



Installation Guide for Cisco Unified Communications Integration for Microsoft Office Communicator Release 8.0

July 7, 2011

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

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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

Installation Guide for Cisco Unified Communications Integration for Microsoft Office Communicator Release 8.0
© 2010 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Overview of Cisco Unified Communications Integration for Microsoft Office Communicator 1-1

Cisco UC Integration for Microsoft Office Communicator 1-1

Installation Prerequisites 1-3

CHAPTER 2

Configuring Servers for Cisco Unified Communications Integration for Microsoft Office Communicator 2-1

How to Configure Active Directory Server and OCS Server 2-1

E.164 Formatting 2-2

Phone Numbers for Active Directory Users Must Use +E.164 Formatting 2-2

Enabling Users for OCS 2-2

Configuration of Telephony Options for Users 2-3

Updating OCS Address Book Manually 2-3

Verifying OCS Address Book Synchronization 2-4

Dial Plan Options for Cisco UC Integration for Microsoft Office Communicator 2-4

Dialing Rules Required for Cisco UC Integration for Microsoft Office Communicator 2-5

Application Dialing Rules 2-5

Directory Lookup Dialing Rules 2-6

How to Configure Cisco Unified Communications Manager Server 2-8

Prerequisites for Configuring Cisco Unified Communications Manager 2-8

Cisco Unified Client Services Framework Device Type 2-8

Enabling LDAP Synchronization 2-9

Enabling LDAP Authentication 2-10

Creating Client Services Framework Devices and Directory Numbers for Users 2-10

Adding Users to User Groups and Associating Controlled Devices 2-12

How to Configure Cisco Unified IP Phones for Video 2-13

Connecting a Cisco Unified IP Phone to the Network and Your Computer 2-13

Enabling Video for a Cisco Unified IP Phone 2-13

Securing IP Phones 2-14

Configuring Cisco Unified Communications Manager for Ad-Hoc Video Conferencing 2-14

(Optional) Specifying a Minimum Number of Video-Capable Participants for Ad-Hoc Conferences 2-15

How to Make Cisco Unified Communications Manager Dialing Rules Accessible 2-15

Verifying That Dialing Rules Are Configured on Cisco Unified Communications Manager 2-16

Generating Copies of the Dialing Rules 2-16

Verifying That Copies of the Dialing Rules Were Generated 2-17

- Restarting the TFTP Service 2-17
- Ensuring That Cisco UC Integration for Microsoft Office Communicator Clients Are Restarted 2-18
- Configuring Failover to Cisco Unified Survivable Remote Site Telephony (SRST) 2-18
- How To Configure Cisco Unified MeetingPlace 2-19
 - Meeting Types and Authentication 2-19
 - Reservationless Meetings 2-19
 - Authentication 2-19
 - Reserving Audio and Video Resources 2-20
 - Configuring a Cisco Unified MeetingPlace Application Server for Ad-Hoc Video Conferencing 2-20
 - Configuring a Cisco Unified MeetingPlace Application Server for Scheduled Video Conferencing 2-21
 - Adding Custom Cisco Unified MeetingPlace Template Files to a Cisco Unified MeetingPlace 7.x Web Server 2-21
- How to Configure Cisco Unity Server for Voicemail Access 2-22
 - Installing the Voicemail Web Service (VMWS) 2-22
 - Setting the DCOM Permissions 2-22
 - Testing That the Voicemail Web Service Is Accessible 2-23
- How to Configure Cisco Unity Connection Server for Voicemail Access 2-23
 - Configuring User Access 2-23
 - Enabling Secure Access to Voice Messages 2-24

CHAPTER 3

Configuring Client Computers for Cisco Unified Communications Integration for Microsoft Office Communicator 3-1

- About Client Computer Configuration 3-1
- Location of Client Services Framework Configuration Data 3-2
- Configuring Value Names for the Client Services Framework Client Integration 3-2
 - Specifying TFTP, CTIManager, and CCMCIP Server Value Names 3-3
 - Specifying Cisco Unified MeetingPlace Server Value Names 3-4
 - Specifying Voicemail and Visual Voicemail Value Names 3-4
 - Specifying Video Value Names 3-6
 - Specifying Security Certificate Value Names 3-6
 - Specifying LDAP Value Names 3-7
 - Specifying Account Credential Synchronization Value Names 3-10
 - Using an Active Directory Group Policy Administrative Template to Configure Client Services Framework Clients 3-10
- Enabling LDAP Over SSL 3-11
 - Creating a Certificate on the Active Directory Server 3-11
 - Installing the Certificate on the Client Computer 3-11
 - Configuring Client Services Framework 3-12

Configuring Microsoft Office Communicator 2007 to Use HTTPS to Access Custom Availability Statuses	3-13
Microsoft Office Communicator 2007 R1	3-13
Microsoft Office Communicator 2007 R2	3-13
Location of Custom Availability Statuses File	3-14
Configuration of Policies for Microsoft Office Applications	3-14
Microsoft Office Communicator Policies	3-14
Microsoft Office Phone Policy	3-15
About the Client Services Framework Cache and LDAP Searches	3-15
Incoming Calls	3-16
Outgoing Calls to Contacts Who Are Enabled for OCS	3-16
Outgoing Calls to Contacts Who Are Not Enabled for OCS	3-17
Outgoing Calls to Microsoft Outlook Contacts	3-17
How to Configure Cisco UC Integration for Microsoft Office Communicator Clients for Secure Access to Cisco Unified MeetingPlace	3-18
Configuring Secure Access to Cisco Unified MeetingPlace	3-18
Downloading the IIS Certificate from Cisco Unified MeetingPlace	3-18
How to Configure Cisco UC Integration for Microsoft Office Communicator Clients to Enable Secure Voicemail Access	3-19
Configuring Secure Voicemail Access to a Cisco Unity Server	3-19
Downloading the IIS Certificate from Cisco Unity	3-19
Configuring Secure Voicemail Access to a Cisco Unity Connection Server	3-20
Downloading the Tomcat Certificate from Cisco Unity Connection	3-20
Installing Security Certificates on Client Computers	3-21

CHAPTER 4**Installing Cisco Unified Communications Integration for Microsoft Office Communicator 4-1**

Removing Cisco Unified Video Advantage	4-1
Cisco UC Integration for Microsoft Office Communicator Deployment	4-1
Executable File	4-2
Windows Installer (MSI) File	4-3
Deployment Options	4-3
Automated Mass Deployment	4-3
Standalone Installation	4-4
Upgrading Cisco UC Integration for Microsoft Office Communicator	4-4
Information to Provide to Users After Installation	4-4

CHAPTER 5**Support for Microsoft Business Productivity Online Standard Suite 5-1**

Requirements for Using Cisco UC Integration for Microsoft Office Communicator with BPOS	5-1
---	-----

Architecture of Cisco UC Integration for Microsoft Office Communicator in a BPOS Environment 5-2

User Phone Numbers Must Use +E.164 Formatting 5-2

User Authentication 5-3

Using Cisco UC Integration for Microsoft Office Communicator with Microsoft Exchange in a BPOS Environment 5-3

CHAPTER 6

Troubleshooting Cisco Unified Communications Integration for Microsoft Office Communicator 6-1

Setting Logging Levels Before You Create a Problem Report 6-1

Moving a Device to Another Cluster 6-2

How to Resolve General Problems with the Integration 6-3

 Cisco UC Integration for Microsoft Office Communicator Fails to Start 6-4

 Cisco UC Integration for Microsoft Office Communicator Is Slow To Start 6-5

 Users Cannot See the Cisco UC Integration for Microsoft Office Communicator Menu Items 6-5

 Cisco Unified IP Phone 7931G Users Cannot Control Desk Phone from Cisco UC Integration for Microsoft Office Communicator 6-5

 Audio Devices Are Selected Incorrectly 6-6

 Cisco UC Pane Takes a Long Time to Connect 6-6

 Cisco UC Pane Stops Responding If Windows Security Fails 6-6

 Incorrect Caller Name Displayed for Shared Lines 6-7

 Users with More Than One Directory Number Not Added to Conference Call 6-7

 CAST Connection from IP Phone Times Out 6-8

 Users Lose Control of the Active Call on the Desk Phone 6-8

 Users Cannot See the Participant List for the Conference Call 6-8

 Participant List for the Conference Call is Incorrect 6-8

 Numbers Published by Users in Microsoft Office Communicator Not Recognized 6-8

 Cisco UC Integration for Microsoft Office Communicator Menu Items Available but Not Functional 6-9

 Call Ends Unexpectedly 6-9

 Users Can Only Control One Line on Phones Configured for Multiple Lines 6-9

 Cannot See All Calls in Progress on Cisco Unified IP Phone 9900, 8900, and 6900 Model Series 6-9

 Conversation History Events Marked as Unread 6-10

How to Resolve Synchronization Problems 6-10

 Users See “Cannot Synchronize...” Error Message 6-10

 Users See “Cannot Synchronize... Communicator 2007” Error Message 6-10

How to Resolve Availability Status Problems 6-11

 “Inactive” and “Away” Availability Statuses and Custom Availability Statuses 6-11

 “On the Phone” Availability Status Not Available in Some Locales 6-11

 Availability Status Incorrect for Previously-Called Contacts 6-12

Availability Status Incorrect After a Call Ends	6-12
Availability Status Is Reset from "Do Not Disturb" to "Available"	6-13
Availability Status Does Not Return to Initial Status After Call Ends	6-13
How to Resolve Click to Call Problems	6-13
Users Cannot See "Call" or "Call with Edit" in Microsoft Excel 2003 or Word 2003	6-14
Users Cannot See "Call" or "Call with Edit" in Microsoft Word 2003 or Word 2007	6-14
Users Cannot See "Call" or "Call with Edit" in Microsoft Excel, Outlook, PowerPoint, or Word	6-15
Users Cannot See "Additional Actions" Menu in Microsoft Outlook Contacts	6-15
How to Resolve Instant Message Window Problems	6-16
Instant Message Window Closes When You Try to Call a Contact Who Has No Number in LDAP	6-16
Instant Message Window Displayed When Users Select the Place a Call Menu Item	6-16
Meeting URL Displayed in the Instant Message Window Does Not Work	6-16
How to Resolve Voicemail Problems	6-17
Deleted Voice Messages Might Appear as Not Deleted	6-17
How to Resolve Video Problems	6-17
Users Cannot Use Video Features on Their Computers When They Use Their Desk Phone	6-17
Users Cannot See Video in Ad-Hoc Conference Calls	6-18
How to Resolve Camera Problems	6-18
Camera Troubleshooting Tips	6-18
Some Cameras Zoom In Suddenly During a Call	6-18
How to Resolve LDAP Problems	6-19
How Do I Determine Which LDAP Server OCS Is Using?	6-19
"Host/Network reports server unavailable"	6-19
"The server has rejected the provided credentials"	6-19

APPENDIX A**Normalization Rules for OCS A-1****APPENDIX B****Enabling Display of Photos in Notification Windows, the Conversations Window, and Contact Cards B-1**

Adding the Active Directory Schema Snap-In	B-1
Creating the photoUri Attribute	B-2
Setting a Default Value for the photoUri Attribute Using ADSI Edit	B-2
Enabling the ADSI Edit Application	B-3
Configuring IIS to Display Photos	B-4
Verifying the User Object	B-4



CHAPTER 1

Overview of Cisco Unified Communications Integration for Microsoft Office Communicator

Revised: July 7, 2011

- [Cisco UC Integration for Microsoft Office Communicator, page 1-1](#)
- [Installation Prerequisites, page 1-3](#)

Cisco UC Integration for Microsoft Office Communicator

The Cisco UC Integration for Microsoft Office Communicator adds a Cisco UC pane at the bottom of the Microsoft Office Communicator window. Users can perform the following tasks from the Cisco UC pane:

- Place and receive phone calls, including high-definition video calls.
- Start meetings to talk to, and to share documents with, one or more people.
- Start and participate in conference calls.
- Transfer your calls to other contacts, or depending on your configuration, to a mobile device or other remote device.
- Forward your calls to your voicemail service, another contact, or another number.
- Park your call, then retrieve the call from another device.
- Call your voicemail service.
- Access voice messages visually.
- Display your conversation history.
- (Optional) Save your conversation history in Microsoft Outlook.
- Set options for the Cisco UC pane.
- Switch from using your computer for phone calls to using your desk phone, and switch back.

