presence nodes in all clusters:

- Cisco UP XCP Authentication Service
- Cisco UP 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 Cisco Unified Presence XCP services are running on all Cisco Unified Presence nodes in all clusters:

- Cisco UP XCP Text Conference Manager, for group chat and persistent chat rooms. If you have a mixture of Cisco Unified Personal Communicator Release 8.x and Cisco Unified Personal Communicator Release 7.x users, then the Cisco UP XCP Text Conference Manager service must be running for them to communicate with one another.
- Cisco UP XCP Web Connection Manager, to manage connections for web-based client applications, that connect to Cisco Unified Presence using HTTP.
- Cisco UP XCP SIP Federation Connection Manager, to support federation services with third-party applications that use SIP.
- Cisco UP XCP XMPP Federation Connection Manager, to support federation services with third-party applications that use XMPP.
- Cisco UP XCP Counter Aggregator, if you want system administrators to be able to view statistical data on XMPP components.
- Cisco UP XCP Message Archiver, for automatic archiving of all instant messages.
- Cisco UP 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.

REVIEW DRAFT—CISCO CONFIDENTIAL

Related Topics

How to Configure Chat

Configuring the Service Parameters for the 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 Cisco Unified Presence IM Gateway for IM interoperability between SIP and XMPP clients.

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

Related Topics

(Cisco Unified Personal Communicator Release 8.x) 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 Cisco Unified Presence see the *Database Setup Guide for Cisco Unified Presence* at the following URL:

http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

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

When a Cisco Unified Personal Communicator user joins a persistent chat room, Cisco Unified Presence sends instant message history information to the Cisco Unified Personal Communicator user. The number of messages in instant message history that Cisco Unified 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 Cisco Unified 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 Cisco Unified Presence server.

REVIEW DRAFT—CISCO CONFIDENTIAL

Related Topics

- Turning On the Cisco Unified Presence Service, page 4-63
- Configuring Persistent Chat Room Settings, page 11-5

(Cisco Unified Personal Communicator Release 8.5) Disabling Chat

You can configure Cisco Unified Presence to disable the chat feature on Cisco Unified Personal Communicator. For information about how to disable chat, see Turning On or Off Instant Messaging for a Cisco Unified Presence Cluster, page 4-58.

Related Topic

Turning On or Off Instant Messaging for a Cisco Unified Presence Cluster, page 4-58

(Cisco Unified Personal Communicator Release 8.5) Configuring Chat History

You can configure Cisco Unified Presence 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 Cisco Unified Personal Communicator. For information about how to configure the chat history on Cisco Unified Presence, see Allowing Clients to Log Instant Message History, page 4-60.

Related Topic

Allowing Clients to Log Instant Message History, page 4-60

About Configuring Cisco Unified Personal Communicator on Cisco Unified Communications Manager

- Application Dialing and Directory Lookup Rules, page 1-11
- Transformation of Dialed Numbers by Cisco Unified Personal Communicator, page 1-12
- Cisco Unified Client Services Framework Device Type, page 1-13
- Extension Mobility Configuration, page 1-13
- (Cisco Unified Personal Communicator Release 8.x) Guidelines for Configuring the Softphone Device Name, page 1-14
- (Cisco Unified Personal Communicator Release 7.1) Guidelines for Configuring the Softphone Device Name, page 1-14

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. Cisco Unified 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.

- Cisco Unified Personal Communicator Release 7.1 does not remove the plus character from dialed numbers.

- Releases of Cisco Unified Personal Communicator earlier than Release 7.1 do remove the plus character from dialed numbers.

Table 1-1 defines the application dialing rules and directory lookup rules, and provides examples and the menu path for each.

Table 1-1   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 Communications Manager 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 Communications Manager 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 Topic

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 Cisco Unified 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.

REVIEW DRAFT—CISCO CONFIDENTIAL

Related Topics

- [Application Dialing and Directory Lookup Rules, page 1-11](#)

- For detailed conceptual and task-based information about dialing rules, see the *Cisco Unified Communications Manager Administration Guide*:

    [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 publisher server. After you apply the COP file, you must restart the Cisco Unified Communications Manager publisher server, and all other servers.

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 Communications Manager Administration by selecting **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

- [Creating a Softphone Device for Each Cisco Unified Personal Communicator User, page 1-15](#)

- *Cisco Unified Communications Manager Features and Services Guide*

(Cisco Unified Personal Communicator Release 8.x) Guidelines for Configuring the Softphone Device Name

When you create a softphone device for each Cisco Unified Personal Communicator Release 8.0 user, you select 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.

