Cisco Unified Personal Communicator Administration on IM and Presence Service, Release 10.0(1)

First Published: December 03, 2013

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

Text Part Number: OL-30821-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2013 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface ix

Purpose ix

Audience ix

Organization ix

Related documentation xi

Conventions xii

Obtain support xii

CHAPTER 1

License configuration for this integration 1

User license requirements 1

CHAPTER 2

Cisco Unified Personal Communicator 3

Pre-deployment tasks 4

Applications dependent on Cisco Unified Client Services Framework 4

Cisco Unified Video Advantage 4

IM and Presence node discovery 4

Automatic server discovery 4

Default address for IM and Presence node 5

Location of registry key 6

Cisco Unified Personal Communicator deployment 6

Executable file 7

Windows Installer (MSI) file 7

Software download site and installer package names 8

Deployment options 9

Automated mass deployment 9

Standalone installation 9

Deploy the application 10

(Cisco Unified Personal Communicator Release 8.5 and Earlier) deploying application in Mac OS environment 10
Deploy application and camera drivers in Microsoft Windows environment 10
Install security certificates on client computers for Client Services Framework (CSF) 11
Enable availability status for Microsoft Office 2010 users 12
Upgrade application 13
Headsets and other audio devices 13
Third-party headsets with Cisco Unified Personal Communicator 14
Do Not Disturb feature in Cisco Unified Personal Communicator 14
Information to provide to users 16
Troubleshooting 18
Cisco Unified Personal Communicator fails to start or starts with black background with no visible controls 18
Limitations creating group chats 19
Cannot place or receive calls after secure profile enabled 20
Error connecting to CSF device 20

CHAPTER 3 **Basic feature configuration for Cisco Unified Personal Communicator 23**
Roadmap for deploying Cisco Unified Personal Communicator 24
Prerequisites for integrating Cisco Unified Personal Communicator 26
Configure firewalls to pass Cisco Unified Personal Communicator traffic 27
Verify Cisco XCP Router service is running 28
(Cisco Unified Personal Communicator Release 8.x) about configuring XCP services for Cisco Unified Personal Communicator 28
(Cisco Unified Personal Communicator Release 8.x) required XCP services 28
(Cisco Unified Personal Communicator Release 8.x) optional XCP services 28
Chat configuration 29
Service parameter configuration for IM Gateway 29
Configuring persistent chat rooms 29
(Cisco Unified Personal Communicator Release 8.5) disabling chat 30
(Cisco Unified Personal Communicator Release 8.5) configuring chat history 30
Cisco Unified Personal Communicator configuration on Cisco Unified Communications Manager 30
Application dialing and directory lookup rules 30
Transformation of dialed numbers by Cisco Unified Personal Communicator 31

Cisco Unified Client Services Framework device type 32
Extension Mobility configuration 32
(Cisco Unified Personal Communicator Release 8.x) guidelines for configuring softphone device name 33
Desk phone control and CTI connection failures 33
Configure CTI Gateway server names and addresses 34
Create CTI Gateway profiles 35
Cisco Unified Personal Communicator configuration on Cisco Unified Communications Manager 37
Create softphone device for each Cisco Unified Personal Communicator user 37
Associate users with softphone devices 39
Add users to access control groups 40
Associate new device with a user 41
Reset device 41
Specify softphone device for user with multiple associated softphone devices 41
About Cisco Unified Personal Communicator configuration on IM and Presence 42
TFTP server connection 42
High Availability 43
Cisco Unified Personal Communicator configuration on IM and Presence 43
Configure TFTP addresses 43
(Cisco Unified Personal Communicator Release 8.x) configure settings 44
Video calls and Videoconferencing configuration 46
Configure users for point-to-point video calls and for multipoint videoconferencing 46
Configure videoconferencing resources and Ad-Hoc conferencing on Cisco Unified Communications Manager 47
Configure bandwidth capability for Cisco Unified Personal Communicator 48
(Cisco Unified Personal Communicator Release 8.x) Cisco Unified IP phones configuration for video 49
(Cisco Unified Personal Communicator Release 8.x) connect Cisco Unified IP phone to network and your computer 49
(Cisco Unified Personal Communicator Release 8.x) Enable video for Cisco Unified IP phone 50

CHAPTER 4 **Voicemail, conferencing, and other features for Cisco Unified Personal Communicator 51**
Voicemail server configuration for Cisco Unified Personal Communicator 52

Configure Cisco Unity Connection servers 52
Configure Cisco Unity servers 54
Conferencing server configuration for Cisco Unified Personal Communicator 56
Conferencing servers for Cisco Unified Personal Communicator 56
Configure Cisco Unified MeetingPlace Servers 56
(Cisco Unified Personal Communicator Release 8.x) configure Cisco Unified MeetingPlace web server 58
Add custom Cisco Unified MeetingPlace template files to Cisco Unified MeetingPlace7.x web server 58
(Cisco Unified Personal Communicator Release 8.5) Cisco Webex server configuration 59
Single sign-on configuration for Cisco Webex and Cisco Unified MeetingPlace 59
Configure CCMCIP profiles for Cisco Unified Personal Communicator release 8.x 59
Third-Party client configuration on IM and Presence 61
(Cisco Unified Personal Communicator Release 8.5) Cisco Unified Personal Communicator as desktop agent 62
Cisco Unified Personal Communicator running as desktop agent 62
Configure Cisco Unified Personal Communicator as desktop agent 62
Start Cisco Unified Personal Communicator as desktop agent 63
Stop Cisco Unified Personal Communicator as desktop agent 63
(Cisco Unified Personal Communicator Release 8.5) Distribute HTML files for display in Cisco Unified Personal Communicator window 64
User configuration update after deploying Cisco Unified Personal Communicator 65
Application profiles 65
Change application profiles for single user 65
Change application profiles for multiple users 66
New user configuration for full Cisco Unified Personal Communicator functionality 67

CHAPTER 5 **Active directory configuration for Cisco Unified Personal Communicator 69**
Feature comparison of enhanced and basic directory integration 70
Cisco Unified Client Services Framework integration with Active Directory 71
Mapping keys required for Basic and Enhanced Directory integration 72
Enhanced Directory Integration 73
Automatic discovery of directory service 73
Directory servers that cannot be discovered automatically 74
Connections to Global Catalog servers or domain Controllers 74

Usage of SSL 74
Usage of SSL for users not part of your domain 75
Usage of Windows credentials 75
Usage of non-Windows credentials 75
Topics to consider before you use Enhanced Directory Integration 75
Enhanced Directory Integration configuration with Active Directory 76
Default configuration of Active Directory with Enhanced Directory Integration 76
Connection configuration for Enhanced Directory Integration 77
Default values for directory attributes 80
Additional directory attribute configuration 81
Active Directory attributes that must be Indexed 82
Sample configuration questions 82
Basic Directory Integration 84
Use Active Directory Group Policy administrative template to configure Client Services Framework clients 84
Deploy Group Policy administrative templates in a Windows Server 2003 environment 85
Deploy Group Policy administrative templates in a Windows Server 2008 environment 86
Registry location on client machines 86
LDAP registry settings 87
Phone number masks 92
Elements of phone number masks 92
Subkey names for specifying masks 94
Contact photo retrieval 94
Binary photos retrieval from Active Directory 95
Static URL retrieval from Active Directory 95
Dynamic URL retrieval from Active Directory 95

CHAPTER 6 **Additional registry keys configuration for Cisco Unified Personal Communicator 97**
Registry key mapping 98
Video registry setting configuration 98
CTI registry setting configuration 98
Web conferencing registry setting configuration 98
Dial via Office registry setting configuration 99
Additional registry setting configuration 99

Preface

- Purpose, page ix
- Audience, page ix
- Organization, page ix
- Related documentation, page xi
- Conventions, page xii
- Obtain support, page xii

Purpose

The purpose of this document is to provide the necessary information for administering Cisco Unified Personal Communicator on Cisco Unified Communications Manager IM and Presence Service.

Audience

This document is intended for administrators of Cisco Unified Personal Communicator.

Organization

Module	This Module Describes...	Notes
Licensing	• Licensing requirements for Cisco Unified Presence and Cisco Unified Personal Communicator	• This is required configuration

Module	This Module Describes...	Notes
	• This module describes how to configure Cisco Unified Personal Communicator Release 8.x and Cisco Unified Personal Communicator Release 7.x • Instructions to configure Cisco Unified Personal Communicator on Cisco Unified Communications Manager • Instructions to configure Cisco Unified Personal Communicator on Cisco Unified Presence • Configuring firewalls to pass Cisco Unified Personal Communicator traffic • Configuring users for point-to-point video calls and for multipoint video conferencing	• This module is only required if you are deploying Cisco Unified Personal Communicator
Deploying and Upgrading Cisco Unified Personal Communicator	• Instructions on deploying and upgrading Cisco Unified Personal Communicator • Information on installation and use of headsets and other audio devices	• This module is only required if you are deploying Cisco Unified Personal Communicator

Module	This Module Describes...	Notes
Additional Deployment Information for Cisco Unified Personal Communicator	• Instructions to configure the voicemail servers for Cisco Unified Personal Communicator • Instructions to configure the conferencing servers for Cisco Unified Personal Communicator • Instructions to configure the video conferencing resources on Cisco Unified Communications Manager • Updating user configuration after deploying Cisco Unified Personal Communicator	• This module describes optional configuration if you are deploying Cisco Unified Personal Communicator
Configuring Active Directory for Cisco Unified Personal Communicator	• Information about Active Directory and its related mechanisms	• This module is only required if you are deploying Cisco Unified Personal Communicator
Configuring Additional Registry Keys for Cisco Unified Personal Communicator	• Customizations available through registry key settings	• This module is only required if you are deploying Cisco Unified Personal Communicator

Related documentation

Cisco Unified Presence Solution Reference Network Design (SRND) Document:

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

Cisco Unified Presence Compatibility Matrices and Port List:

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

Cisco Unified Presence Release Notes:

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

Cisco Unified Communications Manager Documentation:

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

Cisco Unified Personal Communicator Documentation:

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

Conventions

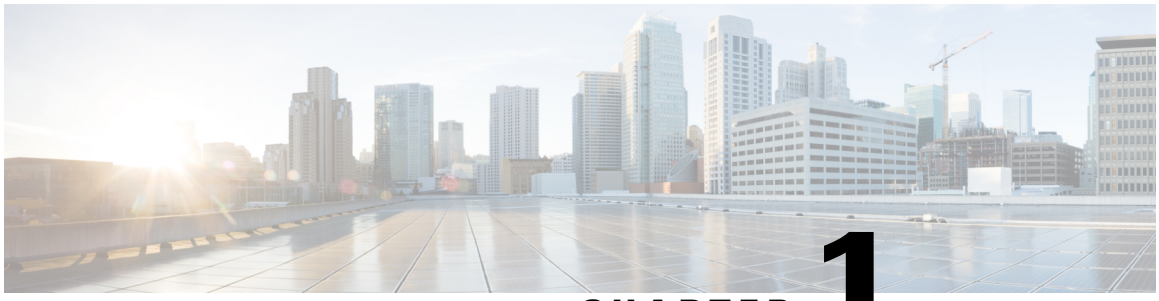
This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
[]	Elements in square brackets are optional.
{x | y | z}	Alternative keywords are grouped in braces and separated by vertical bars.
string	A non-quoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
^	The symbol ^ represents the key labeled Control - for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.

Obtain support

For information about obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html



CHAPTER 1

License configuration for this integration

- User license requirements, page 1

User license requirements

The IM and Presence Service does not require a node license or software version license. However, you must assign the IM and Presence Service to each IM and Presence Service user.

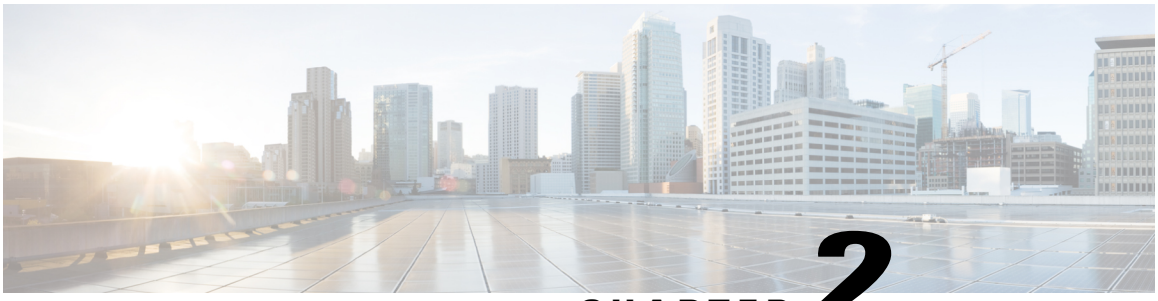
You can assign IM and Presence on a per user basis, regardless of the number of clients you associate with each user. When you assign IM and Presence to a user, this enables the user to send and receive IMs and also to send and receive presence updates. If the user is not enabled for IM and Presence, no presence updates are allowed for that user.

You can enable a user for IM and Presence in the **End User Configuration** window in Cisco Unified Communications Manager. See the *Cisco Unified Communications Manager Administration Guide* for more information.

IM and Presence capabilities are included within both User Connect Licensing (UCL) and Cisco Unified Workspace Licensing (CUWL). Refer to the *Cisco Unified Communications Manager Enterprise License Manager User Guide* for more information.

Related Topics

Create softphone device for each Cisco Unified Personal Communicator user, on page 37



CHAPTER 2

Cisco Unified Personal Communicator

This chapter includes the information required to deploy and upgrade 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:

- Pre-deployment tasks, page 4
- Cisco Unified Personal Communicator deployment, page 6
- Deploy the application, page 10
- Upgrade application, page 13
- Headsets and other audio devices, page 13
- Third-party headsets with Cisco Unified Personal Communicator, page 14
- Do Not Disturb feature in Cisco Unified Personal Communicator, page 14
- Information to provide to users, page 16
- Troubleshooting, page 18

Pre-deployment tasks

Applications dependent on Cisco Unified Client Services Framework

Before you deploy Cisco Unified Personal Communicator to the computers of your users, ensure that there are no other applications that depend on Cisco Unified Client Services Framework installed on the computers.

Cisco Unified Video Advantage

If Cisco Unified Video Advantage is installed on a client computer, you must uninstall it before you can install Cisco Unified Personal Communicator. If you do not uninstall Cisco Unified Video Advantage, you are prompted to do so during the Cisco Unified Personal Communicator installation.

Tip If you are performing a mass deployment of Cisco Unified Personal Communicator, you can use a software deployment tool to silently uninstall Cisco Unified Video Advantage from client computers prior to the installation.