You can also use Cisco UC Integration for Microsoft Office Communicator to do the following:

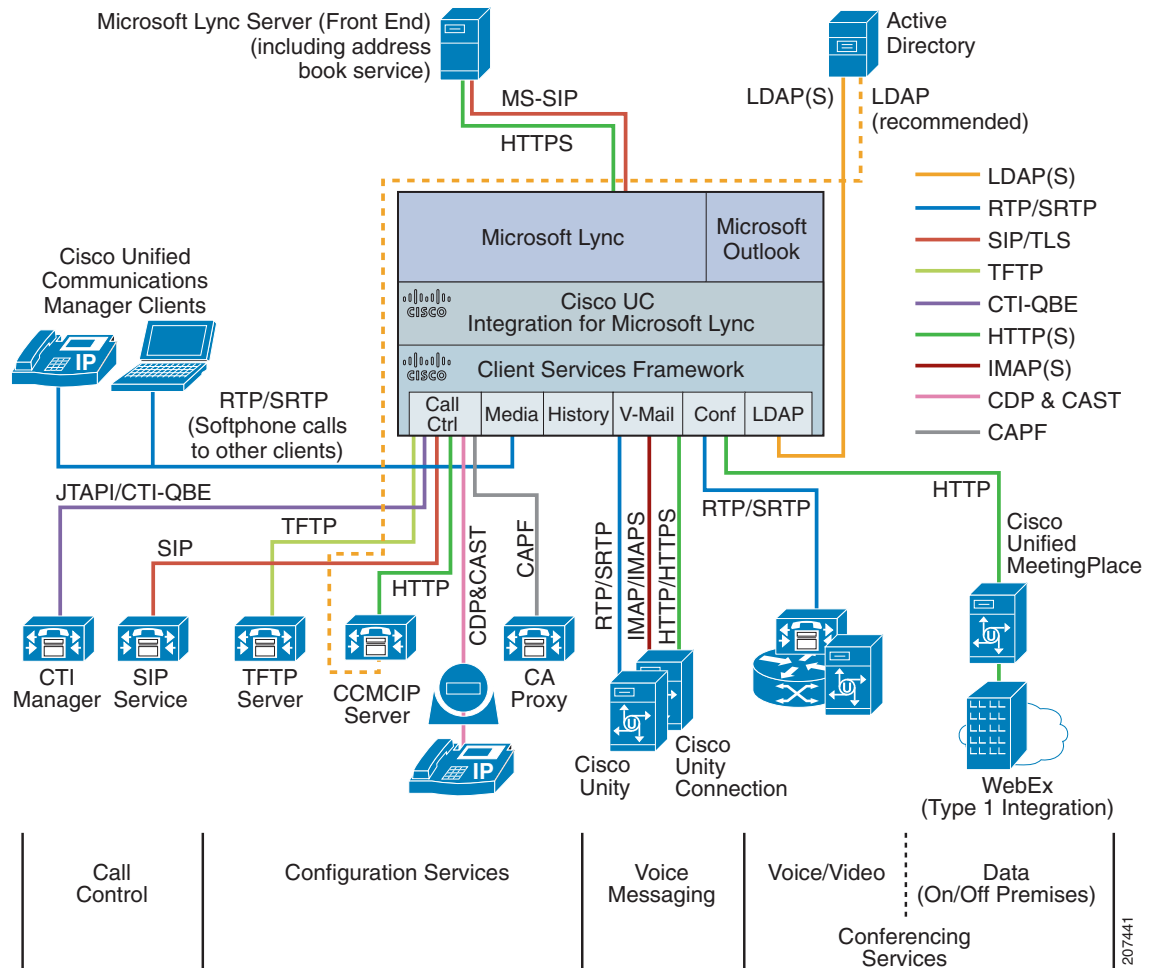
- (Optional) Use the click-to-call feature to place audio and video calls from within Mozilla Firefox and the following Microsoft applications: Excel, Internet Explorer, Outlook, PowerPoint, Sharepoint, and Word.

- (Optional) Use the click-to-call feature to place calls to numbers in your clipboard.

Cisco UC Integration for Microsoft Office Communicator integrates closely with Microsoft Office Communicator. Cisco UC Integration for Microsoft Office Communicator updates the availability status of users automatically. Users can send instant messages through Microsoft Office Communicator to contacts with whom they are currently having a conversation through the Cisco UC pane.

Cisco UC Integration for Microsoft Office Communicator interacts with servers and applications as shown in Figure 1-1:

Figure 1-1 Cisco UC Integration for Microsoft Office Communicator Interactions with Network Servers



Cisco UC Integration for Microsoft Office Communicator provides window management, client security, third-party integration, and Cisco Unified Client Services Framework integration. Client Services Framework provides the engine to provide Cisco telephony and next-generation media services for the desktop.

When you install Cisco UC Integration for Microsoft Office Communicator, the installation application installs all of the required components.

Installation Prerequisites

Before you install Cisco UC Integration for Microsoft Office Communicator, check that your system meets all the necessary prerequisites. Ensure that you have the correct versions of all of the required software, as listed in the release notes at the following URL:

http://www.cisco.com/en/US/products/ps10317/prod_release_notes_list.html



CHAPTER 2

Configuring Servers for Cisco Unified Communications Integration for Microsoft Office Communicator

Revised: July 7, 2011

- [How to Configure Active Directory Server and OCS Server, page 2-1](#)
- [Dial Plan Options for Cisco UC Integration for Microsoft Office Communicator, page 2-4](#)
- [How to Configure Cisco Unified Communications Manager Server, page 2-8](#)
- [How To Configure Cisco Unified MeetingPlace, page 2-19](#)
- [How to Configure Cisco Unity Server for Voicemail Access, page 2-22](#)
- [How to Configure Cisco Unity Connection Server for Voicemail Access, page 2-23](#)

How to Configure Active Directory Server and OCS Server

When you configure your servers for Cisco UC Integration for Microsoft Office Communicator, you must ensure that the user IDs, devices, and directory numbers match in the following servers:

- Active Directory server
- Office Communications Server (OCS)
- Cisco Unified Communications Manager server

You must also configure your users so that each user has a phone number that can be correctly dialed within the context of your Cisco Unified Communications Manager configuration.

For more information about the importance of the use of the +E.164 format to the deployment of Cisco UC Integration for Microsoft Office Communicator, read the following topics:

- [E.164 Formatting, page 2-2](#)
- [Phone Numbers for Active Directory Users Must Use +E.164 Formatting, page 2-2](#)

To configure the Active Directory server and the OCS server for Cisco UC Integration for Microsoft Office Communicator, you must perform the following tasks:

- [Enabling Users for OCS, page 2-2](#)
- [Updating OCS Address Book Manually, page 2-3](#)
- [Verifying OCS Address Book Synchronization, page 2-4](#)

E.164 Formatting

The E.164 standard defines an international numbering plan for public phone systems. In the E.164 standard, each number contains a country code, an area code, and a subscriber number. Each phone user has a globally unique number. In Cisco UC Integration for Microsoft Office Communicator, phone numbers in E.164 format must begin with a plus character (“+”), therefore we say that the numbers are in +E.164 format.

Phone Numbers for Active Directory Users Must Use +E.164 Formatting

You must define phone numbers in +E.164 format for each user in your Active Directory. This ensures the following:

- When Microsoft Office Communicator downloads the OCS address book, each user in the OCS address book is assigned a number in the correct format.
- Each user has a phone number that can be correctly dialed within the context of your Cisco Unified Communications Manager configuration.

The Microsoft Office Communicator Automation API reads contacts and their associated phone numbers from Active Directory, and passes this data to the Cisco UC Integration for Microsoft Office Communicator.



Tip

Define phone numbers in +E.164 format for each user in your Active Directory. If you do not do this, you must configure a set of phone number normalization rules on the OCS server, so that a phone number that can be correctly dialed is available in the OCS address book. Configuring phone number normalization rules can be an error-prone task, especially for international and enterprise dial plans. If you choose not to define phone numbers in +E.164 format, see [Appendix A, “Normalization Rules for OCS”](#).

What to Do Next

- [Enabling Users for OCS, page 2-2](#)

Enabling Users for OCS

Procedure

- Step 1** Start the Active Directory Users and Computers administrative tool.
- Step 2** Expand the domain that contains your users.
- Step 3** Open the organizational unit (OU) that contains your users.
- Step 4** Check the following details for all users that you want to enable for OCS:
 - All users have valid email addresses.
 - All users are assigned to a group.
 - All the phone numbers for each user are in +E.164 format, and can be correctly dialed within the context of your Cisco Unified Communications Manager configuration.
- Step 5** Right-click the users, then select **Enable users for Communications Server**.

Active Directory uses the User logon name field and the domain name to form a SIP email address in the Office Communications Server Address column. This address is used to sign users in to Microsoft Office Communicator, and enables users to send instant messages.

Related Topics

- [Configuration of Telephony Options for Users, page 2-3](#)
- [Phone Numbers for Active Directory Users Must Use +E.164 Formatting, page 2-2](#)

What to Do Next

- [Updating OCS Address Book Manually, page 2-3](#)

Configuration of Telephony Options for Users

We recommend that you do *not* select the following telephony options for your users:

- **Enable Remote call control**
- **Enable Enterprise Voice**

If you select either of these options, voice traffic is allowed from both Cisco UC Integration for Microsoft Office Communicator *and* Microsoft Office Communicator. This can result in the following problems:

- A confusing user experience, as users can place and receive calls from a mixture of user interface elements in both applications.
- Inconsistent voice traffic. That is, calls from Cisco UC Integration for Microsoft Office Communicator might give a different audio experience to Microsoft Office Communicator.
- A mixed configuration is more difficult to manage, as administrators must track traffic from two sources. You might want to monitor voice usage in your network and if you use both applications, you must configure your monitoring tools to track traffic from both applications.

Related Topics

- [Enabling Users for OCS, page 2-2](#)

Updating OCS Address Book Manually

To ensure that the OCS address book has the latest information from the Active Directory server, you must update the OCS address book manually. For information about how to perform this task, see the following URL:

<http://technet.microsoft.com/en-us/library/bb936631.aspx>

What to Do Next

- [Verifying OCS Address Book Synchronization, page 2-4](#)

Verifying OCS Address Book Synchronization

You must verify that the users are enabled for OCS, that the OCS address book is synchronized with the Active Directory server, and that the OCS address book is configured and operational.