(Cisco Unified Personal Communicator Release 7.1) Guidelines for Configuring the Softphone Device Name

When you create a softphone device for each Cisco Unified Personal Communicator user, you must specify a device name. Make sure that the device name conforms to these guidelines:

- Derives from the username.
- Starts with *UPC*.
- Contains only uppercase letters, or numerals.
- Contains no more than 12 additional characters after *UPC*.

Table 1-2 provides some example device names.

Table 1-2   Username Conversion for Cisco Unified Personal Communicator Softphone Device

Cisco Unified Communications Manager Username	Associated Softphone Device Name
jjackson	UPCJJACKSON
johnnie_jackson	UPCJOHNNIEJACKS
johnniejackson	UPCJOHNNIEJACKS
john.jackson	UPCJOHNJACKSON

You must create username that do not collide when converted, for example, the usernames *johnnie_jackson* and *johnniejackson* convert to the same softphone device name and therefore are said to collide.

⚠️

Caution   If Cisco Unified Personal Communicator is unable to derive its softphone device name, it cannot properly register and cannot function as expected. You might have to reconfigure a user to use a name other than their normal username to avoid this problem.

Related Topic

Creating a Softphone Device for Each Cisco Unified Personal Communicator User, page 1-15

REVIEW DRAFT—CISCO CONFIDENTIAL

How to Configure Cisco Unified Personal Communicator on Cisco Unified Communications Manager

Creating a 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 Select **Cisco Unified Communications Manager Administration > Device > Phone**.

Step 2 Select **Add New**.

Step 3 (Cisco Unified Personal Communicator Release 8.x) Select **Cisco Unified Client Services Framework** from the Phone Type menu.

(Cisco Unified Personal Communicator Release 7.1) Select **Cisco Unified Personal Communicator** from the Phone Type menu.

Step 4 Select **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. (Cisco Unified Personal Communicator Release 8.x) Select **Default** from the Device Pool list.

d. (Cisco Unified Personal Communicator Release 8.x) Select **Standard Client Services Framework** from the Phone Button Template list.

e. Configure all the required fields for your environment.

f. Select the user ID from Owner User ID menu.

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

h. (Cisco Unified Personal Communicator Release 8.x) Check **Allow Control of Device from CTI** to enable CTI to control and monitor this device.

(Cisco Unified Personal Communicator Release 7.1) Uncheck **Allow Control of Device from CTI**.

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

Field	Setting
Presence Group	Select **Standard Presence Group**.
Device Security Profile	(Cisco Unified Personal Communicator Release 8.0) Select **Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile**. (Cisco Unified Personal Communicator Release 7.1) Select **Cisco Unified Personal Communicator - Standard SIP Non-Secure Profile**.
SIP Profile	Select **Standard SIP Profile** to specify the default SIP profile. SIP profiles provide specific SIP information for the phone such as registration and keep-alive timers, media ports, and Do Not Disturb control.
Digest User	Select the user ID. This is the same user ID as the one you selected for Owner User ID.

Step 6 Select **Save**.

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

Step 8 Configure the following information:

a. Enter the directory number and route partition for 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 Select **Save**.

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

REVIEW DRAFT—CISCO CONFIDENTIAL

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. Select **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.

Related Topics

- (Cisco Unified Personal Communicator Release 7.1) Guidelines for Configuring the Softphone Device Name, page 1-14
- Cisco Unified Personal Communicator License Requirements, page 2-1
- Extension Mobility Configuration, page 1-13
- Configuring Videoconferencing Resources and Ad-Hoc Conferencing on Cisco Unified Communications Manager, page 1-31

What To Do Next

- Associating Users with Softphone Devices, page 1-17

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

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

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

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

Step 5   Select **Cisco Unified Communications Manager Administration > Device > Phone**.

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

Step 7   Select the name of the device.

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

R E V I E W   D R A F T — C I S C O   C O N F I D E N T I A L

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

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

Step 11   Select the user, then select **Add Selected**.

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

What To Do Next

Adding Users to User Groups

Procedure

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

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

Step 3   Select the user.

Step 4   Select **Add to User Group** in the Permissions Information section.

Step 5   Use the Find and List User Groups window to find and select the following user 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, select the following user group also:

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

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

- Standard CTI Allow Control of Phones supporting Rollover Mode

Step 6   Select **Add Selected**.

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

What To Do Next

Associating a New Device with a User

Procedure

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

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

Step 3   Select the user.

REVIEW DRAFT—CISCO CONFIDENTIAL

Step 4   Select **Device Association** in the Device Information section.