IM and Presence node discovery

Cisco Unified Personal Communicator release 8.5(2) supports two types of server discovery: automatic discovery of IM and Presence nodes and manually setting the default address of the IM and Presence node. Prior to release 8.5(2), administrators were required to push the node address to a client through a registry key or clients had to manually enter the node address on the logon screen. Cisco Unified Personal Communicator release 8.5(2) enables administrators to choose the method of node discovery they desire.

Automatic server discovery

Cisco Unified Personal Communicator release 8.5(2) can use DNS SRV lookup to automatically find the IM and Presence server in the client's Active Directory domain. Automatic discovery of a user's home node is achieved through a combination of DNS lookup and the login redirect feature on IM and Presence. For more information about the redirect feature, see Cisco Unified Personal Communicator sign-in and redirect.

The DNS SRV records details about a particular service on a network. A DNS administrator can map many hosts to the same service name. It is also possible for a DNS administrator to provide load balancing by enabling the round robin option on their DNS server. This ensures that a different server is returned each time an SRV request is made.

A prerequisite of Cisco Unified Personal Communicator being able to perform DNS SRV lookups is that an administrator adds a DNS SRV record for the service name _cuplogin in the DNS server based on the IM and Presence server domain name.

The example below assumes the service name to be _cuplogin and the IM and Presence server domain name to be company.com. In this case, the SRV record defined within the DNS server catering to the domain company.com would be _cuplogin._tcp.company.com. This is an example of a DNS SRV query.

```
_cuplogin._tcp.company.comServer: dns_server.company.com
Address: 10.10.1.10
_cuplogin._tcp.company.com SRV service location:
 priority =0
 weight =0
 port =8443
 srv hostname =cupserver.company.com
 internet address =10.53.56.57
```

Note Cisco Unified Personal Communicator does not use the port mapped in the SRV record. Port 8443 is the default port used.

The DNS SRV record on Cisco Unified Personal Communicator is populated automatically by Cisco Unified Personal Communicator based on the service name and the domain name (connection specific suffix if not Active Directory domain) used by the user upon login.

For example, if the user and IM and Presence node have the same domain name, <company>.com, the IM and Presence node address is cupserver.company.com. The administrator defines the SRV record as _cuplogin._tcp.company.com within the enterprise resolving to cupserver.company.com. Cisco Unified Personal Communicator release 8.5(2) automatically populates the SRV record _cuplogin._tcp.company.com to perform an SRV lookup. If the user logs into a domain different from the IM and Presence domain, you must follow the steps in Location of registry key, on page 6.

When using the DNS SRV feature, Cisco Unified Personal Communicator release 8.5(2) and later uses the following logic:

1. At startup, Cisco Unified Personal Communicator looks up the IM and Presence node address within its local cache. Note that the local cache only exists if the user logged into IM and Presence successfully at least once.
2. If the IM and Presence node address can not be retrieved from the local cache, the local registry is checked. The registry may contain either a host address or a domain hint.
3. If the local registry does not have an address, Cisco Unified Personal Communicator does a DNS SRV query. If the DNS SRV query fails, a DNS A query is performed.
4. After a successful login, Cisco Unified Personal Communicator ensures that the IM and Presence node address is used for subsequent logins. If a user's home node is different IM and Presence node, the original IM and Presence node is capable of redirecting Cisco Unified Personal Communicator to the uses's home IM and Presence node. Successful login will result in Cisco Unified Personal Communicator updating the local cache with the new node address so that redirect only happens once.

Note Steps 2 through 4 above only apply to first-time logins and rare cases.

Default address for IM and Presence node

Cisco Unified Personal Communicator release 8.5(2) continues to support node identification through manual entry or a registry key pushed to the client. You can use the CUPServer registry value name to set this address and the data type is string or REG_SZ. This can be used for two purposes:

Procedure

Step 1 If a user's domain (connection specific suffix if not Active Directory domain) is different from that of the IM and Presence domain and if Cisco Unified Personal Communicator is required to discover IM and Presence node address using DNS SRV lookup, a domain hint needs to be entered. For example, a user's domain is company.com, the IM and Presence node's domain is cupdomain.company.com, and the IM and Presence node address is cupserver.cupdomain.company.com. The administrator defines the SRV record _cuplogin._tcp.cupdomain.company.com within the enterprise resolving to cupserver.cupdomain.company.com. In this case, the registry key should contain cupdomain.company.com to request that Cisco Unified Personal Communicator populate _cuplogin._tcp.cupdomain.company.com and NOT _cuplogin._tcp.company.com.

Step 2 You want to use the auto discovery mechanism and deploy Cisco Unified Personal Communicator release 8.5(2) with a plain IM and Presence node address within the cluster.

Caution IM and Presence release 9.0(1) and higher supports both intracluster and intercluster user login redirect. The mechanism above does not support any form of load balancing. As a result, the administrator is expected to plan Cisco Unified Personal Communicator rollout effectively with the goal of not overwhelming a single node with login requests. Overwhelming a single node with login requests may result in failure of critical services on IM and Presence.

To deploy this change to the computers in your Cisco Unified Personal Communicator system, you can use a software management system. Supported software management systems include Active Directory Group Policy, Altiris, and Microsoft System Management Server (SMS).

Location of registry key

You can specify the CUPServer registry value name in the following registry key:

HKEY_CURRENT_USER\Software\Cisco Systems, Inc.\Client Services Framework\AdminData

If you use Active Directory Group Policy to configure Cisco Unified Personal Communicator, then the CUPServer information is specified in the following registry key:

HKEY_CURRENT_USER\Software\Policies\Cisco Systems, Inc.\Client Services Framework\AdminData

Note

- If CUPServer information is present in both of these registry keys, the policies configuration data takes precedence.
- Cisco Unified Personal Communicator reads only HKEY_CURRENT_USER keys. Cisco Unified Personal Communicator does not read HKEY_LOCAL_MACHINE keys.

Cisco Unified Personal Communicator deployment

The Cisco Unified Personal Communicator installation application installs the following components:

- User interface for Cisco Unified Personal Communicator.
- The client-related components of the Cisco Unified Client Services Framework.

- Click to Call add-on (optional).
- Microsoft Office Integration add-on (optional).

The Cisco Unified Personal Communicator application is provided in two separate installation formats as follows:

- Cisco Unified Personal Communicator executable file.
- Cisco Unified Personal Communicator Windows Installer (MSI) file.

This section describes the installation formats and the deployment options.

Executable file

Users can run the executable file on their own computers. The executable file includes the prerequisite software for the application, as follows:

- Microsoft .NET Framework 3.5 Service Pack 1 (installer stub)
- Microsoft Visual C++ 2005 Redistributable Package (x86)
- Additional software required for Click to Call functionality:
  - Microsoft Office 2003 Primary Interop Assemblies (for machines with Office 2003)
  - Microsoft Office 2007 Primary Interop Assemblies (for machines with Office 2007)
  - Microsoft Visual 2005 Tools for Office Second Edition Runtime (x86)

Cisco Unified Personal Communicator checks if the prerequisite software is installed on the computer and if not, it automatically installs the prerequisites. To save time during the installation process, we recommend that you install the prerequisite software in advance of installing Cisco Unified Personal Communicator. All of the prerequisite software is available from the Microsoft website.

Note If the minimum required version of .NET Framework is not installed on the computer, Cisco Unified Personal Communicator runs the installer stub provided for that application. The installer stub downloads the .NET Framework software from the Microsoft website. This action requires Internet access and takes a considerable amount of time. We recommend that you install the required release of Microsoft .NET Framework in advance of the Cisco Unified Personal Communicator installation to save time and avoid any Internet access issues.

Windows Installer (MSI) file

You can use a software management system to push the Windows Installer (MSI) file to the computers of your users. The MSI file does not contain any of the prerequisite software that is required for Cisco Unified Personal Communicator.

Note If you choose to install the MSI file, you must install the prerequisite software prior to installing Cisco Unified Personal Communicator.

The prerequisite software that you must install prior to installing the Cisco Unified Personal Communicator MSI file is:

- Microsoft .NET Framework 3.5 Service Pack 1
- Microsoft Visual C++ 2005 Redistributable Package (x86)
- Additional software required for Click to Call functionality:
  - Microsoft Office 2003 Primary Interop Assemblies (for computers with Office 2003)
  - Microsoft Office 2007 Primary Interop Assemblies (for computers with Office 2007)
  - Microsoft Visual 2005 Tools for Office Second Edition Runtime (x86)

The prerequisite software is available from the Microsoft website.

Software download site and installer package names

You must register for an account on Cisco.com to access the software download site. On the software download site, the installer packages are offered as .zip files. The .zip files contain all of the files required to deploy the application and the camera drivers.

The installer package names available from the software download site are described in the following table.

Filename	Description
CiscoUnifiedPersonalCommunicatorSetupK9_XXX.exe where XXX = three-letter language locale	This executable contains the required Windows Installer engine, Cisco Unified Client Services Framework, the Outlook plug-in, the user interface, and a set of related DLLs (dynamic link libraries) for deployment. This package is typically used for individual users installing the application.
CiscoVTCameraDriverSetup.exe	This executable contains the installer for the Cisco VT Camera and Cisco VT Camera II device drivers. The installation prompts the user to choose a language if a language other than English is available. Cisco VT Camera III does not require installation of device drivers.

Filename	Description
CiscoUnifiedPersonalCommunicatorSetupK9_XXX.msi	This Microsoft Windows Installer (MSI) package contains the Outlook plug-in, the user interface, and a set of related DLLs for deployment. This package is typically used by IT administrators with the corporate deployment tool (for example, Altiris, System Management Server (SMS), and Active Directory) to distribute the installation to users.
CiscoVTCameraDriverSetup.msi	This MSI package contains the installer for the Cisco VT Camera and Cisco VT Camera II device drivers. For languages other than English, you associate the locale .mst file with the TRANSFORMS parameter to install a language locale.
uc-client-mac-latest.zip	(Cisco Unified Personal Communicator Release 8.x) This package is the disk image (.dmg) of the application for Mac OS X.

Deployment options

You can deploy the Cisco Unified Personal Communicator installation application in one of the following ways listed below.

Automated mass deployment

The mass deployment options for installing Cisco Unified Personal Communicator are as follows:

- Use Active Directory Group Policy. You can use group policy to deploy administrator configuration settings.
- Use a software management system, for example, Altiris Deployment Solution, Microsoft System Center Configuration Manager (SCCM), and so on.
- Use a self-extracting executable with a batch script. You can use the batch script to deploy administrator configuration settings.

Standalone installation

The administrator can install Cisco Unified Personal Communicator on each individual client computer or users can install the application on their own computers. The administrator can use the options listed in Automated mass deployment, on page 9 to deploy the administrator configuration settings.

Note We strongly recommend that you use the executable file for standalone installations.

Deploy the application

(Cisco Unified Personal Communicator Release 8.5 and Earlier) deploying application in Mac OS environment

Before You Begin

Download the disk image (.dmg) from Cisco.com in a Mac OS environment.

Procedure

Step 1 Put the disk image on an internal server so that users can download the image from that location. Alternatively, you can burn the disk image on a CD for internal distribution.

Step 2 Ask users to complete the installation of Cisco Unified Personal Communicator by following the instructions in the user documentation.

What to Do Next

Information to provide to users, on page 16

Related Topics

http://www.cisco.com/en/US/products/ps6844/products_user_guide_list.html
Software download site and installer package names, on page 8
Headsets and other audio devices, on page 13

Deploy application and camera drivers in Microsoft Windows environment

Before You Begin

Download the executable or MSI package from Cisco.com in a Windows environment.

Restriction

Cisco Unified Personal Communicator does not support the advertising or publishing deployment in which users open an icon that the administrator places on their desktops to install the application.

Procedure

Step 1 Perform one of the following actions:

If you want to...	Then...
Deploy the executable or MSI package to a shared location (such as a web server) where users can access it.	Distribute the installer at an elevated privilege so that users can complete the installation (run the installer and follow the installation wizard)
Deploy either the executable or the MSI package directly to the client computer.	Distribute the installer at an elevated privilege so that users can complete the installation (run the installer and follow the installation wizard). or Perform the installation operation directly on a client computer while logged in as the administrator.
Use a software deployment tool to distribute Cisco Unified Personal Communicator and camera drivers to client computers.	Distribute the installer and the drivers using the software deployment tool. No action is required by the users. **Note** Device drivers are not required for Cisco VT Camera III cameras.

Step 2 (If required) Ask users to complete the installation of Cisco Unified Personal Communicator by following the instructions in the user documentation.

What to Do Next

Install security certificates on client computers for Client Services Framework (CSF), on page 11

Related Topics

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

Deployment options, on page 9

Install security certificates on client computers for Client Services Framework (CSF)

The following procedure describes the steps that the administrator needs to take to add security certificates to the keystore on the computer on which Cisco Unified Personal Communicator is running. By default, Cisco Unified Personal Communicator expects self-signed certificates, except when the administrator configures a CCMCIP security profile with a specified certificate type.

Procedure

Step 1 Put the certificate file into the folder where you store your security certificates. The default location for storing security certificates is as follows:

- **Windows XP** - <drive>:\Documents and Settings\<username>\Local Settings\Application Data\Cisco\Unified Communications\Client Services Framework\certificates

- **Windows Vista and Windows 7** - <drive>:\Users\<username>\AppData\Local\Cisco\Unified Communications\Client Services Framework\certificates

Step 2 (Optional) To specify a custom location for storing security certificates, do the following:

a) Choose **Cisco Unified CM IM and Presence Administration** > **Application** > **Legacy Clients** > **Settings**.

b) Use the **CSF certificate directory** field to specify the absolute path to the folder where the certificates are stored.

Step 3 (Optional) To specify the Server Certificate Verification parameter for a CCMCIP security profile, do the following:

a) Choose **Cisco Unified CM IM and Presence Administration** > **Application** > **Legacy Clients** > **CCMCIP Profile (CUPC 8.0 and higher)**.

b) Choose the profile you want to change.

c) In the **Server Certificate Verification** field, choose one of the following options:

- Any Certificate
- **Self Signed or Keystore**
- Keystore Only

What to Do Next

Enable availability status for Microsoft Office 2010 users, on page 12

Enable availability status for Microsoft Office 2010 users

To enable the availability status feature of Cisco Unified Personal Communicator to work with the supported Microsoft Office 2010 applications, the administrator must configure an attribute in Microsoft Active Directory.

Procedure

Step 1 Start the ADSIEdit administrative tool.

Step 2 Expand the domain that contains your users.

Step 3 Open the organizational unit (OU) that contains your users.

Step 4 Add a new value to the proxyAddresses attribute in the format 'SIP:email-address', for example, 'SIP:johndoe@cisco.com'.

Note If Cisco Unified Communications Manager is not AD integrated, the proxyAddress LDAP attribute must be equal to sip uri on the IM and Presence node.