To resolve problems associated with synchronization of the OCS address book, see [Troubleshooting Cisco Unified Communications Integration for Microsoft Office Communicator, page 6-1](#).

Alternatively, see the relevant Microsoft documentation.

Procedure

-
- Step 1** Use one of the user accounts to sign in to Microsoft Office Communicator.
This step signs the user in to OCS.
- Step 2** Verify that the following message is *not* displayed in the notifications area in Microsoft Office Communicator after the user signs in:
Cannot Synchronize Address Book
-

Dial Plan Options for Cisco UC Integration for Microsoft Office Communicator

The following table summarizes the dial plan options available when you deploy Cisco UC Integration for Microsoft Office Communicator:

Option	Phone Numbers in Active Directory	Phone Numbers in Cisco Unified Communications Manager	Comments
1	+E.164 number format	+E.164 number format	Requires Cisco Unified Communications Manager Release 7.0 or later.
2	+E.164 number format	Private numbering plan	Requires you to do the following: <ul style="list-style-type: none"> • Configure application dialing rules and directory lookup dialing rules on Cisco Unified Communications Manager.
3	Private numbering plan	Private numbering plan	Requires you to do the following: <ul style="list-style-type: none"> • Configure normalization rules on OCS. • Configure application dialing rules and directory lookup dialing rules on Cisco Unified Communications Manager.

This chapter deals with options 1 and 2. [Appendix A, “Normalization Rules for OCS”](#) deals with option 3.

**Note**

If you choose option 3, you must configure a set of phone number normalization rules on the OCS server. Configuring OCS normalization rules can be an error-prone task, especially for international and enterprise dial plans. For more information about this topic, see [Appendix A, “Normalization Rules for OCS”](#).

Dialing Rules Required for Cisco UC Integration for Microsoft Office Communicator

If your Cisco Unified Communications Manager uses a private numbering plan, you must configure the following types of dialing rules in Cisco Unified Communications Manager:

- [Application Dialing Rules, page 2-5](#)
- [Directory Lookup Dialing Rules, page 2-6](#)

For detailed conceptual and task-based information on dialing rules, see the Cisco Unified Communications Manager Administration online help or the *Cisco Unified Communications Manager Administration Guide* and the *Cisco Unified Communications Manager System Guide*:

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

**Note**

If your Cisco Unified Communications Manager uses dialing rules, you must ensure that Cisco UC Integration for Microsoft Office Communicator and Cisco Unified Client Services Framework can access these dialing rules.

Related Topics

- [How to Make Cisco Unified Communications Manager Dialing Rules Accessible, page 2-15](#)

Application Dialing Rules

Application dialing rules modify the dial string on outbound calls to conform to the route plan on the Cisco Unified Communications Manager. For Cisco UC Integration for Microsoft Office Communicator, application dialing rules map numbers in the OCS address book to a number format that can be correctly dialed within the context of your Cisco Unified Communications Manager configuration. That is, you must define application dialing rules to map +E.164 numbers to the private numbering plan.

Example Application Dialing Rule for Contacts with North American Numbers

The following table illustrates the application dialing rule that you need to use to resolve +E.164-format numbers to a Cisco Unified Communications Manager private numbering plan that uses six-digit numbers beginning with 8.

	1	2	3	4	5	6	7	8	9	10	11	12
Number for contact in OCS address book in +E.164 format	+	1	4	0	8	5	5	5	0	1	0	0
	Number begins with +1408555											
	Number of digits is 12											

	1	2	3	4	5	6	7	8	9	10	11	12
Operations performed by application dialing rule	+	1	4	0	8	5	5	5	0	1	0	0
	Number of digits to remove is 7											
	Prefix with 8											
Dialed number	850100											

Example of Application Dialing Rule for Contacts with Spanish Numbers

The following table illustrates the application dialing rule that you need to use to resolve +E.164-format numbers to a Cisco Unified Communications Manager private numbering plan that uses nine-digit numbers beginning with 91.

	1	2	3	4	5	6	7	8	9	10	11	12
Number for contact in OCS address book in +E.164 format	+	3	4	9	1	2	3	4	5	6	7	8
	Number begins with +34											
	Number of digits is 12											
Operations performed by application dialing rule	+	3	4	9	1	2	3	4	5	6	7	8
	Number of digits to remove is 3											
	No prefix required											
Dialed number	912345678											

Directory Lookup Dialing Rules

Directory lookup dialing rules transform caller identification numbers into numbers that can be looked up in the directory. For example, if the Cisco Unified Communications Manager reports a call from 85550100, that number must be transformed into the +E.164 format of +14085550100, as stored in LDAP to identify the caller as a contact. If numbers in the LDAP are not in +E.164 format, but the enterprise routable number is stored in LDAP, then the directory lookup dialing rules need to map incoming numbers to the enterprise routable numbers.

For Cisco UC Integration for Microsoft Office Communicator, directory lookup dialing rules map private numbering plan numbers to the number format used in Active Directory. That is, you must define directory lookup dialing rules to transform private numbering plan numbers to +E.164-format numbers.

Example of Directory Lookup Dialing Rule for Contacts with North American Numbers

The following table illustrates the directory lookup dialing rule that you need to use to resolve a number from a Cisco Unified Communications Manager private numbering plan that uses six-digit numbers beginning with 81, to a +E.164-format number.

	1	2	3	4	5	6	7	8	9	10	11	12	
Private numbering plan number from Cisco Unified Communications Manager							8	1	0	1	9	9	
							Number begins with 81						
	Number of digits is 6												
Operations performed by directory lookup dialing rule	+	1	4	0	8	5	5	5	0	1	9	9	
	Prefix with +1408555												
	Digits to remove is 2												
Resulting +E.164-format number	+14085550199												

Example of Directory Lookup Dialing Rule for Contacts with Spanish Numbers

The following table illustrates the directory lookup dialing rule that you need to use to resolve a number from a Cisco Unified Communications Manager private numbering plan that uses nine-digit numbers beginning with 91, to a +E.164-format number.

	1	2	3	4	5	6	7	8	9	10	11	12
Private numbering plan number from Cisco Unified Communications Manager				9	1	2	3	4	5	6	7	9
				Number begins with 91								
	Number of digits is 9											
Operations performed by directory lookup dialing rule	+	3	4	9	1	2	3	4	5	6	7	9
	Prefix with +34											
	Digits to remove is 0											
Resulting +E.164-format number	+34912345679											

How to Configure Cisco Unified Communications Manager Server

Before you configure the Cisco Unified Communications Manager server, read the following topics:

- [Prerequisites for Configuring Cisco Unified Communications Manager, page 2-8](#)
- [Cisco Unified Client Services Framework Device Type, page 2-8](#)

To configure the Cisco Unified Communications Manager server for Cisco UC Integration for Microsoft Office Communicator, you must perform the following tasks:

- [Enabling LDAP Synchronization, page 2-9](#)
- [Enabling LDAP Authentication, page 2-10](#)
- [Creating Client Services Framework Devices and Directory Numbers for Users, page 2-10](#)
- [Adding Users to User Groups and Associating Controlled Devices, page 2-12](#)
- [How to Configure Cisco Unified IP Phones for Video, page 2-13](#)
- [Configuring Cisco Unified Communications Manager for Ad-Hoc Video Conferencing, page 2-14](#)
- [How to Make Cisco Unified Communications Manager Dialing Rules Accessible, page 2-15](#)
- [Configuring Failover to Cisco Unified Survivable Remote Site Telephony \(SRST\), page 2-18](#)

Prerequisites for Configuring Cisco Unified Communications Manager

You must have a properly working Cisco Unified Communications configuration with the following servers:

- Cisco Unified Communications Manager server

For information about Cisco Unified Communications Manager servers, see the documentation at the following URL:

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

- Cisco Trivial File Transfer Protocol (TFTP) server

For information about Cisco TFTP servers, see the *Cisco Unified Communications Manager System Guide*.

- Cisco CTIManager server

For information about Cisco CTIManager servers, see the *Cisco Unified Communications Manager System Guide*.

- Cisco Unified Communications Manager IP Phone (CCMCIP) server

Cisco Unified Client Services Framework Device Type

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

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

For information about which releases of Cisco Unified Communications Manager require you to run the COP file to install the Cisco Unified Client Services Framework device type, see the release notes at the following URL:

http://www.cisco.com/en/US/products/ps10317/prod_release_notes_list.html

The COP file is included in the Administration Toolkit for Cisco UC Integration for Microsoft Office Communicator. To access the Administration Toolkit, navigate to Cisco UC Integration for Microsoft Office Communicator from the Download Software page at the following URL:

<http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=282588075>

What to Do Next

- [Enabling LDAP Synchronization, page 2-9](#)

Enabling LDAP Synchronization

This procedure allows Cisco Unified Communications Manager to integrate with Active Directory and build the Cisco Unified Communications Manager user database from the same data source where Windows users and Microsoft Office Communicator users are defined.

If you synchronize the Cisco Unified Communications Manager with Active Directory, the Cisco UC Integration for Microsoft Office Communicator user IDs will be the same as the Windows and Microsoft Office Communicator user IDs. If you synchronize the Cisco Unified Communications Manager with Active Directory, you must also enable LDAP authentication. For more information about how to enable LDAP authentication, see [Enabling LDAP Authentication, page 2-10](#).



Note

If you choose not to synchronize the Cisco Unified Communications Manager with Active Directory, you must set the value of the ContactService_UseCredentialsFrom registry key to specify the source of the credentials for Cisco UC Integration for Microsoft Office Communicator.

Procedure

- Step 1** Select **System > LDAP > LDAP System** in Cisco Unified Communications Manager Administration.
- Step 2** Select **Enable Synchronizing from LDAP Server**.
- Step 3** Select **Microsoft Active Directory** from the LDAP Server Type list box.
- Step 4** Select the LDAP attribute that you want to use as the User ID in Cisco Unified Communications Manager from the LDAP Attribute for User ID list box.
- Step 5** Select **Save**.
- Step 6** Select **System > LDAP > LDAP Directory**.
- Step 7** Select **Add New**.
- Step 8** Enter data in the LDAP Directory window as required.
- Step 9** Select **Save**.
- Step 10** Select **Perform Full Sync Now**.

For information about how to synchronize with LDAP, see the LDAP Directory Integration information in the Cisco Unified Communications System Solution Reference Network Design (SRND) guides at the following URL:

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

What to Do Next

- [Enabling LDAP Authentication, page 2-10](#)

Related Topics

- [Normalization Rules for OCS, page A-1](#)
- [Specifying Account Credential Synchronization Value Names, page 3-10](#)

Enabling LDAP Authentication

If you enable LDAP authentication in Cisco Unified Communications Manager, the Active Directory provides authentication services to Cisco Unified Communications Manager by proxy. For example, Cisco Unified Communications Manager can forward authentication requests from the Cisco UC Integration for Microsoft Office Communicator to Active Directory, and Active Directory responds to the request.