Step 5   Search for the device in the User Device Association window.

Step 6   Select the device.

Step 7   Select **Save Selected/Changes**.

Step 8   Select **Back to User** from the menu in the Related Links navigation box at the top right of the window.

Step 9   Select **Go**.

Step 10   Verify that the device is listed in the Device Information section on the End User Configuration window.

What To Do Next

- Resetting a Device, page 1-19

Resetting a Device

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

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

Step 3   Select the name of the device.

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

Step 5   Select **Reset** on the Directory Number Configuration window.

Specifying Which Softphone Device to Use for a 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.

REVIEW DRAFT—CISCO CONFIDENTIAL

About Configuring Cisco Unified Personal Communicator on Cisco Unified Presence

TFTP Server Connection

Cisco Unified Personal Communicator connects to the primary Trivial File Transfer Protocol (TFTP) server (whose address is retrieved from Cisco Unified 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 Presence Administration.

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

	Release 8.x	**Release 7.1**
Windows XP	*drive*:\Documents and Settings*username*\Local Settings\Application Data\Cisco\Unified Communications\Client Services Framework\Config	*drive*:\Documents and Settings*username*\Application Data\Cisco\Unified Personal Communicator
Windows Vista		*drive*:\Users*username*\AppData\Local\ Cisco\Unified Personal Communicator

- 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.

REVIEW DRAFT—CISCO CONFIDENTIAL

- 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 Topic

Configuring the Proxy Listener and TFTP Addresses, page 1-21

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 7.*x* with Cisco Unified Presence Release 7.*x*

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

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

To configure high availability for Cisco Unified Personal Communicator clients, you configure high availability on the Cisco Unified Presence server. For more information, refer to How To Configure High Availability Cisco Unified Presence Deployments, page 4-25.

The impact of failover on Cisco Unified Personal Communicator is described in Impact of Failover to Cisco Unified Presence Clients and Services, page 4-16.

How to Configure Cisco Unified Personal Communicator on Cisco Unified Presence

- Configuring the Proxy Listener and TFTP Addresses, page 1-21 (required)

- (Cisco Unified Personal Communicator Release 8.x) Configuring Settings, page 1-22

- (Cisco Unified Personal Communicator Release 7.1) Configuring the Service Parameters, page 1-24 (required)

- (Cisco Unified Personal Communicator Release 7.1) Configuring a Secure Connection Between Cisco Unified Presence and Cisco Unified Personal Communicator, page 1-25

Configuring the Proxy Listener and TFTP Addresses

Before You Begin

- Read the TFTP server connection topic.

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

Restriction

We recommend that Cisco Unified Personal Communicator use TCP to communicate with the proxy server. If you use UDP to communicate with the proxy server, availability information for contacts in the Cisco Unified Personal Communicator contact list might not be available for large contact lists.

Procedure

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

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

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

Step 4   Select **Save**.

Troubleshooting 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 Topic

What To Do Next

(Cisco Unified Personal Communicator Release 8.x) Configuring Settings

Procedure

Step 1   Select **Cisco Unified Presence Administration** > **Application** > **Cisco Jabber** > **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
Credentials source for voicemail service	If user credentials for the voicemail service are shared with another service, select the appropriate service from this list box. The user credentials automatically synchronize from the service that you select. Default Setting: Not set **Troubleshooting Tip** If this value is set to Not set, users must use their client preference settings to manually select a source for voicemail service credentials.
Credentials source for web conferencing service	If user credentials for the meeting service are shared with another service, select the appropriate service from this list box. The user credentials automatically synchronize from the service that you select. Default Setting: Not set **Troubleshooting Tip** If this value is set to Not set, users must use their client preference settings to manually select a source for meeting service credentials.

REVIEW DRAFT—CISCO CONFIDENTIAL

Field	Setting
Maximum message size	Enter the allowed size limit for instant messages, in bytes.
Allow cut & paste in instant messages	Check this check box to allow users to cut and paste in their instant messages (IMs).
	Most deployments have this option turned on. If you turn off this option, the Cisco Unified Presence server flags and passes the setting to the Cisco Unified Personal Communicator client, where the behavior is enforced.
	Default Setting: On
Always begin calls with video turned off	Check this check box if you want all video calls to start without sending video from the camera. Instead, an icon is displayed that indicates that video is not being sent from the camera. If users want to send video from their camera, they must explicitly select to send video from the camera.
	This setting overrides the Start video calls with my video signal muted setting that users can select in the Cisco Unified Personal Communicator options.
	If you turn this option off, video calls start according to the Cisco Unified Personal Communicator options.
	Default Setting: Off

Step 3   Select **Save**.