Upgrade application

Before You Begin

Register for an account on Cisco.com to access the software download site.

Restrictions

In a Windows environment, command-line options are not supported on upgrades. Command-line options are only supported on new installations.

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

Procedure

Step 1 Download the latest available Cisco Unified Personal Communicator software from the Software Center.

Step 2 For Windows, download the Cisco VT Camera drivers from the Software Center also.
Device drivers are not required for Cisco VT Camera III cameras.

Step 3 Make the updated software available for deployment.

Step 4 (Optional) For Windows, ask users to uninstall the previous version of Cisco Unified Personal Communicator from the Control Panel.

Step 5 Ask users to perform the following steps to upgrade the application:

a) Exit Cisco Unified Personal Communicator.
b) Disconnect the camera.
c) Install Cisco Unified Personal Communicator.
d) Install the camera software, if any.
e) Reconnect the camera.

Related Topics

http://www.cisco.com/en/US/products/ps6844/products_user_guide_list.html
Software download site and installer package names, on page 8
(Cisco Unified Personal Communicator Release 8.5 and Earlier) deploying application in Mac OS environment, on page 10
Deploy application and camera drivers in Microsoft Windows environment, on page 10

Headsets and other audio devices

You need to install and configure any audio devices that require drivers, such as sound cards or USB headsets. Follow the headset instructions that are supplied with the headset.

For information about establishing the audio device and the control panel settings, see the user documentation for Cisco Unified Personal Communicator.

For information about supported headsets and other audio devices, see the *Release Notes for Cisco Unified Personal Communicator*.

Related Topics

http://www.cisco.com/en/US/products/ps6844/products_user_guide_list.html
http://www.cisco.com/en/us/products/ps6844/prod_release_notes_list.html
Third-party headsets with Cisco Unified Personal Communicator, on page 14

Third-party headsets with Cisco Unified Personal Communicator

While Cisco performs basic testing of third-party headsets for use with the Cisco Unified Personal Communicator application, it is ultimately the responsibility of the customer to test this equipment in their own environment to determine suitable performance. Because of the many inherent environmental and hardware inconsistencies in the locations where this application is deployed, there is not a single best solution that is optimal for all environments.

Before customers begin deploying any headsets (especially deployment in quantity) in their production network, Cisco recommends thorough testing at the customer site to check for voice quality issues, especially hum and echo.

The primary reason that support of a headset would be inappropriate for an installation is the potential for an audible hum. This hum can either be heard by the remote party or by both the remote party and this application user. Causes for this humming sound range from electrical lights near the computer to the computer power source itself. In some cases, a hum heard on a headset plugged directly into the computer Universal Serial Bus (USB) port might be reduced or eliminated by using a powered USB hub.

In some instances, the mechanics or electronics of various headsets can cause remote parties to hear an echo of their own voice when speaking to Cisco Unified Personal Communicator users. The application user will not be aware of this echo.

Finally, some analog headsets do not match the electrical characteristics for which some sound cards are designed. The microphones on such headsets are frequently too sensitive, even when the input levels in Cisco Unified Personal Communicator are reduced to their lowest values. The users of such headsets will sound distorted to remote parties.

It is important to ask Cisco Unified Personal Communicator users whether a particular headset sounds good to them. In addition, ask remote parties about the reception from this application when they use a particular headset.

Related Topic

Headsets and other audio devices, on page 13

Do Not Disturb feature in Cisco Unified Personal Communicator

The Do Not Disturb (DND) feature in Cisco Unified Personal Communicator is always available in the interface and is supported in both softphone and desk phone modes as described in Do Not Disturb feature in Cisco Unified Personal Communicator, on page 14.

Table 1: DND Behavior in Cisco Unified Personal Communicator

Configuration	Behavior
Cisco Unified Personal Communicator is in softphone mode and set to DND by the user	Ringer off. • User can answer incoming calls from Cisco Unified Personal Communicator. • Incoming call notifications are displayed. • Incoming calls display in the Conversation History as Missed. • Unanswered calls are diverted to the call forward no answer (CFNA) target. The default setting for CFNA is voicemail in Cisco Unified Communications Manager. If the CFNA target is not configured, incoming calls are rejected by Cisco Unified Communications Manager, and the caller hears a busy tone. • (Shared line) If Cisco Unified Personal Communicator shares the line appearance with other devices, the endpoints that are not set to DND are alerted to the incoming call, and the caller hears the ringing tone. If all endpoints sharing the line appearance are set to DND, incoming calls are forwarded to the CFNA target.
Cisco Unified Personal Communicator is in desk phone mode with DND **Call Reject** configured in Cisco Unified Communications Manager	The DND behavior for Cisco Unified Personal Communicator is the same as the controlled Cisco Unified IP Phone: • User cannot answer calls from either Cisco Unified Personal Communicator or from the desk phone. • Incoming call notifications are not displayed. • Incoming calls do not display in Recent section of Cisco Unified Personal Communicator. • (Shared line) If Cisco Unified Personal Communicator shares the line appearance with other devices, the endpoints that are not set to DND are alerted to the incoming call, and the caller hears the ringing tone. If all endpoints sharing the line appearance are set to DND, incoming calls are forwarded to the call forward busy (CFB) target.

Configuration	Behavior
Cisco Unified Personal Communicator is in desk phone mode with DND **Ringer Off** configured in Cisco Unified Communications Manager	The DND behavior for Cisco Unified Personal Communicator is the same as the controlled Cisco Unified IP Phone: • User can answer incoming calls from Cisco Unified Personal Communicator or from the desk phone. In both cases, Cisco Unified Personal Communicator displays a call progress window with the connected call status. • An incoming call notification displays without an audio alert on the Cisco Unified IP Phone under Cisco Unified Personal Communicator desk phone control, and Cisco Unified Personal Communicator displays the incoming call notification. If the call is not answered, it is diverted to the Call Forward No Answer (CFNA) target. If CFNA is not configured, the call is rejected, and the caller hears a busy tone. • Incoming calls display in both Cisco Unified Personal Communicator and the desk phone communication histories.

If the DND status is set on other devices, Cisco Unified Personal Communicator displays the DND status. Similarly, IM and Presence passes the DND setting from Cisco Unified Personal Communicator to other devices associated with this Cisco Unified Personal Communicator user.

Note If the DND status is set from the Cisco Unified IP Phone (desk phone), IM and Presence does not pass the DND status to other devices associated with the user, and the status of the user does not change to the DND status on Cisco Unified Personal Communicator. Similarly if the DND status is set from the Cisco Unified IP Phone (desk phone), the DND status clears from the phone, but does not clear on any other devices.

Related Topics

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
http://www.cisco.com/en/US/products/hw/phones/ps379/prod_maintenance_guides_list.html

Information to provide to users

After Cisco Unified Personal Communicator is deployed, provide the information listed in the table to users.

Provide This	Explanation	Give to Users Who Install	Give to Users If You Install
Information about client hardware and software requirements.	You can copy the information from the Release Notes for Cisco Unified Personal Communicator.	Yes	Yes

Provide This	Explanation	Give to Users Who Install	Give to Users If You Install
Location of Cisco Unified Personal Communicator and camera driver installers.	Provide the shared folder location or the CD with the executable files.	Yes	No
Sign-in information.	If Cisco Unified Communications Manager is synchronized with Active Directory, provide this information: • Active Directory Username • Active Directory Password If Cisco Unified Communications Manager is not synchronized with Active Directory, provide this information: • Username • Password • IM and Presence host name or IP address	Yes	Yes
User capabilities (presence, instant messaging, video softphone) available through Cisco Unified Communications Manager licenses.	Provide users with information about the capabilities (license) they have.	Yes	Yes
Cisco Unified Communications Manager extension mobility.	Inform users that you configured for Cisco Unified Communications Manager extension mobility. For a description of the type of information to provide to them, see the *Features and Services Guide for Cisco Unified Communications Manager, Release 9.0(1)* http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.	Yes	Yes
Account information	If Cisco Unified Communications Manager is synchronized with Active Directory, provide this information: • Active Directory Username • Active Directory Password	Yes	Yes

Provide This	Explanation	Give to Users Who Install	Give to Users If You Install
User Options web page access information	Provide the URL (https://node-address/ccmuser), user ID, and password for accessing user options interface on these nodes: • Cisco Unified Communications Manager • IM and Presence From these interfaces, users can control certain settings, features, and services associated with the Cisco Unified IP Phone and with Cisco Unified Personal Communicator.	Yes	Yes
Instructions for using the application.	Provide the user documentation for Cisco Unified Personal Communicator. Remind users to use the application online help.	Yes	Yes
Troubleshooting information.	Provide the information in the section called Troubleshooting, on page 18.	Yes	Yes
Internal company support for the application.	Provide users with the names of people to contact for assistance and with instructions for contacting those people.	Yes	Yes

Related Topics

http://www.cisco.com/en/US/products/ps6844/products_user_guide_list.html
http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html
http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
Troubleshooting, on page 18

Troubleshooting

Cisco Unified Personal Communicator fails to start or starts with black background with no visible controls

Cisco Unified Personal Communicator fails to start, displaying a general exception error, or starts with a black background with no visible controls.

There can be a number of possible causes for this problem, as described in the following table:

Possible Cause	Description
1	This can occur if the sPositiveSign registry key is corrupt. To check if this is the problem, search the client log files for the presence of one or more of the following error messages: • Getting positive key - the user does not have the permissions required to read from the registry keyRequested registry access is not allowed. • Cannot convert string '0.5,0' in attribute 'StartPoint' to object of type 'System.Windows.Point'. • System.FormatException: Input string was not in a correct format.
2	This can occur if you customize the Regional Options for the English (United States) language to change the Decimal symbol or the List separator default settings. To check if this is the problem, search the client log files for the presence of multiple instances of the following error message: • Cannot convert string '0,0' in attribute 'StartPoint' to object of type 'System.Windows.Point'

The location of the client log files is:

- **Windows XP** - <drive>:\Documents and Settings\<username>\Local Settings\Application Data\Cisco\Unified Communications\CUPC8\Logs
- **Windows Vista and Windows 7** - <drive>:\Users\<username>\AppData\Local\Cisco\Unified Communications\CUPC8\Logs

  To resolve this issue, do the following:

  1. Open the **Control Panel**.
  2. Choose **Regional and Language Options**.
  3. Choose the **Regional Options** tab.
  4. In the Standards and formats section, choose a different language from the drop-down list. For example, choose **English (Australia)**.
  5. Click **Apply**.
  6. In the Standards and formats section, choose **English (United States)** from the drop-down list.
  7. Click **Apply** again, then click **OK**.

You may need to reboot your computer for the change to take effect.

Limitations creating group chats

You cannot create a group chat in the following circumstances:

- Your chosen default policy is to block all users, except those explicitly allowed.

- Your policy does not include any exceptions for conference aliases.

Cannot place or receive calls after secure profile enabled

After a secure profile is enabled for a user, the user cannot place or receive calls. The user might see the following error message multiple times:

Failed to start conversation

The user can use the instant messaging features.

This problem occurs if a secure profile is enabled for the user in Cisco Unified Communications Manager while either of the following is true:

- The user is signed in to Cisco Unified Personal Communicator.
- The cucsf.exe process is running on the computer of the user, that is, Cisco Unified Personal Communicator is running, but the user has not signed in.

  Ask the user to sign out of Cisco Unified Personal Communicator, then sign in again.

Error connecting to CSF device

When Cisco Unified Personal Communicator tries to connect to the Client Services Framework (CSF) device on Cisco Unified Communications Manager after an upgrade, the user sees the error "CTL reset is required [1002]" and the phone on the computer does not function.

If you configure security in your Cisco Unified Communications system, you use Certificate Trust List (CTL) files. The CTL file contains certificates for all of the servers in your Cisco Unified Communications system with which Client Services Framework might need to communicate securely.

When a device connects to a server in your Cisco Unified Communications system, the server is verified against this list. Client Services Framework does not allow secure connections to servers that are not explicitly listed in the CTL.

If a device is moved from one cluster to another or you upgrade to a new version of Cisco Unified Communications Manager, you must update the CTL file for the device list of servers in the new cluster.

Procedure

1. Delete the contents of the appropriate folder as described in the following table:
2. Delete the contents of the appropriate folder as described in the following table:
3. If a device is moved from one cluster to another, update the device settings for the user to point to the new cluster. For example, update the references to the Cisco Unified Communications Manager IP Phone (CCMCIP) server, Trivial File Transfer Protocol (TFTP) server, and Computer Telephony Integration (CTI) servers.