Procedure

- Step 1** Select **System > LDAP > LDAP Authentication** in Cisco Unified Communications Manager Administration.
- Step 2** Select **Use LDAP Authentication for End Users**.
- Step 3** Select **Save**.
-

What to Do Next

- [Creating Client Services Framework Devices and Directory Numbers for Users, page 2-10](#)

Creating Client Services Framework Devices and Directory Numbers for Users

The Client Services Framework device is required for users who want to use the phone on the computer.

Procedure

- Step 1** Select **Device > Phone** in Cisco Unified Communications Manager Administration.
- Step 2** Select **Add New**.
- Step 3** Select **Cisco Unified Client Services Framework** from the Phone Type list box, then select **Next**.

Step 4 Enter information for the phone in the Phone Configuration window, as follows:

Field	Description
Device Name	Enter a name to identify the Cisco Unified Client Services Framework device. The name can contain 1 to 15 characters, including alphanumeric characters, periods, hyphens, and underscores. The device name does not need to relate to the user ID of the user.
Device Pool	Select the device pool to which you want the phone assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, softkey template, and Multilevel Precedence and Preemption (MLPP) information.
Phone Button Template	Select the appropriate phone button template. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button.
Allow Control of Device from CTI	Uncheck this option. Client Services Framework does not support Computer Telephony Integration (CTI) servitude.
Device Security Profile	Select the security profile you require for the phone. If you select Cisco Unified Client Services Framework- Standard SIP Secure Profile, do the following: <ol style="list-style-type: none"> a. Enter certification and authentication information in the Certification Authority Proxy Function (CAPF) Information section. b. Select Generate String. c. Email the contents of the Authentication String field to the user.
SIP Profile	Select the default SIP profile or a specific profile that was previously created. SIP profiles provide specific SIP information for the phone such as registration and keepalive timers, media ports, and do not disturb control.

Step 5 Enter any other required information, then select **Save**.

Step 6 Select the **Add a new DN** link in the Association Information section on the Phone Configuration window.

Step 7 Enter information for the directory number on the Directory Number Configuration window.

Step 8 Select **Save**.

Step 9 Select **Reset** on the Phone Configuration window to reset the phone.

Step 10 Select **Associate End Users** on the Directory Number Configuration window.

Step 11 Search for the user in the Find and List Users window, select the user, then select **Add Selected**.

Step 12 Select **Save**.

Step 13 Select **User Management > End User** in Cisco Unified Communications Manager Administration.

Step 14 Search for the user in the Find and List Users window, then select the user.

Step 15 Verify that the device is listed for the user in the Controlled Devices list box in the Device Associations group.

What to Do Next

- [Adding Users to User Groups and Associating Controlled Devices, page 2-12](#)

Related Topics

- [Cisco Unified Client Services Framework Device Type, page 2-8](#)

Adding Users to User Groups and Associating Controlled Devices

Before You Begin

To configure Cisco UC Integration for Microsoft Office Communicator to control the desk phone and soft phone of the user, you must do each of the following:

- Select the **Allow Control of Device from CTI** option when you create the desk phone device for the user in Cisco Unified Communications Manager.
- Ensure that the user is added to the appropriate user groups, as described in the following procedure.
- Select the Cisco Unified Client Services Framework device and any desk-phone devices as controlled devices for the user, as described in the following procedure.

Procedure

-
- Step 1** Select **User Management > End User** in Cisco Unified Communications Manager Administration.
- Step 2** Select the user that you want to add.
- Step 3** Select **Add to User Group** in the Permissions Information group in the End User Configuration window.
- Step 4** Search for “Standard CTI” in the Find and List User Groups window.
- Step 5** Select the **Standard CTI Enabled** user group.
- Step 6** If the phone of the user is a Cisco Unified IP Phone 9900 or 8900 series model, also select the **Standard CTI Allow Control of Phones supporting Connected Xfer and conf** group.
- Step 7** If the phone of the user is a Cisco Unified IP Phone 6900 series model, also select the **Standard CTI Allow Control of Phones supporting Rollover Mode** group.
- Step 8** Select **Add Selected**.
- Step 9** Select **Device Association** in the Device Information group.
- Step 10** Search for the devices that you want to associate with the user in the User Device Association window.
- Step 11** Select the devices you require, then select **Save Selected/Changes**.
- For example, you might select a device whose type is Cisco Unified Client Services Framework, and a desk-phone device.
- Step 12** Select **Back to User** from the Related Links drop-down list, then select **Go**.
- Step 13** Select **Save** in the End User Configuration window.
-

How to Configure Cisco Unified IP Phones for Video

The Client Services Framework 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 UC Integration for Microsoft Office Communicator to be able to send and receive video, you must also select the following devices as controlled devices for the user:

- The Cisco Unified Client Services Framework device
- Any desk-phone devices

**Note**

Only Skinny Client Control Protocol (SCCP) Cisco Unified IP Phones support video with Client Services Framework.

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

- [Connecting a Cisco Unified IP Phone to the Network and Your Computer, page 2-13](#)
- [Enabling Video for a Cisco Unified IP Phone, page 2-13](#)
- [Adding Users to User Groups and Associating Controlled Devices, page 2-12](#)
- [Securing IP Phones, page 2-14](#)

For more information about how to configure Cisco UC Integration for Microsoft Office Communicator for video, see the release notes for the product at the following URL:

http://www.cisco.com/en/US/products/ps10317/prod_release_notes_list.html

For more detailed information about IP video telephony in Cisco Unified Communications Manager, please refer to the *Cisco Unified Communications System Release 8.x SRND* at the following URL:

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

Connecting a Cisco Unified IP Phone to the Network and Your Computer

Procedure

-
- Step 1** Connect the SW port on the Cisco Unified IP Phone to the network.
- Step 2** Connect the PC port on the Cisco Unified IP Phone to the controlling PC with an Ethernet cable.
-

What to Do Next

- [Enabling Video for a Cisco Unified IP Phone, page 2-13](#)

Enabling Video for a Cisco Unified IP Phone

Procedure

-
- Step 1** Select **Device > Phone** in Cisco Unified Communications Manager Administration.
- Step 2** Find the device that you want to configure.

- Step 3** Click on the Device Name.
- Step 4** Scroll to the **Product Specific Configuration Layout** section.
- Step 5** Select **Enabled** from the **PC Port** drop-down list.
- Step 6** Select **Enabled** from the **Video Capabilities** drop-down list.
- Step 7** Select **Save**.

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

What to Do Next

- [Adding Users to User Groups and Associating Controlled Devices, page 2-12](#)

Related Topics

- [Securing IP Phones, page 2-14](#)

Securing IP Phones

For information about how to secure your IP phone device, see the *Cisco Unified Communications Manager Security Guide* at the following URL:

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

Configuring Cisco Unified Communications Manager for Ad-Hoc Video Conferencing

To enable ad-hoc video conferencing on your Cisco Unified Communications system, you must do the following:

- Configure a conference bridge. The conference bridges supported are:
 - Cisco Unified MeetingPlace
 - Cisco Unified Video Conferencing (CUVC)
 - Cisco IP Video Conferencing (IPVC) 35xx series MCU

For detailed task-based information about how to configure a conference bridge, see the *Configuration Guide for Cisco Unified MeetingPlace*:

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

- Configure a media resource group and a media resource group list. For information about how to configure a media resource group and a media resource group list, 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
- Configure the devices of your users to use the media resource group list that contains the conference bridge. For information about how to configure the devices of your users, 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

(Optional) Specifying a Minimum Number of Video-Capable Participants for Ad-Hoc Conferences

If you enable ad-hoc video conferencing on your Cisco Unified Communications system, you can also specify a minimum number of video-capable participants for ad-hoc conferences. 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 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.

Procedure

-
- Step 1** Select **System > Service Parameters** in Cisco Unified Communications Manager Administration.
 - Step 2** Select your Cisco Unified Communications Manager server from the Server drop-down list.
 - Step 3** Select the appropriate Cisco Unified Communications Manager service from the Service drop-down list.
 - Step 4** Enter the minimum number of video-capable participants in the **Minimum Video Capable Participants To Allocate Video Conference** field in the Clusterwide Parameters (Feature - Conference) section.
 - Step 5** Select **Save**.
-

How to Make Cisco Unified Communications Manager Dialing Rules Accessible

If your Cisco Unified Communications Manager uses dialing rules, you must ensure that Cisco UC Integration for Microsoft Office Communicator and Client Services Framework can access these dialing rules.

You must run a COP file to generate copies of the dialing rules in XML format, which Cisco UC Integration for Microsoft Office Communicator and Client Services Framework can access. You can get the COP file, called `cmterm-CUPC-dialrulewizard.cop`, from the Administration Toolkit. To access the Administration Toolkit, navigate to Cisco UC Integration for Microsoft Office Communicator from the Download Software page at the following URL:

<http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=282588075>



Note

- Every time you update the dialing rules in your Cisco Unified Communications Manager, you must run the COP file again, to ensure that Cisco UC Integration for Microsoft Office Communicator and Client Services Framework can access the updated dialing rules.
 - You must run the COP file on each Cisco Unified Communications Manager that runs a TFTP server.
-

To make the Cisco Unified Communications Manager dialing rules accessible by Cisco UC Integration for Microsoft Office Communicator and Client Services Framework, you must perform the following tasks:

- [Verifying That Dialing Rules Are Configured on Cisco Unified Communications Manager, page 2-16](#)
- [Generating Copies of the Dialing Rules, page 2-16](#)
- [Verifying That Copies of the Dialing Rules Were Generated, page 2-17](#)
- [Restarting the TFTP Service, page 2-17](#)
- [Ensuring That Cisco UC Integration for Microsoft Office Communicator Clients Are Restarted, page 2-18](#)

Verifying That Dialing Rules Are Configured on Cisco Unified Communications Manager

Procedure

-
- Step 1** Select **Call Routing > Dial Rules > Application Dial Rules** in Cisco Unified Communications Manager Administration.
- Step 2** Search for the dialing rules in the Find and List Application Dial Rules window.
- Step 3** Verify that application dialing rules are found.
- Step 4** Select **Call Routing > Dial Rules > Directory Lookup Dial Rules** in Cisco Unified Operating System Administration.
- Step 5** Search for the dialing rules in the Directory Lookup Dial Rule Find and List window.
- Step 6** Verify that directory lookup rules are found.

If there are no application dialing rules or directory lookup dialing rules on your Cisco Unified Communications Manager, you do not need to make dialing rules accessible by Cisco UC Integration for Microsoft Office Communicator.



Tip

To ensure that the dialing rules are working properly, try making a call from Cisco UC Integration for Microsoft Office Communicator.