Related Topics

- How to Integrate the LDAP Directory with Cisco Unified Personal Communicator, page 13-8
- (Cisco Unified Personal Communicator Release 8.0) How to Integrate the LDAP Directory for Contact Searches on XMPP Clients, page 13-14

(Cisco Unified Personal Communicator Release 7.1) Configuring the Service Parameters

You need to configure all the availability-related notifications sent between Cisco Unified Personal Communicator and Cisco Unified Presence use TCP.

Procedure

Step 1   Select **Cisco Unified Presence Administration** > **System** > **Service Parameters**.

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

Step 3   Select **Cisco UP SIP Proxy** as the service on the Service Parameter Configuration window.

Step 4   Set **Use Transport in Record-Route Header** to **On** in the SIP Parameters (Clusterwide) section.

This forces the Proxy to use the transport parameter in the record-route header.

Step 5   Select **Save**.

Related Topic

Configuring the Proxy Listener and TFTP Addresses, page 1-21

What To Do Next

(Cisco Unified Personal Communicator Release 7.1) Configuring a Secure Connection Between Cisco Unified Presence and Cisco Unified Personal Communicator, page 1-25

(Cisco Unified Personal Communicator Release 7.1) Configuring a Secure Connection Between Cisco Unified Presence and Cisco Unified Personal Communicator

If you want to exchange a CA-signed certificate between Cisco Unified Presence and Cisco Unified Personal Communicator, you must generate a Certificate Signing Request (CSR) and import a tomcat certificate for Cisco Unified Presence. Refer to the steps below for a high level overview of this process.

Cisco Unified Personal Communicator uses the certificate called tomcat. The trust chain for this certificate is called tomcat-trust. Note that there can only be one tomcat certificate, but there can be more than one tomcat-trust.

Procedure

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

Step 2   Select **Find** to list all certificates.

Step 3   Select the tomcat certificate.

Step 4   Select **Generate CSR**.

Step 5   Send your CSR to your Certificate Authority (CA).

Step 6   Upload the signing chain of the certificate one at a time as "tomcat-trust" on Cisco Unified Presence. You will need to do this before you upload the signed certificate that you receive from your CA. If you receive a Geotrust (Equifax) or Verisign certificate, you just need to upload the appropriate root certificate.

Step 7   When the CA returns your signed certificate, select **Cisco Unified OS Administration > Security > Certificate Management > Upload Certificate** to upload the signed certificate to Cisco Unified Presence.

Step 8   Upload the signed certificate as 'tomcat'. Make sure to save this certificate file. List the name of your signing certificate as the 'Root Certificate'.

Step 9   Restart the Tomcat service from the CLI using this command:

```
utils service restart Cisco Tomcat
```

The new certificate is not valid until you restart the Tomcat service .

REVIEW DRAFT—CISCO CONFIDENTIAL

Troubleshooting Tips

*   When you generate the CSR, we recommend that you backup your system using the Disaster Recovery System on Cisco Unified Presence. If you do not backup your system, and you regenerate the tomcat certificate, you will invalidate your signing chain and you will no longer be able to use your signed certificate.

*   If you have an internal CA, in a signing chain, there will be at least a trusted root certificate. The trusted root certificate may sign an intermediate certificate, or may sign your certificate directly. If there is an intermediate certificate, then it will sign your certificate. The root and the intermediate certificate make up the "signing chain". You need to upload each of the certificates in the chain to Cisco Unified Presence. In each case, upload the certificate as "tomcat-trust".

*   Do not attempt to upload a PKCS#7 (concatenated certificate chain), sometimes called a 'p7b'.

*   You should only upload public keys. Do not upload a PKCS#12.

Related Topic

Disaster Recovery System Administration Guide for Cisco Unified Presence

What To Do Next

About Configuring CTI Gateway Settings for Desk Phone Control on Cisco Unified Presence

Note   The procedures in this topic are only applicable if you are configuring Cisco Unified Personal Communicator for desk phone control.

*   Desk Phone Control and the CTI Connection Failures, page 1-26
*   (Cisco Unified Personal Communicator Release 7.x) Desk Phone Control and LDAP TelephoneNumber Field, page 1-27

Desk Phone Control and the 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 servers. Connection attempts continue on a round-robin basis, beginning again with the primary server. Successive attempts to reconnect to a server occur at intervals of 4, 8, 16, 32, and 60 seconds (maximum) until a connection is re-established.