Operating System

Folder

Windows XP

<drive>:\Documents and Settings\<username>\Application Data\Cisco\Unified Communications\Client Services Framework\Security\sec

Windows VistaWindows 7

<drive>:\Users\<username>\AppData\Roaming\Cisco\Unified Communications\Client Services Framework\Security\sec

Operating System

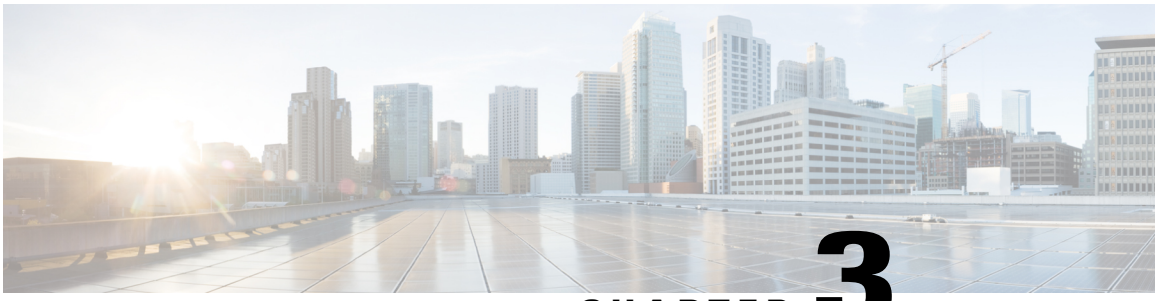
Folder

Windows XP

<drive>:\Documents and Settings\<username>\Application Data\Cisco\Unified Communications\Client Services Framework\Config

Windows VistaWindows 7

<drive>:\Users\<username>\AppData\Roaming\Cisco\Unified Communications\Client Services Framework\Config



CHAPTER 3

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, page 24
- Prerequisites for integrating Cisco Unified Personal Communicator, page 26
- Configure firewalls to pass Cisco Unified Personal Communicator traffic, page 27

- Verify Cisco XCP Router service is running, page 28
- (Cisco Unified Personal Communicator Release 8.x) about configuring XCP services for Cisco Unified Personal Communicator, page 28
- Chat configuration, page 29
- Cisco Unified Personal Communicator configuration on Cisco Unified Communications Manager, page 30
- Cisco Unified Personal Communicator configuration on Cisco Unified Communications Manager, page 37
- About Cisco Unified Personal Communicator configuration on IM and Presence, page 42
- Cisco Unified Personal Communicator configuration on IM and Presence, page 43
- Video calls and Videoconferencing configuration, page 46

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 26	• Assign the licensing capabilities on Cisco Unified Communications Manager. • Configure firewalls to pass Cisco Unified Personal Communicator traffic, on page 27
Availability status information and instant messaging	• (Cisco Unified Personal Communicator Release 8.x) required XCP services, on page 28 • (Cisco Unified Personal Communicator Release 8.x) optional XCP services, on page 28	• Verify Cisco XCP Router service is running, on page 28 • Turn on IM and Presence Services to support XMPP clients • (Cisco Unified Personal Communicator Release 8.x) configure settings, on page 44 • (Cisco Unified Personal Communicator Release 8.5) configuring chat history, on page 30

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 28	• Service parameter configuration for IM Gateway, on page 29 • Configuring persistent chat rooms, on page 29
Place calls from a computer	• Application dialing and directory lookup rules, on page 30 • Transformation of dialed numbers by Cisco Unified Personal Communicator, on page 31 • Cisco Unified Client Services Framework device type, on page 32 • Extension Mobility configuration, on page 32 • (Cisco Unified Personal Communicator Release 8.x) guidelines for configuring softphone device name, on page 33 • TFTP server connection, on page 42	
Place calls from a desk phone	• Desk phone control and CTI connection failures, on page 33	
Video calls and videoconferencing	-	• Configure users for point-to-point video calls and for multipoint videoconferencing, on page 46 • Configure videoconferencing resources and Ad-Hoc conferencing on Cisco Unified Communications Manager, on page 47 • (Cisco Unified Personal Communicator Release 8.x) configure settings, on page 44

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, on page 59
Security features	-	• (Cisco Unified Personal Communicator Release 8.x) configure settings, on page 44
High availability features	• High Availability, on page 43	• High Availability IM and Presence deployments configuration
Third-party client applications	• (Cisco Unified Personal Communicator Release 8.x) optional XCP services, on page 28	• Third-Party client configuration on IM and Presence, on page 61
HTML content display	-	• (Cisco Unified Personal Communicator Release 8.5) Distribute HTML files for display in Cisco Unified Personal Communicator window, on page 64
Desktop agent	• (Cisco Unified Personal Communicator Release 8.5) Cisco Unified Personal Communicator as desktop agent, on page 62	• Configure Cisco Unified Personal Communicator as desktop agent, on page 62 • Start Cisco Unified Personal Communicator as desktop agent, on page 63

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 2: 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, on page 31

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

Application dialing and directory lookup rules, on page 30
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

Create softphone device for each Cisco Unified Personal Communicator user, on page 37

(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 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.

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, on page 34
Create CTI Gateway profiles, on page 35

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 35

Related Topics

User and device configuration on Cisco Unified Communications Manager

Desk phone control and CTI connection failures, on page 33

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

Configure CTI Gateway server names and addresses, on page 34
Desk phone control and CTI connection failures, on page 33

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

- Associate users with softphone devices, on page 39

Related Topics

Extension Mobility configuration, on page 32
Configure videoconferencing resources and Ad-Hoc conferencing on Cisco Unified Communications Manager, on page 47

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, on page 40

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, on page 41

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, on page 41

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 43

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

TFTP server connection, on page 42

(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, on page 47

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

Create softphone device for each Cisco Unified Personal Communicator user, on page 37
Configure users for point-to-point video calls and for multipoint videoconferencing, on page 46

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 50

(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.

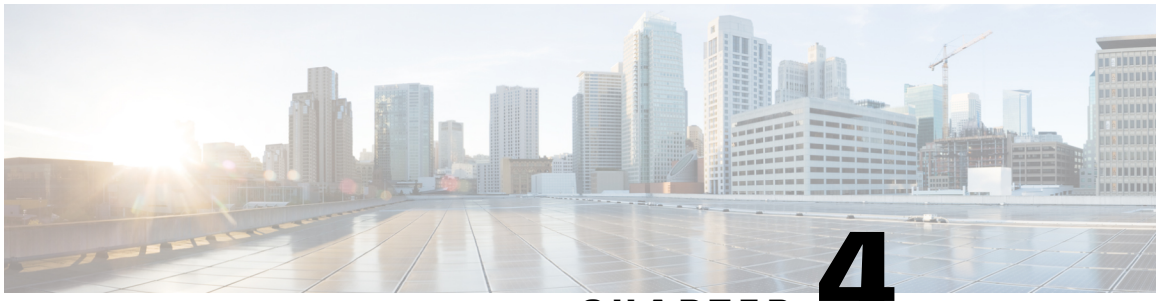
Step 3 Click on the Device Name.

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.



CHAPTER 4

Voicemail, conferencing, and other features for Cisco Unified Personal Communicator

This chapter includes the information required to configure Cisco Unified Personal Communicator features. 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 Voicemail, mailstore, conferencing, and audio profile configuration on IM and Presence has been moved to Cisco Unified Communications Manager. For more information, see the *Cisco Unified Communications Manager Administration Guide, Release 9.0(1)*.

- Voicemail server configuration for Cisco Unified Personal Communicator, page 52
- Conferencing server configuration for Cisco Unified Personal Communicator, page 56
- Configure CCMCIP profiles for Cisco Unified Personal Communicator release 8.x, page 59
- Third-Party client configuration on IM and Presence, page 61

- (Cisco Unified Personal Communicator Release 8.5) Cisco Unified Personal Communicator as desktop agent, page 62
- (Cisco Unified Personal Communicator Release 8.5) Distribute HTML files for display in Cisco Unified Personal Communicator window, page 64
- User configuration update after deploying Cisco Unified Personal Communicator, page 65

Voicemail server configuration for Cisco Unified Personal Communicator

Note Before you perform the tasks described here, make sure that you fully integrate Cisco Unified Personal Communicator with Cisco Unified Communications Manager and IM and Presence.

Configure Cisco Unity Connection servers

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

Before You Begin

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

Procedure

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

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

Step 2 Configure the user:

a) If the users are existing Cisco Unity Connection users, add them to the Cisco Unified Communications Manager database and to IM and Presence. Proceed to Step 4.

b) If the user is a new Cisco Unified Personal Communicator user, add the user to Cisco Unified Communications Manager database, Cisco Unity Connection, and to IM and Presence.

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

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

Step 4 (Optional) Enable secure messaging as follows:

a) Expand **Class of Service** in the section on the left-hand side, and then choose **Class of Service**.
b) Choose an option from Require Secure Messaging in the Message Options section to enable secure messages.

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

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

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

Troubleshooting Tips

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

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

Related Topics

http://www.cisco.com/en/us/products/ps6844/prod_release_notes_list.html
http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html

Configure Cisco Unity servers

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

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

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

Before You Begin

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

Procedure

Step 1 Configure the Microsoft Exchange server to use the IMAP virtual server:
To configure Microsoft Exchange 2003:

a) Choose **Start** > **All Programs** > **Microsoft Exchange** > **System Manager** .
b) In the section on the left-hand side of the System Manager, expand **Servers** .
c) Choose the server name.
d) Choose **Protocols** > **IMAP** .
e) Right-click, and choose **Start Server** .

To configure Microsoft Exchange 2007:

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

Step 2 Configure the port and encryption type:
To configure Microsoft Exchange 2003:

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

To configure Microsoft Exchange 2007:

a) Choose **Start** > **Programs** > **Microsoft Exchange Server 2007** > **Exchange Management Shell**.
b) Specify the authentication settings for the Client Access Server that is running the IMAP4 service through the Exchange Power Shell.
Note Microsoft Exchange 2007 uses SSL by default.
c) Execute one of the following commands for the appropriate setting:
- For plain text login: set-imapsettings -LoginType PlainTextLogin
- For SSL: set-imapsettings -LoginType SecureLogin

Step 3 Configure the user:
a) If the user is an existing Cisco Unity user, add the user to the Cisco Unified Communications Manager database and to IM and Presence.
b) If the user is a new user, add the user to the Cisco Unified Communications Manager database, Cisco Unity (which adds the user to Exchange and to Active Directory), and to IM and Presence.

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

Step 5 (Optional) Enable secure messaging as follows:
a) Choose **Subscribers** > **Subscribers** > **Features** to make the change on a subscriber template.
The change you make here is not applied to current subscriber accounts that were created by using this template. The setting applies only to subscriber accounts that are created by using this template after the change has been made.
b) Choose an option from the Message Security When Sending a Message list to enable secure messages. For example, choose **Encrypt All Messages**.
This setting specifies whether messages are encrypted when subscribers send messages to other subscribers.
c) Click **Save**.
d) Repeat these steps for additional subscribers or subscriber templates, as applicable.

Step 6 (Optional) Enable secure messaging for messages from unidentified callers:
a) Choose **System** > **Configuration** > **Message Security Settings**.
b) Specify whether messages from unidentified callers are encrypted. Choose an option from the list.
c) Click **Save**.
Troubleshooting Tip

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

Conferencing server configuration for Cisco Unified Personal Communicator

Note Before you perform the tasks described here, make sure you fully integrate Cisco Unified Personal Communicator with Cisco Unified Communications Manager and IM and Presence.

Conferencing servers for Cisco Unified Personal Communicator

Cisco Unified Personal Communicator can be configured to launch ad-hoc conference calls and web meetings on the following products:

Conferencing Server(s)	Cisco Unified Personal Communicator Version
Cisco Unified MeetingPlace	All versions
Cisco Unified MeetingPlace Express	7.1
Cisco Unified MeetingPlace Express VT [1] [2]	8.x
Cisco Webex Node for MCS integrated with Cisco Unified MeetingPlace	8.0
Cisco Webex Node for MCS	7.1, 8.5

1 Can be used for conference calls with video if Cisco Unified Communications Manager is configured to use Cisco Unified MeetingPlace Express VT.
2 Does not support web meetings.

You can use Cisco Unified Personal Communicator to join Cisco Unified MeetingPlace and Cisco Webex scheduled meetings as follows:

Conferencing Server	Cisco Unified Personal Communicator Version
Cisco Unified MeetingPlace	All versions
Cisco Webex	8.5

Configure Cisco Unified MeetingPlace Servers

Cisco Unified MeetingPlace provides a more extensive feature set (such as scheduled and reservationless rich-media conferencing) and allows more concurrent users than Cisco Unified MeetingPlace Express or Cisco Unified MeetingPlace Express VT. With Cisco Unified MeetingPlace, a Cisco Unified Personal

Communicator user can start a meeting from an instant message conversation, from a phone conversation, or from a phone conversation with video.

Before You Begin

- Install a supported release of the Cisco Unified MeetingPlace web conferencing server. For more information about how to install and configure Cisco Unified MeetingPlace, see the Administration Documentation for Cisco Unified MeetingPlace: http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html
- Integrate the web conferencing server with Cisco Unified Communications Manager.
- Determine the number of web and audio conferencing user licenses that provide enough web ports for meetings initiated through Cisco Unified MeetingPlace and through Cisco Unified Personal Communicator.

Procedure

Step 1 Install web and audio conferencing user licenses.

Step 2 If not already enabled, enable the Secure Sockets Layer (SSL) encryption technology on the web conference server. You must obtain and upload the required certificates from a trusted certificate authority (CA). The certificate is required for secure communications between Cisco Unified Personal Communicator and the web conference server. Without SSL, clear text passwords are sent from Cisco Unified Personal Communicator to the web conferencing server and from the sign in browser to the web conferencing server.

Step 3 Set up a user authentication method on the web conference server.
The following authentication methods are supported for use with Cisco Unified Personal Communicator:

a) MeetingPlace
b) HTTP Basic Authentication (Domain)
c) LDAP
d) LDAP, then MeetingPlace

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

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

Related Topics

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html
http://www.cisco.com/en/us/products/ps6844/prod_release_notes_list.html
http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_installation_and_configuration_guides_list.html

(Cisco Unified Personal Communicator Release 8.x) configure Cisco Unified MeetingPlace web server

Before You Begin

Install a supported release of the Cisco Unified MeetingPlace conferencing server. For more information about how to install and configure Cisco Unified MeetingPlace, see the Administration Documentation for Cisco Unified MeetingPlace:

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

Procedure

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

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

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

What to Do Next

Related Topic

Administration Documentation for Cisco Unified MeetingPlace:

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

Add custom Cisco Unified MeetingPlace template files to Cisco Unified MeetingPlace7.x web server

If your Cisco Unified Communications system uses Cisco Unified MeetingPlace Release 7.x, you must install the following files on the Cisco Unified MeetingPlace Web server:

- CSFGetProfileSuccess.tpl
- CSFScheduleSuccess.tpl

You can get the above files from the Administration Toolkit. To access the Administration Toolkit, navigate to Cisco Unified Personal Communicator from the Download Software page.

You can copy these files to the correct location on the Cisco Unified MeetingPlace Web server. You do not need to restart the server. The default location for these files is as follows:

C:\Program Files\Cisco Systems\MPWeb\Template

(Cisco Unified Personal Communicator Release 8.5) Cisco Webex server configuration

There is no specific configuration required to use Cisco Webex conferencing servers with Cisco Unified Personal Communicator. Install a supported version of Cisco Webex Node for MCS or use a Cisco Webex SaaS (software as a service) solution. For information about supported versions, see the *Release Notes for Cisco Unified Personal Communicator*:

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

What To Do Next

Single sign-on configuration for Cisco Webex and Cisco Unified MeetingPlace, on page 59

Single sign-on configuration for Cisco Webex and Cisco Unified MeetingPlace

To deploy Cisco Unified Personal Communicator in an environment where users join Cisco Webex meetings using their Cisco Unified MeetingPlace credentials, and the credentials are verified by Cisco Unified MeetingPlace, you must set a registry key value as follows:

Registry Key	Value
WebConfSSOIdentityProvider	meetingplace

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

Configure CCMCIP profiles for Cisco Unified Personal Communicator release 8.x

The CCMCIP service runs on Cisco Unified Communications Manager and retrieves a list of devices associated with each user. CCMCIP profiles are required before Cisco Unified Personal Communicator Release 8.x clients can retrieve the list of user devices from Cisco Unified Communications Manager. You can create a profile to control Cisco Unified Personal Communicator Release 8.x in deskphone mode and to facilitate device discovery for desk phones and softphones. You can then associate chosen users to the newly created profile.

Procedure

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

Step 2 Click **Add New**.

Step 3 Enter the profile name and description.