What to Do Next

- [Generating Copies of the Dialing Rules, page 2-16](#)

Generating Copies of the Dialing Rules

You must run a COP file to generate copies of the dialing rules in XML format. You can get the COP file, called `cmterm-CUPC-dialrulewizard.cop`, from the Administration Toolkit. To access the Administration Toolkit, navigate to Cisco UC Integration for Microsoft Office Communicator from the Download Software page at the following URL:

<http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240>

Procedure

- Step 1** Select **Software Upgrades > Install/Upgrade** in Cisco Unified Operating System Administration.
- Step 2** Specify the location of the COP file in the Software Installation/Upgrade window.
- Step 3** Select **Next**.
- Step 4** Select the appropriate file from the **Available Software** list box.
- Step 5** Select **Next**.
- Step 6** Select **Install**.
-

What to Do Next

- [Verifying That Copies of the Dialing Rules Were Generated, page 2-17](#)

Verifying That Copies of the Dialing Rules Were Generated

Procedure

- Step 1** Select **Software Upgrades > TFTP File Management** in Cisco Unified Operating System Administration.
- Step 2** Search for a directory that begins with CUPC in the TFTP File Management window.
- Step 3** Verify that the following files are found:
- AppDialRules.xml
 - DirLookupDialRules.xml
-

What to Do Next

- [Restarting the TFTP Service, page 2-17](#)

Restarting the TFTP Service

After you verify the generation of the copies of the dialing rules, restart the TFTP service. You must restart the TFTP service on every server on which you ran the COP file.

For information about how to restart TFTP services, see *Cisco Unified Serviceability Administration Guide* at the following URL:


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

What to Do Next

- [Ensuring That Cisco UC Integration for Microsoft Office Communicator Clients Are Restarted, page 2-18](#)

Ensuring That Cisco UC Integration for Microsoft Office Communicator Clients Are Restarted


Procedure

Step 1 Select  in the Microsoft Office Communicator title bar.

Step 2 Select **Tools > Stop Cisco UC**.



Note It can take approximately 2 minutes for the cucsf.exe process to stop. Use the Task Manager to check if the process has stopped before proceeding to Step 3.

Step 3 Select  in the Microsoft Office Communicator title bar.

Step 4 Select **Tools > Start Cisco UC**.

The Cisco UC Integration for Microsoft Office Communicator client and the cucsf.exe process are automatically restarted.

Configuring Failover to Cisco Unified Survivable Remote Site Telephony (SRST)

Cisco UC Integration for Microsoft Office Communicator supports failover to Cisco Unified Survivable Remote Site Telephony (SRST) to keep calls connected if Cisco Unified Communications Manager becomes unavailable.

Procedure

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

Step 2 Select **Add New** and specify the SRST reference information.

Step 3 Select **System > Device Pool**.

Step 4 Select the device pool for the target office.

Step 5 In the Roaming Sensitivity Settings section, select the SRST reference that you created in Step 2 from the SRST Reference drop-down list.

Step 6 Select **Save**.



Note To configure an SRST router that connects directly to the target Branch office LAN and is the default gateway for the branch office LAN, you can omit steps 1-2, and in the target office Device Pool Configuration > Roaming Sensitivity Settings section, select **Use Default Gateway** from the SRST Reference drop-down list.

How To Configure Cisco Unified MeetingPlace

Before You Begin

You must have a working Cisco Unified MeetingPlace Release 8.0 server configured in one of the following modes:

- Software Mixing Mode (SMS Mode). This mode supports ad-hoc and scheduled video conferences in all video resolutions, that is, QCIF, CIF, VGA, and 720p HD.
- Hardware Mixing Mode (HMS Mode) using an external hardware mixer. This mode supports scheduled and reservationless meetings only.

For more information about how to configure video conferences on Cisco Unified MeetingPlace Release 8.0, see the documentation at the following URL:

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

To configure Cisco Unified MeetingPlace, you must perform the following tasks:

- [Configuring a Cisco Unified MeetingPlace Application Server for Ad-Hoc Video Conferencing, page 2-20](#)
- [Configuring a Cisco Unified MeetingPlace Application Server for Scheduled Video Conferencing, page 2-21](#)
- [Adding Custom Cisco Unified MeetingPlace Template Files to a Cisco Unified MeetingPlace 7.x Web Server, page 2-21](#)

Meeting Types and Authentication

Reservationless Meetings

If reservationless meetings are enabled for users, users can start a meeting from Cisco UC Integration for Microsoft Office Communicator. For these meetings, Cisco Unified MeetingPlace is the front-end server. Cisco UC Integration for Microsoft Office Communicator schedules the meeting through Cisco Unified MeetingPlace.

Users can have only one reservationless meeting at a time. If the reservationless meeting of the user is in use at the time the user starts the meeting from Cisco UC Integration for Microsoft Office Communicator, their existing reservationless meeting is used.

To avoid this behavior, users must either end their reservationless meeting before they start a meeting, or ask their administrator to disable reservationless meetings in their Cisco Unified MeetingPlace user profile.

Meeting passwords are ignored for reservationless meetings.

Authentication

Cisco UC Integration for Microsoft Office Communicator includes support for all types of Cisco Unified MeetingPlace authentication, except for Trust External Authentication.

Reserving Audio and Video Resources

When a user starts a meeting, Cisco Unified MeetingPlace reserves audio resources, but does not reserve any video resources.

Configuring a Cisco Unified MeetingPlace Application Server for Ad-Hoc Video Conferencing

Procedure

- Step 1** Select **System Configuration > Call Configuration** in Cisco Unified MeetingPlace Administration Center.
- Step 2** Select **Ad-Hoc Cisco Unified Communications Manager Configuration**.
- Step 3** Enter the IP address and port for your Cisco Unified Communications Manager in the **Primary TFTP server** fields.
- Step 4** Select **Save**.
- Step 5** Select **System Configuration > Media Resource Configuration**.
- Step 6** Select **Yes** in the Enable ad-hoc video drop-down list.
- Step 7** Select one of the H.264 options from the Ad-hoc video mode drop-down list.

For mobile video, select **H.264 AVC (Level 1.1)**. For video on computers, select **H.264 AVC (Level 1.3)**, **H.264 AVC (Level 3.0)**, or **H.264 AVC (Level 3.1)**.



Note The setting that you select here is used for all video endpoints joining all ad-hoc conferences. If a video endpoint does not support the specified profile, this endpoint joins the conference in audio-only.

- Step 8** Select **Save**.
-

Related Topics

- [Configuring Failover to Cisco Unified Survivable Remote Site Telephony \(SRST\)](#), page 2-18

Configuring a Cisco Unified MeetingPlace Application Server for Scheduled Video Conferencing

Procedure

-
- Step 1** Select **User Configuration > User Groups** in Cisco Unified MeetingPlace Administration Center.
- Step 2** Select **Edit** next to the name of the User Group that you want to configure for scheduled video conferencing.
- Step 3** In the Video Preferences section, select one of the following options from the Available video types drop-down list:
- Mobile
 - Compatibility
 - High Quality
 - HD
- This setting determines the type of video for scheduled video conferencing.
- Step 4** Select **Save**.
-

Adding Custom Cisco Unified MeetingPlace Template Files to a Cisco Unified MeetingPlace 7.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 Communications Integration for Microsoft Office Communicator from the Download Software page at the following URL:

<http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240>

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

How to Configure Cisco Unity Server for Voicemail Access

Cisco Unity provides Cisco UC Integration for Microsoft Office Communicator users with the ability to view, play, sort, and delete voicemail messages from the Cisco UC Integration for Microsoft Office Communicator interface.

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.
- Install the Cisco Unity VoiceMail Web Service (VMWS).
- Set the Distributed Component Object Model (DCOM) permissions.

For more information, see the following topics:

- [Installing the Voicemail Web Service \(VMWS\), page 2-22](#)
- [Setting the DCOM Permissions, page 2-22](#)
- [Testing That the Voicemail Web Service Is Accessible, page 2-23](#)

Installing the Voicemail Web Service (VMWS)

Procedure

- Step 1** To install the Cisco Unity Voicemail Web Service, go to the following URL:
http://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html
- Step 2** Select the **Download Software** link, navigate to your Cisco Unity version, select **Unity System Software**, and select the installation file for VMWS.
- Step 3** Run the installation file and follow the instructions in the installation wizard to install VMWS.
-

What To Do Next

[Setting the DCOM Permissions, page 2-22](#)

Setting the DCOM Permissions

Use the Cisco Unity Permissions Wizard to grant DCOM permissions to the accounts that you require.

We recommend that you download and run the latest version of the Permissions wizard that is applicable to your version of Cisco Unity. The Permissions wizard is available at:

<http://www.ciscounitytools.com/Applications/Unity/PermissionsWizard/Unity50/PW50.html>

For information on granting permissions with the Permissions wizard, see the Permissions wizard Help file PWHelp_<language>.htm that is included with the version of the Permissions wizard that you are using.

Testing That the Voicemail Web Service Is Accessible

Procedure

- Step 1** Start a browser.
- Step 2** Use the HTTP or HTTPS protocol to access the URL of the voicemail web service on the Cisco Unity server.
- You can access the URL structured as follows:
- `http://<domain-name-of-Cisco Unity-server>/vmws/vmws.dll?Handler=GenAuthenticationWSDL`
- For example, access a URL similar to the following:
- `http://unityserver/vmws/vmws.dll?Handler=GenAuthenticationWSDL`
- If the source of an XML file is displayed, the voicemail web service has been correctly installed.
-

How to Configure Cisco Unity Connection Server for Voicemail Access

Cisco Unity Connection provides Cisco UC Integration for Microsoft Office Communicator users with the ability to view, play, sort, and delete voicemail messages from the Cisco UC Integration for Microsoft Office 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 servers must be installed and running to configure voicemail ports.

Configuring User Access

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, as follows:
- a. Expand **Class of Service** in the left pane.
 - b. Select **Class of Service**.
 - c. Select the display name of the applicable class of service in the Search Results table, in the Search Class of Service window.
 - d. For all other ports and protocols, perform the following steps:

- Check **Allow Users to Access VoiceMail Using an IMAP Client** under Licensed Features.
 - Select **Allow Users to Access Message Bodies**.
 - Check **Allow Users to Use Unified Client to Access Voice Mail** under Features.
- e. Select **Save**.
- Step 2** In Cisco Unity Connection Serviceability, select **Tools > Service Management > Optional Services**.
- a. Validate that the **Activate Status** of the **Connection IMAP Server** is **Activated**.
 - b. Validate that the **Service Status** of the **Connection IMAP Server** is **Started**.
- Step 3** Configure the user:
- If the users are existing Cisco Unity Connection users, add them to the Cisco Unified Communications Manager database. Proceed to Step 4.
 - If the user is a new Cisco UC Integration for Microsoft Office Communicator user, add the user to Cisco Unified Communications Manager database and Cisco Unity Connection.
- Step 4** Create a Connection user account on the Cisco Unity Connection server with a voice mailbox for each Cisco UC Integration for Microsoft Office Communicator user.
-
-  **Note** To avoid problems with conflicting user IDs, consider importing users from the Cisco Unified Communications Manager database where possible.
-
- Step 5** If one does not already exist, specify a web application password in Cisco Unity Connection for the applicable user accounts.
- Step 6** You must populate the Cisco Unity Connection SMTP proxy addresses for subscribers if either of the following is true:
- The voice message system and the Microsoft Office Communicator directory are not in the same domain.
 - The user IDs of the Cisco Unity Connection subscribers are different to the Cisco Unified Communications Manager user IDs or Windows and Microsoft Office Communicator user IDs.
-

Enabling Secure Access to Voice Messages

Procedure

- Step 1** Enable secure messaging in Cisco Unity Connection Administration as follows:
- a. Expand **Class of Service** in the left pane.
 - b. Select an existing Class of Service from the right pane.
 - c. Select an option from Require Secure Messaging in the Message Options section to enable secure messages.
- Step 2** (Optional) Specify how to handle unidentified caller message security for your users as follows:
- a. Expand **Users** in the left pane.
 - b. Select **Users**.
 - c. Select the alias of a user.