REVIEW DRAFT—CISCO CONFIDENTIAL

Table 1-3   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.
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 server (whether primary or backup) until the user relaunches Cisco Unified Personal Communicator or when a connection failure causes it to reconnect.

Related Topics

(Cisco Unified Personal Communicator Release 7.x) Desk Phone Control and LDAP TelephoneNumber Field

You may need to index the telephoneNumber field on the LDAP server for desk phone control to work. There are two possible scenarios that this applies to:

• Desk phone control is not working, and the server health on Cisco Unified Personal Communicator displays the status "Not Connected - Stopped".

• The contact search on Cisco Unified Personal Communicator does not return the full results.

These issues could occur when you have a large Cisco Unified Personal Communicator user base, and the LDAP server is slow to respond to queries from Cisco Unified Presence. To fix the issue, index the telephoneNumber field on the LDAP server. Alternatively, if you use Windows Active Directory, change the Global Catalog port to 3268 (instead of using the standard LDAP port 389).

How to Configure CTI Gateway Settings for Desk Phone Control on Cisco Unified Presence

Configuring 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 Communications Manager Administration** > **System > Server** menu. Cisco Unified Presence dynamically creates a TCP-based CTI gateway host profile for that address, and automatically populates the CTI gateway fields on Cisco Unified 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   Select **Cisco Unified Presence Administration** > **Application > Cisco Jabber > CTI Gateway Server**.

Step 2   Select **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   Select **Save**.

REVIEW DRAFT—CISCO CONFIDENTIAL

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).

Related Topics

- User and Device Configuration on Cisco Unified Communications Manager, page 3-2
- Desk Phone Control and the CTI Connection Failures, page 1-26

What To Do Next

Creating CTI Gateway Profiles, page 1-29

Creating CTI Gateway Profiles

You must create CTI gateway profiles in Cisco Unified 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 select the servers as primary or backup servers in this procedure.

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

Step 2   Select **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	Select 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 Cisco Unified 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   Select **Add Users to Profile**.

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

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

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

Related Topics

- Configuring CTI Gateway Server Names and Addresses, page 1-28
- Desk Phone Control and the CTI Connection Failures, page 1-26

How to Configure Video Calls and Videoconferencing

Configuring Users for Point-to-Point Video Calls and for Multipoint Videoconferencing

Procedure

Step 1   (Cisco Unified Personal Communicator Release 7.1) For point-to-point video calls, configure users for softphone use.

Step 2   (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 3   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.

- 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 4   Provide users with the appropriate documentation to complete the installation.

Related Topics

- 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

What To Do Next

Configuring Videoconferencing Resources and Ad-Hoc Conferencing on Cisco Unified Communications Manager

Using 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 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.

REVIEW DRAFT—CISCO CONFIDENTIAL

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.	
Add the licensing information.	**Maintenance > Licenses > Install Licenses**

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. Select the device, then select 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. Select **Cisco Unified CM Administration > System > Service Parameters** in Cisco Unified Communications Manager Administration.

b. Select your Cisco Unified Communications Manager server from the Server drop-down list.

c. Select **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. Select **Save**.

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

   a. Select **Cisco Unified CM Administration > Device > Phone**.

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

   c. 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.

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

   e. Select **Save**.

   f. Select **Reset**.

Related Topics

- For details about the Cisco Unified Videoconferencing server installation, see the product installation guide:

   http://www.cisco.com/en/US/products/hw/video/ps1870/tsd_products_support_series_home.html

- For detailed instructions about media resource configuration for Cisco Unified Videoconferencing, 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

- For details about supported Cisco Unified Videoconferencing releases, see the *Release Notes for Cisco Unified Personal Communicator*:

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

- For detailed Cisco Unified MeetingPlace configuration instructions, see the *Administration Documentation for Cisco Unified MeetingPlace*:

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

- For detailed Cisco Unified Communications Manager 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

Configuring 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) How to Configure Cisco Unified IP Phones 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).

To configure a Cisco Unified IP Phone for video, you must perform the following tasks:

-
-

(Cisco Unified Personal Communicator Release 8.x) Connecting a Cisco Unified IP Phone to the 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

Chapter 1   Configuring Basic Features for Cisco Unified Personal Communicator

How to Configure Video Calls and Videoconferencing

(Cisco Unified Personal Communicator Release 8.x) Enabling Video for a Cisco Unified IP Phone

Procedure

Step 1   Select **Device > Phone** in Cisco Unified Communications Manager 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   Select **Enabled** from the **PC Port** drop-down list.

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

Step 7   Select **Save**.

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

Book Title

OL-xxxxx-xx

1-35