Step 4 Enter information into the fields:

Field	Setting
Primary CCMCIP Host	Enter the address of the node for the CCMCIP service to use to retrieve the list of associated devices when users sign in to a device or phone. Enter the address in one of the following forms: • IP address • Host name • FQDN This value must match exactly the IP address, host name, or FQDN of the CCMCIP server.
Backup CCMCIP Host	Enter the address of the backup server for the CCMCIP service to use if the primary CCMCIP server fails. Enter the address in one of the following forms: • IP address • Host name • FQDN This value must match exactly the IP address, host name, or FQDN of the backup CCMCIP server.

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

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

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

Step 7 Click **Save**.

Third-Party client configuration on IM and Presence

You must configure LDAP settings that allow IM and Presence to search for contacts in third-party XMPP clients.

Related Topic

LDAP directory integration

(Cisco Unified Personal Communicator Release 8.5) Cisco Unified Personal Communicator as desktop agent

You can start Cisco Unified Personal Communicator as a background application, which you can control as a CTI device. Cisco Unified Personal Communicator starts without a graphical user interface and you can only communicate with the client via a CTI connection. When you are running Cisco Unified Personal Communicator as a desktop agent, there is no indicator on the desktop to show that the application is running.

Cisco Unified Personal Communicator running as desktop agent

When you start Cisco Unified Personal Communicator as a desktop agent, the following features are not available:

- Availability - you appear offline.
- Chat - you do not receive any instant messages.
- Conversation history - any calls that you make are not listed in the call logs.
- Video - you can make voice-only calls without video.
- Web meetings are not available.
- Call and chat features from applications such as Microsoft Outlook and Office are not available. You can only modify your audio or call settings, such as the audio device or call forwarding options, while running Cisco Unified Personal Communicator in normal mode. Any changes that you make in normal mode are applied when you restart the application as a desktop agent.

Before you can start Cisco Unified Personal Communicator as a desktop agent, you must first:

- Start the application in the normal manner.
- Set the CcmcipServer1 andTftpServer1 registry keys.

Related Topics

Configure Cisco Unified Personal Communicator as desktop agent, on page 62
Start Cisco Unified Personal Communicator as desktop agent, on page 63
Stop Cisco Unified Personal Communicator as desktop agent, on page 63

Configure Cisco Unified Personal Communicator as desktop agent

Before you can start Cisco Unified Personal Communicator in desktop agent mode, you must perform some actions.

Procedure

Step 1 Set the following registry keys:

- CcmcipServer1 - the IP address of the CCMCIP server
- TftpServer1 - the IP address of the TFTP server

The registry keys are located at:

HKEY_CURRENT_USER/Software/Cisco Systems, Inc./Client Services Framework/AdminData

Note These registry keys are ignored when you are using Cisco Unified Personal Communicator in normal mode.

Step 2 Start Cisco Unified Personal Communicator in normal mode.

Step 3 Enter your credentials and check the **Automatically sign in** check box.

Step 4 Verify that your phone services are working as expected.

Note Cisco Unified Personal Communicator will not operate in agent desktop mode if you are using your desk phone for phone calls. Do not check the **Use my desk phone for audio** check box.

Step 5 Verify that your audio and call settings meet your requirements, for example, chosen audio device and call forwarding options. These settings cannot be modified in desktop agent mode.

Step 6 Choose **File** > **Exit** to close the application.

Note You must perform steps 2 to 6 each time your user credentials in Cisco Unified Communications Manager change.

Related Topics

Start Cisco Unified Personal Communicator as desktop agent, on page 63
Stop Cisco Unified Personal Communicator as desktop agent, on page 63

Start Cisco Unified Personal Communicator as desktop agent

Enter the following command line:

cupc.exe -START_AGENT_DESKTOP_MODE

Cisco Unified Personal Communicator starts a background application accepting CTI connections from third party clients. You can only start one instance of Cisco Unified Personal Communicator, so if you execute the command again, nothing happens. The command is not case sensitive and if multiple arguments are used, only the first argument is considered by the system.

Related Topics

Configure Cisco Unified Personal Communicator as desktop agent, on page 62
Stop Cisco Unified Personal Communicator as desktop agent, on page 63

Stop Cisco Unified Personal Communicator as desktop agent

Enter the following command line:

cupc.exe -SHUTDOWN

This command terminates all Cisco Unified Personal Communicator processes and exits the client. The command is not case sensitive and if multiple arguments are used, only the first argument is considered by the system.

Note This command also terminates any Cisco Unified Personal Communicator process that is running in normal mode.

Related Topics

Configure Cisco Unified Personal Communicator as desktop agent, on page 62
Start Cisco Unified Personal Communicator as desktop agent, on page 63

(Cisco Unified Personal Communicator Release 8.5) Distribute HTML files for display in Cisco Unified Personal Communicator window

This feature of Cisco Unified Personal Communicator enables you to distribute HTML content for display on the Cisco Unified Personal Communicator main window. You can include up to three pages of content, and specify the title and icon to display for each page. To set up the HTML content, you must perform the steps in the following procedure.

Procedure

Step 1 Start the Registry Editor.

Step 2 Go to the following location in the registry:
HKEY_CURRENT_USER/Software/Cisco Systems, Inc/Unified Communications/CUPC

If CUPC does not exist under Unified Communications, right-click on **Unified Communications** and choose **New** > **Key** and create the CUPC key.

Step 3 Right-click on the **CUPC** key, and choose **New** > **Multi-String Value.**

Step 4 Name the multistring value CustomTabDescriptions.

Step 5 Right-click on **CustomTabDescriptions** and choose **Modify**.

Step 6 In the Value data field, enter up to three lines in the following format:
Label, icon1.png, filename1.html, True

where

- Label is the title for the HTML page that you want to appear in the Cisco Unified Personal Communicator window. Keep the labels short as long labels will be truncated.
- icon1.jpg is the location and filename of the icon that you want to use with the label for the HTML page. The supported formats are PNG (recommended), JPG, GIF, and BMP. The recommended icon size is 24x24 pixels. Any icons that are larger than this size are scaled to size.
- filename1.html is the page that you want to display. This can be a local file or a link to an external URL.
- True can be true or false to indicate if the HTML page is automatically refreshed each time you click on the icon. This value is optional and if not specified, a value of false is assumed.

For example:

Cisco, C:\images\icon1.png, http://www.cisco.com, true

Products, \\web\images\icon2.png, \\web\content\products.html, true

Pricing, \\web\images\icon3.png, \\web\content\pricing.html, false

Some particular notes about this feature are:

- If the icon is not valid, it is replaced by a default icon.
- If the HTML content is not valid, the item is not displayed in the Cisco Unified Personal Communicator main window.
- If there are problems accessing the HTML content (for example, network connection issues) and you specified True in the registry value to refresh the content every time you click on the icon, the page is not displayed. If you specified False, not to refresh the content each time you click on the icon, the previously-cached content is displayed.

User configuration update after deploying Cisco Unified Personal Communicator

Application profiles

This module describes how to change the following application profile for a single user, or for multiple users:

- (Cisco Unified Personal Communicator Release 8.x) CCMCIP Profile

Application profiles enable you to partition your Cisco Unified Personal Communicator user base for performance and scalability. You can change individual application profiles for each user.

Change application profiles for single user

Procedure

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

Step 2 Click **Find** to populate the search results fields, or search for a user, and then click **Find**.

Step 3 Click the link to choose the user.

Step 4 Specify the profiles to change for the user in the Application Profile Configuration section.
If you change a user application profile in this window (for example, change from LDAP Profile 1 to LDAP Profile 2), the change is reflected in **Cisco Unified CM IM and Presence Administration** > **ApplicationLegacy ClientLDAP Profile** window.

Step 5 Click **Save**.
The user must exit and restart Cisco Unified Personal Communicator for the changes to take effect.

Related Topics

Change application profiles for multiple users, on page 66

Change application profiles for multiple users

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Cisco Jabber/Microsoft RCC** > **Export.**

Step 2 Perform the following actions:

a) Click **Find** in the Export Users Query window to obtain current profile information by finding all users.
b) Click **Next** at the bottom of the window.
c) Specify the filename to be exported in the Export CUP Users Configuration window.

Step 3 Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Upload/Download Files**.

Step 4 Perform the following actions:

a) Find and choose the file that you want to download.
b) Click **Download Selected**.
c) Add or remove profile names according to the instructions in the sample file.

Step 5 Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Upload/Download Files**.

a) Click **Add New**.
b) Enter the name of the file to upload.
c) Choose the target for which you want to use the file.
d) Choose the transaction type that the file defines.
e) Click **Overwrite File if it exists** if you want to overwrite an existing file with the same name.
f) Click **Save**.

Step 6 Choose **Cisco Unified CM IM and Presence Administration** > **Bulk Administration** > **Cisco Jabber/Microsoft RCC** > **Update**.

Step 7 Perform the following actions:

a) Choose the updated .csv file.
b) Click **Save** to submit the file to update profile information in bulk.

Related Topics

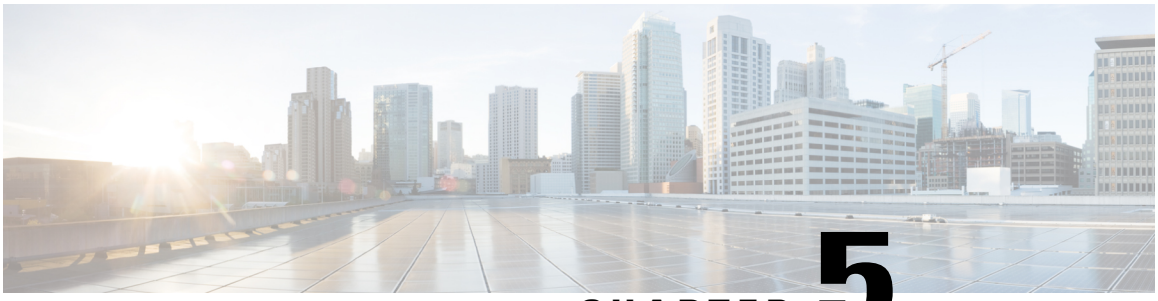
Change application profiles for single user, on page 65

New user configuration for full Cisco Unified Personal Communicator functionality

The table lists the required configuration steps to add a new user to various servers after the initial deployment. By completing these tasks, the new user will have full Cisco Unified Personal Communicator functionality after the initial deployment.

Task	Where to Find Information
Cisco Unified Communications Manager Configuration	• User and device configuration on Cisco Unified Communications Manager
• Add the phone to the Cisco Unified Communications Manager database. • Allow control of the Cisco Unified IP Phone from the computer telephony interface (CTI). • Associate a directory number with the phone.	
• Set up the user account, and associate the directory number with the user. • Associate the phone with the user. • Add the user to the Standard CTI-Enabled group. • Add the user to the CCM End User group.	
• Enable Cisco Unified Personal Communicator softphone features by manually creating a new device for each user.	• Cisco Unified Personal Communicator configuration on Cisco Unified Communications Manager, on page 30
• Make sure that availability status in Cisco Unified Personal Communicator is accurately displayed. • Associate the line of the user with the user in Cisco Unified Communications Manager.	
IM and Presence Configuration	
• Configure the LDAP attribute map for Cisco Unified Personal Communicator.	• LDAP directory integration • About Cisco Unified Personal Communicator configuration on IM and Presence, on page 42
• Add the new user to the server profiles.	

Task	Where to Find Information
Point-to-point video calls Multipoint videoconferencing Video telephony camera	• Configure users for point-to-point video calls and for multipoint videoconferencing, on page 46 • Configure videoconferencing resources and Ad-Hoc conferencing on Cisco Unified Communications Manager, on page 47
Provide information to users	• Information to provide to users, on page 16
Headset and audio device Information	• Headsets and other audio devices, on page 13



CHAPTER 5

Active directory configuration for Cisco Unified Personal Communicator

The phone numbers and other user information for Cisco Unified Personal Communicator are provided by Active Directory. Cisco Unified Client Services Framework provides Active Directory services for Cisco Unified Personal Communicator.

Cisco Unified Client Services Framework can use either of the following mechanisms to retrieve contact information from an Active Directory server:

- Enhanced Directory Integration (EDI): EDI uses native Windows APIs. If you chose to use EDI, you might not need to do any further configuration, depending on how your clients can access the directory.
- Basic Directory Integration (BDI): The integration is not native to Windows environments, and requires configuration.

We recommend that you use EDI because EDI provides significant advantages over BDI, as described in Feature comparison of enhanced and basic directory integration, on page 70.

If you use BDI, or use EDI and do additional configuration, you must deploy the configuration settings to the computers in your Cisco Unified Communications system. To do this, you can use Active Directory Group Policy.

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

- Feature comparison of enhanced and basic directory integration, page 70
- Cisco Unified Client Services Framework integration with Active Directory, page 71
- Mapping keys required for Basic and Enhanced Directory integration, page 72
- Enhanced Directory Integration, page 73
- Enhanced Directory Integration configuration with Active Directory, page 76
- Basic Directory Integration, page 84
- Phone number masks, page 92
- Contact photo retrieval, page 94

Feature comparison of enhanced and basic directory integration

The following table lists the features that are available with enhanced and basic directory integration. Use this table to help you decide which mechanism is most suitable for your Cisco Unified Communications system.

Table 4: Feature Comparison of Enhanced and Basic Directory Integration

Feature	Enhanced	Basic
Configured as the default mechanism for Active Directory integration	No	Yes
Requires minimal configuration	Yes	No
Automatic discovery of directory service	Yes	No, requires configuration
Supports connection to the Active Directory domain controller (DC)	Yes	Yes, requires configuration
Supports connection to the Active Directory global catalog (GC)	Yes, supported by default	Yes, requires configuration
Supports connection to Active Directory Lightweight Directory Services (AD LDS) and Active Directory Application Mode (ADAM) servers	Yes	Partial, proxy authentication not supported
You can define the service and port for the directory service	Yes, optional	Yes, required
You can configure a back-up directory server	Yes	No
You can define search bases	Yes, up to 5	Yes, up to 5
SSL is supported	Yes	Yes

Feature	Enhanced	Basic
You can use the Windows certificate store for SSL	Yes	No, you must use the Java store
Support for encryption of Active Directory credentials	Yes	No, unless you use SSL
Support for integrated authentication with Windows credentials	Yes	No
Administrator can define alternative credentials	Yes	No
User can define alternative credentials	Yes	Yes
Custom attribute map	Yes	Yes, but the map must be defined
Phone attribute search scope control	Yes	No
Can customize LDAP queries	Yes	Yes
Support for phone number masks	Yes	Yes
Can retrieve contact photo URL	Yes	Yes
Can retrieve binary photo object	Yes	No

Cisco Unified Client Services Framework integration with Active Directory

The following table lists the registry subkeys that can be created or modified to specify whether to use Enhanced or Basic Directory Integration. The subkeys will be located in the following registry location:

[HKEY_CURRENT_USER\Software\Cisco Systems, Inc.\Client Services Framework\AdminData].