- d. Select **Edit > Message Settings**.
 - e. Check **Mark Secure** in Unidentified Callers Message Security.
-



CHAPTER 3

Configuring Client Computers for Cisco Unified Communications Integration for Microsoft Office Communicator

Revised: July 7, 2011

- [About Client Computer Configuration, page 3-1](#)
- [Location of Client Services Framework Configuration Data, page 3-2](#)
- [Configuring Value Names for the Client Services Framework Client Integration, page 3-2](#)
- [Enabling LDAP Over SSL, page 3-11](#)
- [Configuring Microsoft Office Communicator 2007 to Use HTTPS to Access Custom Availability Statuses, page 3-13](#)
- [Configuration of Policies for Microsoft Office Applications, page 3-14](#)
- [About the Client Services Framework Cache and LDAP Searches, page 3-15](#)
- [How to Configure Cisco UC Integration for Microsoft Office Communicator Clients for Secure Access to Cisco Unified MeetingPlace, page 3-18](#)
- [How to Configure Cisco UC Integration for Microsoft Office Communicator Clients to Enable Secure Voicemail Access, page 3-19](#)
- [Installing Security Certificates on Client Computers, page 3-21](#)

About Client Computer Configuration

Before you install Cisco UC Integration for Microsoft Office Communicator, you must perform some configuration on the computers of your users:

- Specify the Client Services Framework client settings.
- Specify the Microsoft Office Communicator settings.
- Specify the Microsoft Office settings.
- Specify other security-related settings that you want the client computers to use.
- Deploy the policy changes to the computers in your Cisco Unified Communications system. To do this, you can use software management system, for example, Active Directory Group Policy, Altiris Deployment Solution, Microsoft System Center Configuration Manager (SCCM), and so on.

- Configure the Client Services Framework on the computers of your users so that the Client Services Framework can function as the phone device for that user, to specify where Client Services Framework can connect to, and to specify the LDAP parameters.

Location of Client Services Framework Configuration Data

You specify the configuration for Client Services Framework 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 UC Integration for Microsoft Office Communicator, then Client Services Framework configuration data is specified in the following registry key:

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



Note

- If Client Services Framework configuration data is present in both of these registry keys, the policies configuration data takes precedence.
- Client Services Framework reads only HKEY_CURRENT_USER keys. Client Services Framework does not read HKEY_LOCAL_MACHINE keys.

Configuring Value Names for the Client Services Framework Client Integration

- [Specifying TFTP, CTIManager, and CCMCIP Server Value Names, page 3-3](#)
- [Specifying Cisco Unified MeetingPlace Server Value Names, page 3-4](#)
- [Specifying Voicemail and Visual Voicemail Value Names, page 3-4](#)
- [Specifying Video Value Names, page 3-6](#)
- [Specifying Security Certificate Value Names, page 3-6](#)
- [Specifying LDAP Value Names, page 3-7](#)
- [Specifying Account Credential Synchronization Value Names, page 3-10](#)
- [Using an Active Directory Group Policy Administrative Template to Configure Client Services Framework Clients, page 3-10](#)

Specifying TFTP, CTIManager, and CCMCIP Server Value Names

Table 3-1 lists the name-value pairs that you must use to specify the TFTP, CCMCIP, and CTIManager server configurations.

Table 3-1 TFTP, CCMCIP, and CTIManager Server Value Names

Value Names	Description
TftpServer1, TftpServer2, TftpServer3	Enter the IP address or fully-qualified domain name of the primary TFTP server in your Cisco Unified Communications system, and any other TFTP servers. If you are using certificates, this value must match the name of the server as specified on the certificate.
CtiServer1, CtiServer2	Enter the IP address or fully-qualified domain name of the primary CTIManager server in your Cisco Unified Communications system, and the secondary CTIManager server, if present. If you are using certificates, this value must match the name of the server as specified on the certificate.
CcmcipServer1, CcmcipServer2	Enter the IP address or fully-qualified domain name of the primary CCMCIP server in your Cisco Unified Communications system, and the secondary CCMCIP server, if present. If you are using certificates, this value must match the name of the server as specified on the certificate.
CcmcipServerValidation	<p>Enter the type of security certificate validation for Client Services Framework to use with HTTPS to sign in to Cisco Unified Communications Manager to retrieve the device list. Enter one of the following values:</p> <ul style="list-style-type: none"> • 0: Client Services Framework accepts all certificates. • 1: Client Services Framework accepts certificates that are defined in the keystore and self-signed certificates. • 2: Client Services Framework only accepts certificates that are defined in the keystore. <p>Note Client Services Framework uses this certificate to verify the Cisco Unified Communications Manager server. When the certificate is accepted, Client Services Framework must use the credentials of the user to sign in to Cisco Unified Communications Manager.</p>

Related Topics

- [Installing Security Certificates on Client Computers, page 3-21](#)

Specifying Cisco Unified MeetingPlace Server Value Names

Table 3-2 lists the name-value pairs that you must use to specify the Cisco Unified MeetingPlace server configuration.

Table 3-2 Cisco Unified MeetingPlace Server Value Names

Value Names	Description
WebConfServer	Enter the fully-qualified domain name (FQDN) of the Cisco Unified MeetingPlace server in your Cisco Unified Communications system. Do not include the IP address.
WebConfProtocol	The protocol to use between Client Services Framework and the Cisco Unified MeetingPlace server. The options are HTTP or HTTPS.
WebConfPort	Enter the port number for the Cisco Unified MeetingPlace server. The port number for HTTP protocol is usually 80 and the port number for HTTPS protocol is usually 443.
WebConfServerValidation	Specify the type of security certificate validation that Client Services Framework uses with HTTPS to validate requests from the Cisco Unified MeetingPlace web conferencing server. Enter one of the following values: <ul style="list-style-type: none"> • 0: Client Services Framework accepts all certificates. • 1: Client Services Framework accepts certificates that are defined in the keystore and self-signed certificates. This is the default. • 2: Client Services Framework only accepts certificates that are defined in the keystore.

Related Topics

- [Installing Security Certificates on Client Computers, page 3-21](#)

Specifying Voicemail and Visual Voicemail Value Names

Table 3-3 lists the name-value pairs that you must use to specify the voicemail and visual voicemail configuration.

Table 3-3 Voicemail and Visual Voicemail Value Names

Value Names	Description
VoicemailPilotNumber	Enter the number of the voice message service in your Cisco Unified Communications system. This value only relates to when users use the desk phone to access their voice messages. If users are using the phone on their computer to access voicemail, the pilot number comes from the voicemail pilot number associated with the voicemail profile configured on the Client Services Framework device.
VVM_SystemServer_0 ¹	Enter the IP address or fully-qualified hostname of the Cisco Unity or Cisco Unity Connection voicemail server.

Table 3-3 Voicemail and Visual Voicemail Value Names

Value Names	Description
VVM_SystemServer_VmwsPort_0 ¹	Enter the port number for the Cisco Unity Voicemail Web Service (VMWS) on the Cisco Unity or Cisco Unity Connection voicemail server. This value is optional with Cisco Unity and Cisco Unity Connection for synchronizing voicemail-related preferences, but the value is required with Cisco Unity for secure message playback.
VVM_SystemServer_VmwsProtocol_0 ¹	Enter the protocol to use for the VMWS. The options are HTTP or HTTPS. This value is optional with Cisco Unity and Cisco Unity Connection for synchronizing voicemail-related preferences, but the value is required with Cisco Unity for secure message playback.
VVM_Mailstore_Server_0 ¹	Enter the IP address or hostname of the IMAP mailstore server that is peered with the Cisco Unity or Cisco Unity Connection server. For Cisco Unity voicemail servers, this is typically the IP address of the peer Microsoft Exchange server. For Cisco Unity Connection voicemail servers, this is typically the IP address of the Cisco Unity Connection server itself.
VVM_Mailstore_ImapPort_0 ¹	Enter the port number to use for IMAP for visual voicemail. The IMAP port number is usually 143. Enter 7993 for this value name if you want to implement secure messages on a Cisco Unity Connection server.
VVM_Mailstore_ImapProtocol_0 ¹	Enter the protocol to use for IMAP for visual voicemail. Enter TCP for this value name. If you want to implement secure messages on a Cisco Unity Connection server, enter TLS. If you want to implement secure signing between a Cisco Unity server and a Microsoft Exchange server, enter TLS. If you use secure transport protocols like TLS and HTTPS, the certificate presented by the server must be a trusted certificate, signed by a trusted authority. If you use a local authority or a self-signed certificate, you must add these to the Client Services Framework keystore and mark them as trusted.
VVM_Mailstore_EncryptedConnection	Set this value to True to enable an encrypted IMAP connection to the voicemail server.
VVM_Mailstore_InboxFolderName	Enter “INBOX” as the name of your voicemail message inbox on the voicemail server.
VVM_Mailstore_PollingInterval	Enter the number of seconds that pass between calls to the visual voicemail server to check for new, updated, deleted or purged voice messages. For example, enter 60 seconds.
VVM_Mailstore_TrashFolderName	Enter the name of the folder to which deleted voice messages are moved on the Cisco Unity voicemail server. For example, “Deleted Items”. This value is not required for Cisco Unity Connection voicemail servers.
VVM_Mailstore_IdleEnabled	Set this value to True to enable an idle timeout.
VVM_Mailstore_IdleExpireTimeInMin	Specify the number of minutes that must elapse to trigger an idle timeout. The value can be between 5 and 29. The default is 29.

1. The last character of this value name can be 0 or 1 depending on whether the voicemail server is a primary (0) or secondary (1) server.

Specifying Video Value Names

Table 3-4 lists the name-value pair that you must use to specify video values.

Table 3-4 Video Value Names

Value Names	Description
SetVideoEnablePref	This value determines whether the user option to “Show my video automatically” is displayed in the Cisco UC Options dialog box in Cisco UC Integration for Microsoft Office Communicator. To hide this option from users, set this value to False. To show this option to users, set this value to True.
SetVideoStaticThrottlingPref	This value determines whether the user option to “Optimize video quality for your computer” is displayed in the Cisco UC Options dialog box in Cisco UC Integration for Microsoft Office Communicator. If selected, this option enables static video throttling. To hide this option from users, set this value to False. To show this option to users, set this value to True.

Specifying Security Certificate Value Names

Table 3-5 lists the name-value pair that you must use to specify the location of security certificates.

Table 3-5 Security Value Names

Value Names	Description
SECURITY_CertificateDirectory	<p>Specify the location of the directory where the security certificates are stored. For example, you might store LDAP or CCMCIP certificates in this location.</p> <p>Use this setting to specify a location for the certificates where the certificates will not be overwritten if you reinstall Cisco UC Integration for Microsoft Office Communicator.</p> <p>If you do not specify a value for this setting, the certificates are stored in the following locations:</p> <ul style="list-style-type: none"> Windows XP: <drive>:\Documents and Settings\<username>\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

Specifying LDAP Value Names

Table 3-6 lists the name-value pairs that you must use to specify the LDAP configuration.