The following subkeys must be created if they do not already exist.

Table 5: Registry Subkey for Configuration of Enhanced or Basic Directory Integration

Subkey Name	Description
EnableNativeDirectoryProvider	Specify whether to use Enhanced or Basic Directory Integration to get contact information from Active Directory. Enter one of the following values: • 0: Use Basic Directory Integration. This is the default value. • 1: Use Enhanced Directory Integration. Data type: REG_SZ

If you are configuring Presence or chat for Partitioned Intradomain Federation, you must create or modify the subkeys listed in the following table so that users can be added directly from Active Directory. The subkeys will be located in the following registry location:

[HKEY_CURRENT_USER\Software\Cisco Systems, Inc.\Client Services Framework\AdminData].

Table 6: Registry Subkey for Configuration of Presence and Chat for Partitioned Intradomain Federation

Subkey Name	Value
LDAP_AttributeName_uri	msRTCPSIP
LDAP_UriSchemeName	SIP

Mapping keys required for Basic and Enhanced Directory integration

This chapter provides information on the configuration of both Basic and Enhanced Directory Integration. The following guidelines are provided to ensure registry key explanations that are only applicable to only one type of directory integration or both are clear and easily understood by the administrator:

- The registry keys **LDAP_AttributeName_uri**, **LDAP_SearchByUsername**, and **LDAP_DisableNumberLookups** provide services available to both Basic and Enhanced Directory Integration.
- The registry key **EnableNativeDirectoryProvider** are applicable only to Enhanced Directory Integration.
- All registry keys listed in this chapter that are prefaced with **LDAP_**, with the exception of those listed in the first bullet, are applicable to Basic Directory Integration only.

Related Topics

LDAP registry settings, on page 87
Connection configuration for Enhanced Directory Integration, on page 77
Default values for directory attributes, on page 80

Enhanced Directory Integration

If you use Enhanced Directory Integration (EDI), you can benefit in the following ways:

- You might not need to do any further configuration, depending on how your clients can access the directory.

  Your clients will connect securely to a Global Catalog (GC) server in the domain that the user is logged into. The GC server must be discoverable by DNS with Windows authentication. The credentials used are the credentials of the Windows user who is currently logged in.

- The directory server is discovered automatically by DNS.
- Users can sign in to a Windows domain, then access Active Directory without entering an Active Directory username and password.
- Connections to Active Directory Lightweight Directory Services (AD LDS) and Active Directory Application Mode (ADAM) servers that implement local and proxy authentication are supported.
- SSL is supported. The Windows certificate store is used, so you do not need to configure a separate certificate store.
- DNS provides failover support in Windows domains.
- DNS provides load balancing support in Windows domains.
- Anonymous binds and simple binds are supported.

Related Topics

Automatic discovery of directory service, on page 73
Directory servers that cannot be discovered automatically, on page 74
Connections to Global Catalog servers or domain Controllers, on page 74
Usage of SSL, on page 74
Usage of Windows credentials, on page 75
Usage of non-Windows credentials, on page 75
Topics to consider before you use Enhanced Directory Integration, on page 75

Automatic discovery of directory service

If you configure Enhanced Directory Integration to use automatic discovery, the Cisco Unified Client Services Framework uses a similar method to discover the directory service that Windows uses to discover a domain controller (DC) or Global Catalog (GC). That is, the Cisco Unified Client Services Framework uses a DNS Service record (SRV) request.

The Cisco Unified Client Services Framework searches for a GC server in the domain that the client computer is a member of. To identify the domain the client computer queries, check the value of the USERDNSDOMAIN environment variable of the computer.

Related Topics

Directory servers that cannot be discovered automatically, on page 74

Directory servers that cannot be discovered automatically

If you configure a primary and a secondary server, Cisco Unified Personal Communicator attempts to connect to the primary server. If the primary server is not available, Cisco Unified Personal Communicator attempts to connect to the secondary server. If the connection to the secondary server is successful, the primary server is blacklisted for a period of time.

Related Topics

Automatic discovery of directory service, on page 73

Connections to Global Catalog servers or domain Controllers

We recommend that the LDAP and LDAPS connections in your Cisco Unified Communications system are configured to a Global Catalog (GC) server rather than to a domain controller (DC). The GC server holds primary directory attributes for all users in your Windows domain forest. The default search attributes that the Cisco Unified Client Services Framework uses are normally all available from a GC server.

If LDAP and LDAPS connections are configured to a DC, directory searches from Cisco Unified Client Services Framework are restricted to data within that domain. Searches might not be able to resolve contact from peer subdomains within the organization.

The administrator of the directory server might choose to connect to a DC if some search attributes are not present in the GC server. A DC only holds contact information for use in the domain that the DC manages.

If your Cisco Unified Communications system uses custom attributes for phone numbers, then these attributes might not be available from the GC. If some attributes are not available from the GC, the directory server administrator might configure the Cisco Unified Personal Communicator to connect to a DC or to request the directory manager to enable the missing attribute on the GC server.

If your system uses directory-based photos of contacts, confirm with your directory administrator that photo attributes are available from the GC. The directory administrator might enable these attributes in a GC server.

If you configure Enhanced Directory Integration to use LDAP, any GC or DC server choice that you make is overwritten.

The default ports used for GC and DC server connections are as follows:

- GC: 3268
- DC: 389

Usage of SSL

Enhanced Directory Integration (EDI) encrypts all authentication data by default.

If your system requires encryption for both user credentials and query data, then you can enable SSL. You can use SSL for both global catalog (GC) and domain controller (DC) connections. When you use EDI, the certificate for the SSL connection must be present in the Windows certificate store. In a Windows domain, the certificate is typically already present in the certificate store on the client computer.

The default protocols and ports that are used for GC and DC server connections when you use SSL are as follows:

- GC: TCP, 3269
- DC: TCP, 636

Usage of SSL for users not part of your domain

To use Enhanced Directory Integration (EDI) with users that are not part of your domain, you must use SSL, and each user outside your domain must have a certificate.

Certificates must be in the list of trusted root certificate authority (CA) certificates on the computers of your users. If the certificates come from a third party registrar, then the certificates might chain to a trusted root CA. If your certificates chain to a root CA that is not in the default set of trusted root certificates on the computer of a Cisco Unified Personal Communicator user, then the computer cannot negotiate with the server.

Usage of Windows credentials

When client computers connect to an Active Directory server, encrypted authentication is used. If you connect to a non-Windows server, you might need to disable Windows encryption. When Windows encryption is disabled, a basic bind is used to connect to the directory. When you use a basic bind, the user credentials are transmitted in clear text.

We recommend that you use SSL in this scenario.

Related Topic

Usage of SSL, on page 74

Usage of non-Windows credentials

You might choose to use a common set of credentials for Cisco Unified Personal Communicator to authenticate for directory queries. In this scenario, you can push the credentials to all client computers.

You might use this feature if your Cisco Unified Communications system accesses a third-party directory service.

If the client computer does not provide credentials, then Enhanced Directory Integration (EDI) attempts to make an anonymous bind to the directory service.

Topics to consider before you use Enhanced Directory Integration

Before you use Enhanced Directory Integration (EDI), you must consider the following topics:

- The type of the directory that you need to connect to:
  - Global Catalog (GC)
  - Active Directory or LDAP
  - Active Directory Lightweight Directory Services (AD LDS), or Active Directory Application Mode (ADAM)
- Whether Windows authentication can be used.

- Whether the root of the directory is searched, or whether users are located in several search bases.

Related Topic

Sample configuration questions, on page 82

Enhanced Directory Integration configuration with Active Directory

For information about how to configure Enhanced Directory Integration, read the topics below.

Default configuration of Active Directory with Enhanced Directory Integration

The following table gives details of how Active Directory is configured with Enhanced Directory Integration (EDI) by default. If these configuration details do not meet your requirements, you might need to modify some of the settings appropriately.

Table 7: Default Configuration of Active Directory with EDI

Configuration Area	Description
Locating Global Catalog server	Uses DNS to locate the Global Catalog (GC) server or the domain controller (DC) for the domain of the Windows machine. The GC or DC is located by the DNS service (SRV) _gc record.
Port	3268
Default search base	Domain root, that is RootDSE.
Credentials	Connects with the credentials of the Windows user who is currently logged on.
Security	Uses a secure connection.
Preferences for searches	subtree, chaseReferrals, timeout 5s, pageSize 100, PagedTimeLimit 5s
Directory attribute names	Default Active Directory attribute names.

Related Topics

Connection configuration for Enhanced Directory Integration, on page 77
Default values for directory attributes, on page 80

Connection configuration for Enhanced Directory Integration

If the default configuration of Enhanced Directory Integration (EDI) does not meet your requirements, you might need to modify some of the settings appropriately. The following table lists the Active Directory configuration registry subkeys that can be created or modified. The subkeys are located in the following registry location:

[HKEY_CURRENT_USER\Software\Cisco Systems, Inc.\Client Services Framework\Active Directory]

The data type of the registry settings is REG_SZ, except where noted otherwise.

Keys that do not already exist must be created.

Table 8: Registry Subkeys for Active Directory Connection Configuration

Subkey Names	Description
ConnectionType	Specify how you want Client Services Framework to discover the Active Directory. Enter one of the following values: • 0: Use the Global Catalog (GC) or domain controller (DC) to discover the Active Directory server automatically. This is the default value. • 1: Use LDAP. Data type: REG_DWORD
UseSecureConnection	Specify whether Client Services Framework encrypts usernames and passwords on the connection. Enter one of the following values: • 0: Use encryption. This is the default value. • 1: Do not use encryption. Data type: REG_DWORD
UseSSL	Specify whether Client Services Framework uses SSL to connect securely to the directory. Enter one of the following values: • 0: Do not use SSL. This is the default value. • 1: Use SSL. Data type: REG_DWORD
UseWindowsCredentials	Specify whether Client Services Framework uses credentials, that is, usernames and passwords, from Windows or from another source. Enter one of the following values: • 0: Use credentials from a source other than Windows. • 1: Use Windows credentials. This is the default value. Data type: REG_DWORD

Subkey Names	Description
ConnectionUsername	If you choose to use credentials from a source other than Windows, specify the username to use when Client Services Framework connects to the Active Directory. The default is that this subkey name is not used.
ConnectionPassword	If you choose to use credentials from a source other than Windows, specify the password to use when Client Services Framework connects to the Active Directory. The default is that this subkey name is not used.
BaseFilter	Only use this subkey name if the object type that you want to retrieve with queries that you execute against Active Directory is not a user object. The default value is (objectCategory=person). The following example base filter would exclude disabled users: (&(objectCategory=person)(objectClass=user)(!(userAccountControl:1.2.840.113556.1.4.803:=2)) **Note** Remove the last bracket from all filters. This is the due to the way the filter is loaded.
SearchTimeout	Specify the timeout period for queries, in seconds. The default value is 5.
PrimaryServerName	Specify the FQDN or IP address of the primary server to connect to for directory access, if the server cannot be discovered by DNS. The default is that this subkey name is not used.
SecondaryServerName	Specify the FQDN or IP address of the backup server to connect to for directory access, if the server that cannot be discovered by DNS. The default is that this subkey name is not used.
Port1	Specify the port of the primary server that cannot be discovered by DNS.
Port2	Specify the port of the secondary server that cannot be discovered by DNS.
SearchBase1, SearchBase2, SearchBase3, SearchBase4, SearchBase5	For performance reasons, you might need to specify a location in the Active Directory from which searches begin. If you need to do this, set this subkey name to be the value of the first searchable organizational unit (OU) in the tree. The default value is the root of the tree. Specify any further search bases also.

Subkey Names	Description
DisableSecondaryNumberLookups	Specify whether users can search for the mobile, other, or home numbers of contacts, if the work number is not available. Enter one of the following values: • 0: Users can search for the mobile, other, or home numbers of contacts. • 1: Users cannot search for the mobile, other, or home numbers of contacts. The default is that this subkey name is not used.
PhoneNumberMasks	Set masks to use when users search for a phone number. For example, if a user receives a call from +14085550100, but the number is stored in Active Directory as +(1) 408 555 0100, you can ensure that the contact is found if you set the following mask: +1408|+(#) ### ### #### There is no restriction on the length of a mask string, except that the length cannot exceed the size that is allowed in registry subkey names. Typically, you do not need to use phone number masks if the phone numbers in your directory are in +E.164 format.
UseWildcards	Set this value to 1 if you want to enable wildcard searches for phone numbers in the LDAP. If you set this key to 1, the speed of searches of the LDAP might be affected, particularly when the directory attributes that are searched are not indexed. You can use phone number masks instead of wildcard searches. Typically, you do not need to use wildcard searches if the phone numbers in your directory are in +E.164 format.
UserSearchFields	This value is used to specify the Active Directory fields to search when users search for contacts. Specify one or more of the following values separated by commas: • DisplayName • UserAccountName • FirstName • LastName For example, the **UserSearchFields** key should be set to **UserAccountName,FirstName** if the administrator wants user contact searches to query the equivalent Active Directory fields. All of the above fields are searched if no value is specified. **Note** The Active Directory fields searched for UserAccountName or FirstName values may be customized if the administrator wants to restrict searches to indexed fields.

Related Topic

Phone number masks, on page 92

Default values for directory attributes

The default values for the directory attributes are the standard Active Directory attribute names. In other words, you do not need to set values for the directory attributes unless the directory to which you want to connect has attributes that are different to the Active Directory attribute names.

You specify the values for the directory attributes in the following registry key:

[HKEY_CURRENT_USER\Software\Cisco Systems, Inc.\Client Services Framework\Active Directory]

The following table lists the directory attributes, the corresponding subkey names, and their default values.

Table 9: Default Values of Subkey Names for Directory Attributes

Attribute Description	Subkey Name	Default Value
Common Name	CommonName	cn
Display Name	DisplayName	displayName
First Name	Firstname	givenName
Last Name	Lastname	sn
Email Address	EmailAddress	mail
SIP URI	SipUri	msRTCSIP-PrimaryUserAddress
Photo URI	PhotoUri	photoUri
Work Number	BusinessPhone	telephoneNumber[3]
Mobile Number	MobilePhone	mobile
Home Number	HomePhone	homePhone
Other Number	OtherPhone	otherTelephone
Preferred Number	PreferredNumber	telephoneNumber
Title	Title	title
Company Name	CompanyName	company
Account Name	UserAccount	sAMAccountName

Attribute Description	Subkey Name	Default Value
User Principal Name	Domain	userPrincipalName
Location	Location	co
Nick Name	Nickname	mailNickname
Postcode	PostalCode	postalCode
State	State	st
Street Address	StreetAddress	streetAddress

[3] This is the primary and default directory attribute for contact resolution. Other directory phone number attributes might be used to find contacts, depending on the value of the DisableSecondaryNumberLookups key.

Related Topic

Active Directory attributes that must be Indexed, on page 82

Additional directory attribute configuration

You can configure additional directory attributes if you configure Enhanced Directory Integration. You specify the values for the directory attributes in the following registry key:

[HKEY_CURRENT_USER\Software\Cisco Systems, Inc.\Client Services Framework\Active Directory]

The following table lists the additional directory attributes, the corresponding subkey names, and their default values.

Table 10: Default Values of Subkey Names for Additional Directory Attributes

Attribute Description	Subkey Name	Default Value
Enable substitution of photo URI	PhotoUriSubstitutionEnabled Data type: REG_DWORD	The default is that this subkey name is not used. Example value: True
Photo URI with a variable value	PhotoUriWithToken	The default is that this subkey name is not used. Example value: http://staffphoto.example.com/sAMAccountName.jpg
Value that gets inserted to a photo URI that has a variable value	PhotoUriSubstitutionToken	The default is that this subkey name is not used. Example value: sAMAccountName

Attribute Description	Subkey Name	Default Value
Use wildcards	UseWildcards Data type: REG_DWORD	0
Phone number masks	PhoneNumberMasks	The default is that this subkey name is not used. Example value: +1408|+(#) ### ### ####

Active Directory attributes that must be Indexed

The following Active Directory attributes must be indexed:

- sAMAccountName
- displayName
- mail
- msRTCSIP-PrimaryUserAddress

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

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

Sample configuration questions

The following table lists common questions that arise when you configure Cisco Unified Client Services Framework to use Enhanced Directory Integration (EDI). The table also lists actions that you must take depending on the answers to those questions.

Table 11: Sample Questions About Configuration of Client Services Framework to Use EDI

Configuration Question	Configuration Actions
Is the directory discoverable by DNS?	• If yes, is the directory a Global Catalog (GC) or LDAP server? ◦ If the directory is a GC, no action is required. ◦ If the directory is an LDAP directory, set the ConnectionType subkey name to 1. • If no, do the following: ◦ Set the ConnectionType subkey name to 1. ◦ Specify the appropriate values for PrimaryServerName and Port1. ◦ (Optional) Specify the appropriate values for BackupServerName and Port2. For example, if your directory is an ADAM directory, you might set these values.
Do you use SSL when connecting to the directory?	• If yes, set the UseSSL subkey name to 1. • If no, no action is required.
Can users connect to the directory with integrated Windows authentication?	• If yes, no action is required. • If no, set the values for the following subkey names: ◦ ConnectionUsername ◦ ConnectionPassword **Note** Passwords are stored in the registry unencrypted. This feature is designed to be used for well-known application accounts. An application account might be Cisco Unified Personal Communicator, where every user of Cisco Unified Personal Communicator knows the username and password.
Do you want to create a secure connection?	• If the answer is yes, no action is required. • If the answer is no, set the ConnectionSecurity subkey name to 1. If you do not specify a username and password, Client Services Framework attempts an anonymous bind to the Active Directory server.

Configuration Question	Configuration Actions
Do you want to use a simple bind?	• If yes, set the ConnectionSecurity subkey name to 1. Specify a username and password. The username must be in distinguished name (DN) format. • If no, no action is required.

Basic Directory Integration

Cisco Unified Client Services Framework can use a Basic Directory Integration (BDI) to retrieve contacts from the Active Directory server. Cisco Unified Personal Communicator receives the majority of its LDAP configuration from the LDAP Profile provided by the IM and Presence node. Only a small subset of Basic Directory Integration configuration items are configurable only through registry settings.

For information about the LDAP Profile provided, refer to LDAP directory integration.

Cisco recommends that you use Enhanced Directory Integration (EDI) because EDI provides significant advantages over BDI, as described in Feature comparison of enhanced and basic directory integration, on page 70.

The configuration you must perform if you use BDI to retrieve contacts from the Active Directory server is described here:Phone number masks, on page 92.

Group Policy administrative templates are provided with Cisco Unified Personal Communicator. You can use one of these templates to define the Client Services Framework registry settings on a system, or for groups of users. For information about how to accomplish this task, refer to Use Active Directory Group Policy administrative template to configure Client Services Framework clients, on page 84.

Use Active Directory Group Policy administrative template to configure Client Services Framework clients

Group Policy administrative templates are provided with Cisco Unified Personal Communicator. You can use one of these templates to define the Client Services Framework registry settings on a system or for groups of users.

The administrative templates included in this package provide support for deployment to a group of domain users that is managed through a Group Policy at the Active Directory level. Files intended for deployment through Group Policy have **Group_Policy** in the filename.

The administrative template files provided can be used to support Windows Server 2003 or 2008 environments. The files used depends on the Windows Server environment. These files are as follows:

Procedure

Step 1 ADM - ADM files are used for Group Policy management in a Windows Server 2003 environment. They can be used in a Windows Server 2008 environment if required.

Step 2 ADML / ADMX - ADML / ADMX files are used for Group Policy management in a Windows Server 2008 environment. They are not backward compatible to Windows Server 2003.
The procedures contained in this section should only be used a reference for deploying Group Policies. If you are not already familiar with the Group Policy management process, consult the Windows Server 2003 or Windows Server 2008 documentation provided by Microsoft. This documentation provides full instructions on Group Policy management and should be consulted before deployment.

This section contains the following procedures:

- Deploy Group Policy administrative templates in a Windows Server 2003 environment, on page 85
- Deploy Group Policy administrative templates in a Windows Server 2008 environment, on page 86

Note Registry keys may be deployed on local systems for testing purposes.

Deploy Group Policy administrative templates in a Windows Server 2003 environment

Use the following procedure to guide the deployment of Group Policy administrative templates in a Windows Server 2003 environment.

Procedure

Step 1 Launch **Active Directory Users and Computers**.

Step 2 Browse to the container containing the users to which the new policy will be applied.

Step 3 View the container properties and choose the **Group Policy** tab.

Step 4 Create a new Group Policy object with the desired name.

Step 5 Highlight the new object and click **Edit**.

Step 6 Add a new template to the **Administrative Templates** section.

Step 7 Right click on the **Administrative Templates** folder and choose **Add/Remove Templates**.

Step 8 Browse to the location of the desired ADM file.

Step 9 Choose the file and click **OK**.

Step 10 A folder named **Cisco Unified Client Services Framework** or **Cisco Unified Personal Communicator** should be present below the **Administrative Templates** folder.

Step 11 Manage and deploy registry keys to the chosen access control group from here.

Deploy Group Policy administrative templates in a Windows Server 2008 environment

Use the following procedure to guide the deployment of Group Policy administrative templates in a Windows Server 2008 environment.

Procedure

Step 1 Browse to the location of the policy definitions on the Active Directory server. These are typically found in **C:\Windows\PolicyDefinitions**.

Step 2 Copy the desired ADMX file to that location.

Step 3 Open the **en-US** folder.

Step 4 Copy the desired ADML file to that location.

Step 5 Launch the **Group Policy Management** console. This is typically found on the **Start Menu** at **Start** > **All Programs** > **Administrative Tools**.

Step 6 Right click the container which holds the users to which the policy will be applied.

Step 7 Choose **Create a GPO in this domain and, Link it here**.

Step 8 Provide an appropriate name.

Step 9 Click **OK**.

Step 10 Expand the chosen user container. It should contain the newly created GPO with the provided name.

Step 11 Right click the GPO object and choose **Edit**.

Step 12 Expand the **Policies** folder.

Step 13 Expand the **Administrative Templates** folder.

Step 14 A folder named **Cisco Unified Client Service Framework** or **Cisco Unified Personal Communicator** will be present depending on the imported policy file.

Step 15 Manage and deploy registry keys to the chosen access control group from here.

Registry location on client machines

After the administrative templates are configured and pushed to a client, the key values are located in the following registry locations:

- Keys contained in the Dial via Office Settings folder:
  - HKEY_CURRENT_USER\Software\Policies\Cisco Systems, Inc.\Unified Communications\CUPC8
- Keys used for Basic Directory Integration:
  - HKEY_CURRENT_USER\Software\Policies\Cisco Systems, Inc.\Client Services Framework\AdminData
- Keys used for Enhanced Directory Integration:
  - HKEY_CURRENT_USER\Software\Policies\Cisco Systems, Inc.\Client Services Framework\Active Directory

LDAP registry settings

The following table lists the registry subkeys that you may use for BDI or EDI LDAP configuration. If you use Enhanced Directory Integration (EDI) instead of Basic Directory Integration (BDI), you might not need to specify values for any registry settings.

Table 12: LDAP Registry Subkeys

Subkey Names	Description
LDAP_enableWildcardMatches ForPhoneNumberSearches	Set this value to False to disable wildcard searches for phone numbers in the LDAP. If you set this key to True, the speed of searches of the LDAP might be affected. You can use phone number masks instead of wildcard searches. Typically, you do not need to use wildcard searches if the phone numbers in your directory are in +E.164 format.
LDAP_SearchFields	Specify the Active Directory field or fields to search when users search for contacts. Specify one or more of the following values, separated by spaces: • LDAP_AttributeName_UserAccountName • LDAP_AttributeName_lastName • LDAP_AttributeName_firstName • LDAP_AttributeName_displayName The default behavior is that all of these fields are searched. You might want to search fewer of these fields. For example, you might want to search only those fields that are indexed.

Subkey Names	Description
LDAP_UriSchemeName	The Active Directory attribute that is the value that is specified in the LDAP_AttributeName_uri subkey name. Typically, this Active Directory field value is prefixed by a scheme name, for example, one of the following: • im: • sip: If a scheme name is used, you must specify the scheme name in the LDAP_UriSchemeName subkey name to ensure an exact match for searches. If no value is specified in the LDAP_UriSchemeName subkey name, a wild card search is used. The wild card search might adversely affect Active Directory performance, especially if the field is not indexed. For example, if the Active Directory field msRTCSIP-PrimaryUserAddress is populated with URIs of the format sip:mweinstein@example.com, the following is a recommended configuration: • LDAP_AttributeName_uri subkey name: **msRTCSIP-PrimaryUserAddress** • LDAP_UriSchemeName subkey name: **sip:**
LDAP_AttributeName_uri	Registry Sub keys to Use to Map Client Services Framework Searches to Active Directory. Typical value = msRTCSIP-PrimaryUserAddress

Subkey Names	Description
LDAP_SearchByUsername	Enable or disable voicemail LDAP searches for phone number and email address. If disabled, the User ID from the Unity email address is used. For example, for a user configured as 'calane@cisco.com' in Unity, the LDAP search performed in voicemail will be for user account name 'calene'.Allows you to disable voicemail LDAP searches for phone number and email address and instead uses the User ID from Unity email address. For 'pizza-guy' voicemail contacts, a telephone number lookup is still performed. This registry key is a String value located in HKEY_CURRENT_USER\Software\Policies\Cisco Systems, Inc.\Client Services Framework\AdminData. Set the key to **True** to enable this functionality and **False** to disable it. **False** is the default.
LDAP_DisableSecondaryNumber Lookups	Specify whether users can search for the mobile, other, or home numbers of contacts, if the work number is not available. Enter one of the following values: • 0: Users can search for the mobile, other, or home numbers of contacts. • 1: Users cannot search for the mobile, other, or home numbers of contacts. The default is that this subkey name is not used.
EnableNativeDirectoryProvider	Specify whether to use Enhanced or Basic Directory Integration to get contact information from Active Directory. Enter one of the following values: • 0: Use Basic Directory Integration. This is the default value. • 1: Use Enhanced Directory Integration Data type: REG_SZ

Subkey Names	Description
LDAP_PhoneNumberMask(BDI) / PhoneNumberMasks (EDI)	Set masks to use when users search for a phone number. For example, if a user receives a call from +14085550100, but the number is stored in Active Directory as +(1) 408 555 0100, you can ensure that the contact is found if you set the following mask: +1408|+(#) ### ### #### There is no restriction on the length of a mask string, except that the length cannot exceed the size that is allowed in registry subkey names. Typically, you do not need to use phone number masks if the phone numbers in your directory are in +E.164 format.
LDAP_DisableNumberLookups	When an incoming call is received, or an outgoing call is made, to a number not in the users contact list or communication history, an LDAP query is performed to find that number within the directory. If a match is found, the client can then display contact information about this number. This lookup can be disabled by setting this registry key to **false**. This will disable all phone number lookups. The client will not be able to display contact information for any incoming or outgoing numbers if this value is set to **false**.

Directory attribute default values are the standard Active Directory attribute names. Directory attributes are only configured in the registry when using EDI and default values are not sufficient. BDI uses the LDAP Profile values provided by the IM and Presence node.

The following table outlines the directory attributes and their default values.

Table 13: Directory Attribute Values

Directory Attribute	Value
BusinessPhone	Business Phone attribute (default value is: 'telephoneNumber')
CommonName	Common Name attribute (default value is: 'cn')
CompanyName	Company name attribute (default value is: 'company')
DisplayName	Display name attribute (default value is: 'displayName')

Directory Attribute	Value
DomainName	Domain name attribute (default value is: 'userPrincipalName')
EmailAddress	Email address attribute (default value is: 'mail')
Firstname	Firstname attribute (default value: 'givenName')
HomePhone	Home phone attribute (default value: 'homePhone')
Lastname	Lastname attribute (default value is: 'sn')
Location	Location attribute (default value is: 'co')
MobilePhone	Mobile number attribute (default value is: 'mobile')
Nickname	Nickname attribute (default value is: 'mailNickname')
OtherPhone	Other phone attribute (default value is: 'otherTelephone')
PhotoUri	Photo Uri attribute (default value: 'photoUri')
PostalCode	Post code attribute (default value: 'postalCode')
PreferredNumber	Preferred Number attribute (default value 'telephoneNumber')
SipUri	An IP Uri attribute (default value: 'msRTCSIP-PrimaryUserAddress')
State	State attribute (default value: 'st')
StreetAddress	Street Address attribute (default value: 'streetAddress')
Title	Title attribute (default value 'title')
UserAccount	User account name attribute (default value 'sAMAccountName')

Related Topics

Enhanced Directory Integration, on page 73
Phone number masks, on page 92

Phone number masks

You can set masks to use when the Cisco Unified Personal Communicator searches Active Directory for a phone number.

When you place a call, the Cisco Unified Personal Communicator might search the Active Directory to get the contact information that corresponds to a phone number. When you receive a call, the Cisco Unified Personal Communicator might search the Active Directory to resolve a phone number to a contact name. If the phone numbers in your Active Directory are not in +E.164 format, then these searches might not resolve to users in your Active Directory. You can apply masks to searches to counteract this problem.