Table 3-6 LDAP Value Names


Value Names	Description
LDAP_AttributeName_primaryPhoneNumberForSearches	<p>Specify the phone number that you use to resolve most LDAP queries. This value must match one of the values specified for the following LDAP keys:</p> <ul style="list-style-type: none"> LDAP_AttributeName_businessPhone LDAP_AttributeName_homePhone LDAP_AttributeName_mobilePhone LDAP_AttributeName_otherPhone <p>The values that are valid for the LDAP attribute keys listed above are:</p> <ul style="list-style-type: none"> telephoneNumber homePhone mobilePhone otherTelephone a custom LDAP attribute value, for example, myCustomPhoneNumber <p>The value of the LDAP_AttributeName_primaryPhoneNumberForSearches key must match one of the values in the list above, for example, telephoneNumber. Otherwise, the value of the LDAP_AttributeName_businessPhone key is used.</p>
LDAP_enableWildcardMatchesForPhoneNumberSearches	<p>Set this value to True if you want to enable wildcard searches for phone numbers in the LDAP.</p> <p>Note If you set this key to True, the speed of searches of the LDAP might be affected.</p>
LDAP_MaxCacheSize	Specify the maximum number of LDAP directory records to retain in the cache of the user.

Table 3-6 LDAP Value Names

Value Names	Description
LDAP_Server_1	<p>Enter the protocol name, followed by the fully-qualified domain name (FQDN) of your LDAP server. For example:</p> <p>ldap://ldap.example.com</p> <p>If you want to use a port number other than the default 389, add a colon to the value, followed by the port number. For example:</p> <p>ldap://ldap.example.com:19389</p> <p>If you want to use LDAP over SSL, this IP address must begin with <i>ldaps://</i>. For example:</p> <p>ldaps://ldap.example.com</p> <p>If you want to use a port number other than the default 636, add a colon to the value, followed by the port number. For example:</p> <p>ldaps://ldap.example.com:19636</p> <p>For more information about how to enable LDAP over SSL, see Enabling LDAP Over SSL, page 3-11.</p>
LDAP_SearchBaseDN_1, LDAP_SearchBaseDN_2, LDAP_SearchBaseDN_3, LDAP_SearchBaseDN_4, LDAP_SearchBaseDN_5	<p>Specify the primary distinguished name for the location in the LDAP directory from which searches begin. For example, specify a distinguished name similar to the following:</p> <p>OU=Sales,DC=example,DC=com</p> <p>Specify any further search bases also.</p>
LDAP_ResultSetMaxSize	<p>Specify the maximum number of records to return when the user searches the LDAP directory. That is, when the user searches for contacts in Microsoft Office Communicator.</p>
LDAP_UserLogonDomain	<p>Enter the name of the domain that contains the LDAP account of the user.</p>
LDAP_EnableAnonymousBind	<p>Set this value to True if the LDAP server is enabled for anonymous access. If this is the case, users do not have to supply credentials to access the LDAP server.</p>

Table 3-7 lists the values you must enter for LDAP attribute key names to enable Client Services Framework searches to map to the appropriate fields of the Active Directory.

Table 3-7 Values to Enter to Map Client Services Framework Searches to Active Directory

For This Value Name...	Enter the Following Active Directory Field...
LDAP_AttributeName_objectclassKey	objectclass
LDAP_AttributeName_objectclassValue	person
LDAP_AttributeName_userLogonName	userPrincipalName
LDAP_AttributeName_displayName	displayName
LDAP_AttributeName_commonName	cn
LDAP_AttributeName_firstName	givenName
LDAP_AttributeName_lastName	sn
LDAP_AttributeName_email	mail
LDAP_AttributeName_uri	msRTCSIP-PrimaryUserAddress
LDAP_AttributeName_photoUri	photoUri
LDAP_AttributeName_businessPhone	telephoneNumber
LDAP_AttributeName_homePhone	homePhone
LDAP_AttributeName_mobilePhone	mobilePhone
LDAP_AttributeName_otherPhone	otherTelephone
LDAP_AttributeName_title	title
LDAP_AttributeName_companyName	company
LDAP_AttributeName_userAccountName	sAMAccountName
	 <p>Note Do not use any other Active Directory field for this key name.</p>

Specifying Account Credential Synchronization Value Names

Client Services Framework includes settings that enable you to manage the credentials of Cisco Unified Communications back-end services. You can use these settings to configure the source of credentials for each service.

For example, you might have separate directories for your phone system, voicemail system, and meeting system. If you do not set the appropriate values for these services, your users have to select in the Cisco UC pane, then enter their username and password for each service.

Table 3-8 lists the name-value pair that you must use to specify the location of security certificates.

Table 3-8 Account Credential Synchronization Value Names

Value Names	Description
ContactService_UseCredentialsFrom VoicemailService_UseCredentialsFrom WebConfService_UseCredentialsFrom	You can set each of these names to one of the following values: <ul style="list-style-type: none"> • CONTACT • PHONE • VOICEMAIL • WEBCONF

Using an Active Directory Group Policy Administrative Template to Configure Client Services Framework Clients

A Group Policy administrative template is provided with Cisco UC Integration for Microsoft Office Communicator. You can use this template to define the Client Services Framework registry settings on a system, or for groups of users. The template file is CUCIMOC.adm.

Procedure

- Step 1** Execute the following command to start the Group Policy application:
gpedit.msc
- Step 2** Expand the **User Configuration** node.
- Step 3** Right-click **Administrative Templates**, then select **Add/Remove Templates**.
- Step 4** Add the file CUCIMOC.adm to the list of current policy templates in the Add/Remove Templates dialog box, then select **Close**.
- Step 5** Open the Cisco Unified Communications Integration for Microsoft Office Communicator folder in the right pane.



Note

In Windows Vista and Windows 7, this folder is in the Administrative Templates > Classic Administrative Templates folder. In Windows XP, this folder is in the Administrative Templates folder.

- Step 6** Open the folder for the settings whose value you want to specify.
- Step 7** Double-click the setting whose value you want to specify.

Step 8 Enter the value you require, then select **OK**.

After the ADM file is imported and populated, you can apply the resulting policy to an organizational unit using the Group Policy Management Editor.

Related Topics

- [Configuration of Policies for Microsoft Office Applications, page 3-14](#)

Enabling LDAP Over SSL

- [Creating a Certificate on the Active Directory Server, page 3-11](#)
- [Installing the Certificate on the Client Computer, page 3-11](#)
- [Configuring Client Services Framework, page 3-12](#)

Creating a Certificate on the Active Directory Server

Before You Begin

Ensure that the LDAP server is configured to support LDAP over SSL (LDAPS).

Procedure

Step 1 Sign in to the Active Directory server.

Step 2 Execute the following command:

```
certutil -ca.cert cucimoc.crt
```

This command generates a file called cucimoc.crt. You must install this certificate on each client computer.

What to Do Next

- [Installing the Certificate on the Client Computer, page 3-11](#)

Installing the Certificate on the Client Computer

Before You Begin

Before you install the certificate on the client computer, ensure that neither of the following processes are running:

- Client Services Framework, that is, the cucsfc.exe process.
- Cisco UC Integration for Microsoft Office Communicator, that is, the cucimoc.exe process.

Procedure

-
- Step 1** You install the cucimoc.crt file in the keystore of the Java Runtime Environment (JRE) that Client Services Framework is using. If you configured Client Services Framework to use the default JRE, the JRE is located in %CSF_INSTALL%\jre.
- Step 2** Execute the following command:
- keytool -importcert -keystore <path to cacerts> -storepass changeit -file <path to cert file>**
- For example, if the path to the Client Services Framework installation is C:\Program Files\Common Files\Cisco Systems\Client Services Framework\jre\bin, and the cucimoc.crt file is stored in C:\temp, you execute the following command:
- “C:\Program Files\Common Files\Cisco Systems\Client Services Framework\jre\bin\keytool” -importcert -keystore “C:\Program Files\Common Files\Cisco Systems\Client Services Framework\jre\lib\security\cacerts” -storepass changeit -file “C:\temp\cucimoc.crt”**
- The default password for the cacerts keystore is changeit.
- Step 3** When asked if you trust this certificate, enter **yes**.
-

What to Do Next

- [Configuring Client Services Framework, page 3-12](#)

Configuring Client Services Framework

Procedure

-
- Step 1** Set the value for the LDAP_Server_1 value name to set the URL of the LDAP server. For example, set the value of LDAP_Server_1 to the following:
- ldaps://ldap.example.com
- The only change from using standard LDAP is that you specify the protocol as *ldaps* instead of *ldap*.
- Use the FQDN of the LDAP server as specified in the certificate. You cannot use the IP address of the LDAP server, or the server name alone. Ensure that the FQDN is reachable. If the FQDN cannot be reached using DNS, add an appropriate entry to your hosts file.
- If your LDAP server does not use the default port for LDAPS, specify the port with the URL. For example, enter a value such as the following:
- ldaps://ldap.example.com:19636
- Step 2** Restart Cisco UC Integration for Microsoft Office Communicator.
- Step 3** To verify that you are connected to LDAPS, select the Menu button in the Microsoft Office Communicator title bar, then select **Tools > Server Status**.
- Read the server protocol information in the Server Status tab. The protocol is displayed as *ldap*. Read the server port field to verify that you are connected to LDAPS.
-

Related Topics

- [Configuring Value Names for the Client Services Framework Client Integration, page 3-2](#)

Configuring Microsoft Office Communicator 2007 to Use HTTPS to Access Custom Availability Statuses

Cisco UC Integration for Microsoft Office Communicator includes custom availability statuses such as “On the Phone”. These statuses are stored in the custom availability status file `cisco-presence-states-config.xml`.

For information about how to apply this policy setting to Microsoft Office Communicator, see the following URL:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=dd3cae08-3153-4c6a-a314-daa79d616248&displaylang=en>

Microsoft Office Communicator 2007 R1

The location of the `cisco-presence-states-config.xml` file is set in the *Custom presence states URL* Microsoft Office Communicator group policy setting. In Microsoft Office Communicator 2007 R1 this URL can use any of the following protocols:

- `file://`
- `http://`
- `https://`

Cisco UC Integration for Microsoft Office Communicator installs the `cisco-presence-states-config.xml` file in the local file system of the computer of the user. Cisco UC Integration for Microsoft Office Communicator also updates the Custom presence states URL group policy setting to refer to this file with the `file://` protocol.

Microsoft Office Communicator 2007 R2

By default, in Microsoft Office Communicator 2007 R2, the URL specified in the Custom presence states URL group policy setting must begin with `https://`.

As a result, Microsoft Office Communicator 2007 R2 cannot use the Cisco UC Integration for Microsoft Office Communicator custom availability statuses. In this case, Cisco UC Integration for Microsoft Office Communicator uses the generic Microsoft Office Communicator “Busy” availability status instead of the Cisco UC Integration for Microsoft Office Communicator “Busy: On the phone” custom availability status.

To enable the custom availability statuses, do the following:

1. Put a copy of the `cisco-presence-states-config.xml` file on a secure web server, that is, a server that you can access with the `https://` protocol. You can use the same IIS server that runs on your OCS server.
2. Update the “Custom presence states URL” group policy setting or registry setting on the computers of your users with the `https://` URL of the `cisco-presence-states-config.xml` file.