For example, if a user receives a call from +14085550100, but the number is stored in Active Directory as +(1) 408 555 0100, you can ensure that the contact is found if you set the following mask:

+1408|+(#) ### ### ####

The mask is applied to the number before Active Directory is searched for the number. If you configure masks correctly, directory searches succeed as exact match lookups. Therefore, these searches have a minimal impact on the performance of the directory server.

Typically, you do not need to use phone number masks if the phone numbers in your directory are in +E.164 format. You can use phone number masks with either Enhanced Directory Integration (EDI) or Basic Directory Integration (BDI).

Related Topics

Elements of phone number masks, on page 92
Subkey names for specifying masks, on page 94

Elements of phone number masks

The following table describes the elements that you can include in masks:

Element	Description
Phone number pattern	You must specify a number pattern to which you want to apply the mask. For example, to specify a mask for searches that begin with +1408, you can use the following mask: +1408|+(#) ### ### #### When you identify number patterns to which to apply masks, you can use multiple masks with the same number of digits. This enables the mask to deal with scenarios where phone numbers at different company sites might have the same number of digits, but with different patterns. For example, your company might have site A and site B, and each site maintains their own directory information. You could end up with two formats for number, such as the following: +(1) 408 555 0100 +1-510-5550101 In this scenario, to resolve +E.164 numbers of 12 digits correctly, you can set up the phone masks as follows: +1408|+(#) ### ### ####|+1510|+#-###-#######
Pipe symbol ("|")	Separate pairs of number patterns and masks with a pipe symbol, as shown in the following example: +1408|+(#) ### ### ####|+34|+(##) ### #### When you add multiple masks for your searches, each mask must have a different number pattern. When the Cisco Unified Personal Communicator searches Active Directory for a phone number, only one mask is applied to the phone number before the search. If a phone number matches more than one number pattern, then the number pattern that matches the most digits in the phone number is chosen, and the associated mask is applied.
Wildcard character	You can also use wildcard characters in masks. Use an asterisk (*) to represent one or more characters. For example, you can set a mask as follows: +3498|+##*##*###*#### If Cisco Unified Personal Communicator searches Active Directory for the +E.164-format number +34985550199, the search can find any of the following formats in the directory: +34(98)555 0199 +34 98 555-0199 +34-(98)-555.0199

Element	Description
Reverse mask	You can also use a reverse mask. A reverse mask is applied from right to left. The mask and phone number pattern are traversed from right to left, and each character in the mask is checked to decide whether to copy a digit from the phone number. Use reverse masks if you want to do both of the following when Cisco Unified Personal Communicator searches Active Directory: • Modify some of the leading digits of phone numbers. • Format the numbers to match your directory format. For example, you can set a reverse mask as follows: +3498|R+34 (98) 559 #### If this mask is applied to +34985550199, the result is +34 (98) 559 0199. You can use a mixture of forward and reverse masks.

Related Topics

Subkey names for specifying masks, on page 94

Subkey names for specifying masks

Phone Number lookup mask locations for EDI and BDI are specified as follows:

Type of Directory Integration	Set Mask in This Subkey Name
Enhanced Directory Integration (EDI)	PhoneNumberMasks in [HKEY_CURRENT_USER\Software\Cisco Systems, Inc.\Client Services Framework\Active Directory]
Basic Directory Integration (BDI)	LDAP_PhoneNumberMask in [HKEY_CURRENT_USER\Software\Cisco Systems, Inc.\Client Services Framework\AdminData]

Related Topics

Connection configuration for Enhanced Directory Integration, on page 77
Phone number masks, on page 92
Elements of phone number masks, on page 92

Contact photo retrieval

Cisco Unified Client Services Framework can retrieve photo information for contacts as follows:

- (Enhanced Directory Integration only) Retrieve a binary photo from Active Directory

- (Basic and Enhanced Directory Integration) Retrieve a static URL from Active Directory
- (Enhanced Directory Integration only) Retrieve a dynamically-created URL from Active Directory

Binary photos retrieval from Active Directory

A photo is stored as a binary object in Active Directory. Cisco Unified Client Services Framework retrieves the attribute content of the directory attribute that is defined by the PhotoUri setting.

Enhanced Directory Integration (EDI) parses the content of the attribute returned. If the attribute contains binary data, the content displayed as a JPEG photo. If the attribute contains a URL, the photo is retrieved from the URI.

If a directory user object has a photo stored in the thumbnailphoto attribute setting, set PhotoUri to thumbnailphoto if you want the Cisco Unified Client Services Framework to retrieve the photo from this field. You can also store a photo in the jpegPhoto attribute in Active Directory.

Microsoft Lync and Microsoft Outlook also use the thumbnailphoto binary attribute to retrieve photos.

Static URL retrieval from Active Directory

You can retrieve a static URL that points to a photo from Active Directory in both Enhanced and Basic Directory Integration.

Enhanced Directory Integration (EDI) parses the content of the attribute returned. If the attribute contains binary data, the content displayed as a JPEG photo. If the attribute contains a URL, the photo is retrieved from the URI. For example, the attribute might contain a URL structured as follows:

http://staffphoto.example.com/mweinstein.jpg

The string that is stored in the Active Directory is a static URI string that points to a location of a photo.

Note The basic directory attribute map uses a different setting for attribute name. The EDI PhotoUri must be populated if the photo attribute is not stored in an Active Directory field called PhotoUri.

Dynamic URL retrieval from Active Directory

You can configure EDI to construct a photo URL dynamically based on another directory attribute. The photo URL is constructed from a base URL and a substitution token.

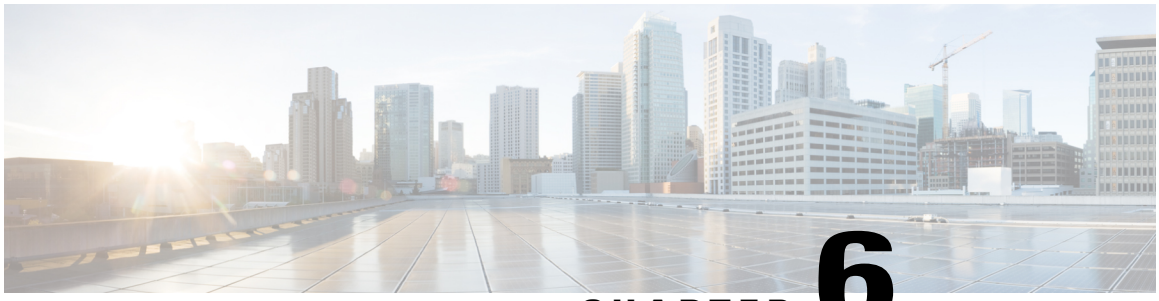
For example, if your organization maintains a web server of staff photos, and the filenames of the photos match the user account names, then you can create the following configuration:

Setting	Value
UserAccount	sAMAccountName
PhotoUri	http://staffphoto.example.com/PHOTONAME.jpg
PhotoUriSubstitutionEnabled	true

Setting	Value
PhotoUriSubstitutionToken	PHOTONAME

The value of the string PHOTONAME is replaced with the directory attribute specified by the AccountName setting. If you use the preceding configuration, a user with a sAMAccountName of mweinstein results in the following URL:

http://staffphoto.example.com/mweinstein.jpg



CHAPTER 6

Additional registry keys configuration for Cisco Unified Personal Communicator

This chapter contains information about the additional registry key customizations provided by Cisco Unified Personal Communicator over and above those set aside for Active Directory.

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:

- Registry key mapping, page 98
- Video registry setting configuration, page 98
- CTI registry setting configuration, page 98
- Web conferencing registry setting configuration, page 98
- Dial via Office registry setting configuration, page 99
- Additional registry setting configuration, page 99

Registry key mapping

All registry keys discussed in this chapter are located in HKEY_CURRENT_USER\Software\Policies\Cisco Systems, Inc.\Client Services Framework\AdminData, with the exception of those associated with Dial via Office (DVO) functionality, unless otherwise noted. Registry keys associated with Dial via Office are located in HKEY_CURRENT_USER\Software\Policies\Cisco Systems, Inc.\Unified Communications\CUPC8.

Video registry setting configuration

The following table lists the registry subkeys that you must use to specify the video registry settings.

Table 14: Video Registry Settings

Subkey Names	Description
VideoEnabled	Setting this key to 'false', will disable all video capabilities in CUPC. Video capabilities are enabled by default.

CTI registry setting configuration

The following table lists the registry subkeys that you must use to specify CTI registry settings.

Table 15: CTI Registry Settings

Subkey Names	Description
CtiServerJtapiLibDownloadPort	Allows for an alternative port to be used to download the Jtapi.jar file from CUCM. This file is used to support deskphone mode. By default, port 80 is used. Currently, the only other alternative port which can be used is '8080'.

Web conferencing registry setting configuration

The following table lists the registry subkeys that you must use to specify web conferencing registry settings.

Table 16: Web Conferencing Registry Settings

Subkey Names	Description
WebConfSSOIdentityProvider	If using WebEx SSO, enter the name of the provider type such as 'meetingplace'.

Related Topics

Conferencing server configuration for Cisco Unified Personal Communicator, on page 56

Dial via Office registry setting configuration

The following table lists the registry subkeys that you must use to specify Dial via Office registry settings.

Table 17: Dial via Office Registry Settings

Subkey Names	Description
DVOModeEnabled	Setting this key to **false** will disable the Dial via Office functionality introduced in Cisco Unified Personal Communicator 8.5(2). This feature is enabled by default

For information about configuring this feature, see the *Release Notes for Cisco Unified Personal Communicator Release 8.5*.

Additional registry setting configuration

The following table lists additional registry keys that provide additional Cisco Unified Personal Communicator customizations.

Table 18: Additional Registry Settings

Subkey Names	Description
AudioCustomRingtone	Cisco Unified Personal Communicator supports the use of custom ring tones. Cisco will provide a set of custom ringtones. Only these ringtones are supported. The ringtone can be specified in a registry setting or in a directory named **ringtone** in the CSF appdata / roaming directory. The ringtone must be copied to that location by the administrator. To change a ringtone, the new file is copied into the correct location and the client restarted. The default is that this subkey name is not used.

Subkey Names	Description
DeskphoneStartupMode	This key is used to start Cisco Unified Personal Communicator in deskphone mode. In a VDI environment the client needs to be started in deskphone mode. To meet this requirement, this registry subkey has been introduced. If the value of this key is set to **1,** the client will start in deskphone mode. If is not set, or has a value other than 1, the client will start up by using the last phone mode the client used during start up. The default is that this subkey name is not used.
AutomaticTetheredPhoneSelection	This key is used to set the Automatic Tethered Phone Selection feature. Cisco Unified Personal Communicator users will often have multiple deskphone devices assigned to them but only one that is tethered to their workstation through an Ethernet cable. This feature ensures that the tethered phone is always chosen when a Cisco Unified Personal Communicator user enters deskphone mode. This feature is disabled by default. The following usage scenarios outline the operation of this feature when it is enabled through the registry: • If the user manually changes their deskphone device from the tethered device to a new one while the device is available, the new device will be chosen and automatic selection will be switched off. • If the user manually changes their deskphone device from tethered while the device is not available, the new phone device will be chosen but when the tethered phone becomes available again Cisco Unified Personal Communicator will automatically switch back to it. • If the user manually changes the deskphone device to tethered, automatic selection will be switched on. • If the user changes phone modes, automatic selection will be switched on. **Note** This feature will also work if the user is logged in to their tethered phone with extension mobility.

INDEX

A

application deployment 8, 10, 13, 67
  adding new user after 67
  deploying in Mac OS environment 10
  deploying in Windows environment 10
  deploying to a shared location 10
  installer package names 8
  updating 13
  using a software deployment tool 10
  using the client computer installer 10
application dialing rules 30
  configuring 30
  described 30
application profiles 65, 66
  changing for a single user 65
  changing for multiple users 66
audio devices 13
  configuration 13
authentication methods 54, 56
  Cisco Unified MeetingPlace 56
  Cisco Unity 54
availability 27
  status and firewalls 27

C

camera drivers 8, 10, 13
  deploying in Windows environment 10
  installer package names 8
  updating 13
Cisco Unified Communications Manager server 32
  Client Services Framework device type 32
Cisco Unified IP Phones 14
  DND behavior in CUPC, described 14
Cisco Unified Personal Communicator 13, 14, 31, 37
  DND behavior, described 14
  sharing the line with the IP Phone 37
  soft-phone device name guidelines for CUCM 37
  transformed dialed numbers, described 31
Cisco Unified Personal Communicator *(continued)*
  uninstalling 13
    previous Mac version 13
  updating the application 13
  URL for downloading latest software 13
Client Services Framework device type 32
conferencing servers 56
  configuring 56
  web meetings 56
    participant privileges 56
configuration file for softphone mode 42
COP file 32
  for Client Services Framework device type 32
CTI gateway 34, 35
  server profiles 35
    creating 35
    dynamically created 35
  specifying 34, 35
    redundant servers 35
    server names and addresses 34

D

desk-phone mode 14, 33
  and the CTI gateway 33
  DND behavior and Call Reject 14
  DND behavior and Ringer Off 14
directory lookup rules 30
  configuring 30
  described 30

E

extension mobility 32
  configuring 32

F

failover, See TFTP servers
firewalls 27
  configuring 27

H

headsets 13, 14
  configuration 13
  use of third-party 14

I

IMAP 52
information needed by users 16
initial deployment 67
  adding new user after 67
Internet Mail Access Protocol, See IMAP

L

licensing 37
  adjunct 37
  configuring 37

M

media resources for videoconferencing 47

N

network ports and firewalls 27
new user 67
  configuration after initial deployment 67

P

point-to-point video calls 37, 46
  configuring device as soft phone 37
  configuring VT camera 46
profiles 35
  automatically created 35
proxy listener 43

R

redundancy 35, 43
  CTI gateway 35
  TFTP server 43

S

server configuration 52, 54, 56
  Cisco Unified MeetingPlace 56
  Cisco Unity 54
  Cisco Unity Connection 52
shared location deployment 10
soft-phone device naming guidelines for CUCM 37
soft-phone mode 14, 42
  configuration file 42
  DND behavior, described 14
  failover, described 42
Software Center 13
  URL for 13
software deployment tools 10
SSL 56
  Cisco Unified MeetingPlace certificates 56

T

TFTP servers 42
  addresses 42
  failover 42
    described 42

U

user information 16
  providing 16

V

video telephony camera 46
  configuring 46
videoconferencing resources 46, 47
  configuring the video conferencing bridge 47
  installing the VT camera 46
voice-mail servers 52, 54
  allowing message body access 52
  configuring 52, 54
    Cisco Unity Connection 52
    Cisco Unity with Exchange 54
  setting class of service 52