For information about how to apply these policy settings to Microsoft Office Communicator, see *Microsoft Office Communications Server 2007 R2 Client Group Policy Documentation* at the following URL:

<http://www.microsoft.com/DOWNLOADS/details.aspx?familyid=5D6F4B90-6980-430B-9F97-FFADBC07B7A9&displaylang=en>

Location of Custom Availability Statuses File

On computers that have Cisco UC Integration for Microsoft Office Communicator installed, the `cisco-presence-states-config.xml` file is in the following location:

```
<drive>:\Program Files\Cisco Systems\Cisco UC Integration TM for Microsoft Office
Communicator\Config\presence
```

Configuration of Policies for Microsoft Office Applications

- [Microsoft Office Communicator Policies, page 3-14](#)
- [Microsoft Office Phone Policy, page 3-15](#)

Microsoft Office Communicator Policies

We recommend that you configure Microsoft Office Communicator policies to allow only IM and availability status traffic on all Cisco UC Integration for Microsoft Office Communicator user groups.

If you do not do this, voice traffic is allowed from both Cisco UC Integration for Microsoft Office Communicator *and* Microsoft Office Communicator. This can result in the following problems:

- A confusing user experience, as users can place and receive calls from a mixture of user interface elements in both applications.
- Inconsistent voice traffic. That is, calls from Cisco UC Integration for Microsoft Office Communicator might give a different audio experience to Microsoft Office Communicator.
- A mixed configuration is more difficult to manage, as administrators must track traffic from two sources. You might want to monitor voice usage in your network and if you use both applications, you must configure your monitoring tools to track traffic from both applications.

We recommend that you configure the Microsoft Office Communicator policies as shown in the following table:

Policy	Set Value To...
TelephonyMode	5 = IM and Presence Only
DisableAVConferencing	1

For information about how to apply these policy settings to Microsoft Office Communicator, see the following URL:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=dd3cae08-3153-4c6a-a314-daa79d616248&displaylang=en>

You can also find the policy administrative template file `Communicator.adm` on that web site.

Alternatively, you can apply the following keys to set the policies manually:

```
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Communicator]"TelephonyMode"=dword:00000005
```

```
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Communicator]"DisableAVConferencing"=dword:00000001
```

Related Topics

- [Configuring Value Names for the Client Services Framework Client Integration, page 3-2](#)

Microsoft Office Phone Policy

We recommend that you configure a Microsoft Office policy to disable the Call menu that appears when you select a contact in a Microsoft Office application. This Call menu only appears if you have the correct smart tag switched on in the relevant Microsoft Office application.

Cisco UC Integration for Microsoft Office Communicator provides an Additional Actions menu that enables you to call contacts that you select in your Microsoft Office applications. If you do not disable the Call menu, this can result in a confusing user experience, as users might think that they can perform similar actions from a mixture of user interface elements.

To disable the Call menu in Microsoft Office, set the value of the Phone policy to zero (0).

Alternatively, you can apply the key to set the policy manually.

```
[HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\PersonaMenu]"Phone"=dword:00000000
```

**Note**

In the registry keys, the values 11.0 and 12.0 refer to the different versions of Microsoft Office; 11.0 refers to Microsoft Office 2003 and 12.0 refers to Microsoft Office 2007.

About the Client Services Framework Cache and LDAP Searches

Cisco Unified Client Services Framework allows users to cache the following user credentials between sign-outs and sign-ins:

- Cisco Unified Communications Manager
- Voicemail
- LDAP
- Cisco Unified MeetingPlace

Client Services Framework also maintains a cache of LDAP contacts. This cache is only updated from LDAP when Client Services Framework is restarted.

When you place a call, receive a call, or miss a call, the contacts for the calls are added to your Client Services Framework cache. Any contact that is in your conversation history is automatically placed in your cache. All of the data for the contacts in your contact list in Microsoft Office Communicator is also cached.

If a contact for a call already exists in the cache, Client Services Framework does not search LDAP. If a contact does not exist in the cache, Client Services Framework searches LDAP. LDAP searches are only performed when you place a call to, or receive a call from a contact who is not in your conversation history or your Microsoft Office Communicator contact list.

All contacts in the Client Services Framework cache have already had the directory lookup dialing rules applied to all of their numbers. When Cisco UC Integration for Microsoft Office Communicator displays numbers for contacts that are in the Client Services Framework cache, the numbers have already had the directory lookup dialing rules applied to them.

The Client Services Framework cache is a memory-only cache. The contents of the cache are *not* copied to a local file system. When the `cucsf.exe` process is restarted, the contents of the Client Services Framework cache are refreshed.

- [Incoming Calls, page 3-16](#)
- [Outgoing Calls to Contacts Who Are Enabled for OCS, page 3-16](#)
- [Outgoing Calls to Contacts Who Are Not Enabled for OCS, page 3-17](#)
- [Outgoing Calls to Microsoft Outlook Contacts, page 3-17](#)

Incoming Calls

When a user receives a call, the following events occur:

1. When Cisco Unified Communications Manager detects the incoming call, it sends the following data to Client Services Framework:
 - The directory number from which the call originates.
 - The Alerting Name of the directory number that is specified in the Directory Number Configuration screen, if the field is not blank.
2. Client Services Framework sends the directory number and alerting name to Cisco UC Integration for Microsoft Office Communicator.
3. Cisco UC Integration for Microsoft Office Communicator displays the directory number and the LDAP name (if resolved, otherwise the alerting name) in a notification window and, if the call is answered, in the conversation window.
4. If the directory number is not in the Client Services Framework cache, Client Services Framework applies any directory lookup dialing rules to the directory number. This occurs while Client Services Framework transmits the data to Cisco UC Integration for Microsoft Office Communicator.
5. If the directory number is not in the Client Services Framework cache, Client Services Framework searches LDAP for the number that is returned *after* the directory number is processed by the directory lookup dialing rules.
6. LDAP sends the LDAP data for any matches back to Client Services Framework, including data such as other phone numbers, and a URI of a photo of the caller.
7. Client Services Framework updates the data for the contact and sends the updated data to Cisco UC Integration for Microsoft Office Communicator.
8. Cisco UC Integration for Microsoft Office Communicator updates the conversation window. For example, at this point a photo of the caller might be displayed as the `photoURI` field from LDAP is passed to Cisco UC Integration for Microsoft Office Communicator by Client Services Framework.

Outgoing Calls to Contacts Who Are Enabled for OCS

When a user places a call to a contact who is enabled for OCS, the following events occur:

1. Cisco UC Integration for Microsoft Office Communicator sends the number for the contact to be called to Client Services Framework, and asks Client Services Framework to place a call to that number.
2. If the contact is not in the Client Services Framework cache, Client Services Framework searches LDAP for details of the party to be called.

3. LDAP sends data back to Client Services Framework.
4. Client Services Framework sends data about the contact back to Cisco UC Integration for Microsoft Office Communicator. If the contact has several numbers, Cisco UC Integration for Microsoft Office Communicator displays a window from which the user selects the number to call. If the contact has only one number, Cisco UC Integration for Microsoft Office Communicator places the call.
5. Client Services Framework applies any directory lookup dialing rules to the number to be called.
6. Client Services Framework searches LDAP for the number that is returned after the directory lookup dialing rules are applied.
7. Client Services Framework applies the application dialing rules and sends the number to Cisco Unified Communications Manager.
8. Cisco Unified Communications Manager places the call.

Outgoing Calls to Contacts Who Are Not Enabled for OCS

When a user places a call to a contact who is not enabled for OCS, the following events occur:

1. Cisco UC Integration for Microsoft Office Communicator sends the display name for the contact to Client Services Framework.
2. If the contact is not in the Client Services Framework cache, Client Services Framework searches LDAP for the contact associated with the display name. The operator for this search is *contains* rather than *equals*.
3. If the LDAP search returns more than one contact, Cisco UC Integration for Microsoft Office Communicator displays a window from which the user selects the number to call. If the contact has only one number, Cisco UC Integration for Microsoft Office Communicator places the call.
4. Client Services Framework applies any directory lookup dialing rules to the number to be called.
5. Client Services Framework searches LDAP for the number that is returned after the directory lookup dialing rules are applied.
6. Client Services Framework applies the application dialing rules and sends the number to Cisco Unified Communications Manager.
7. Cisco Unified Communications Manager places the call.

Outgoing Calls to Microsoft Outlook Contacts

When a user places a call to a Microsoft Outlook contact, the following events occur:

1. The user drags a contact from the Microsoft Office Communicator to the Cisco UC pane.
2. Cisco UC Integration for Microsoft Office Communicator searches the Microsoft Outlook contacts for a user that matches the display name. If a contact is found, then the contact is added to the Client Services Framework cache.
3. Client Services Framework applies any directory lookup dialing rules to the phone numbers of the contact.
4. Client Services Framework searches LDAP for the number that is returned after the directory lookup dialing rules are applied.

5. Client Services Framework applies the application dialing rules and sends the number to Cisco Unified Communications Manager.
6. Cisco Unified Communications Manager places the call.

How to Configure Cisco UC Integration for Microsoft Office Communicator Clients for Secure Access to Cisco Unified MeetingPlace

- [Configuring Secure Access to Cisco Unified MeetingPlace, page 3-18](#)
- [Downloading the IIS Certificate from Cisco Unified MeetingPlace, page 3-18](#)

Configuring Secure Access to Cisco Unified MeetingPlace

For information about how to set up the Cisco Unified MeetingPlace web server for secure access, see the *Administration Documentation for Cisco Unified MeetingPlace* at:

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

What To Do Next

[Downloading the IIS Certificate from Cisco Unified MeetingPlace, page 3-18](#)

Downloading the IIS Certificate from Cisco Unified MeetingPlace

Procedure

- Step 1** Open the Internet Services Manager on the Cisco Unified MeetingPlace Web Server.
Select **Start > Programs > Administrative Tools > Internet Information Services Manager**.
- Step 2** Navigate to Default Web Site.
Select the + sign beside Local Server > Web Sites to open the appropriate directory trees.
- Step 3** Right-click **Default Web Site**.
- Step 4** Select **Properties**.
- Step 5** Select the **Directory Security** tab.
- Step 6** Select **Server Certificate**. The Web Server Certificate wizard displays.
- Step 7** Select **Next**.
- Step 8** Select **Export the current certificate to a pfx file**, then select **Next**.
- Step 9** Select **Browse** and select to save the certificate file to your desktop.
- Step 10** Select **Next**.
- Step 11** Enter a password to encrypt the certificate.

- Step 12** Enter the password again to confirm it, then select **Next**. The Export Certificate Summary Screen displays and the exported certificate file is now on your desktop.
- Step 13** Select **Next**.
- Step 14** Select **Finish** to close the Web Server Certificate wizard.

What To Do Next

[Installing Security Certificates on Client Computers, page 3-21](#)

How to Configure Cisco UC Integration for Microsoft Office Communicator Clients to Enable Secure Voicemail Access

- [Configuring Secure Voicemail Access to a Cisco Unity Server, page 3-19](#)
- [Configuring Secure Voicemail Access to a Cisco Unity Connection Server, page 3-20](#)

Configuring Secure Voicemail Access to a Cisco Unity Server

Procedure

- Step 1** Set the following registry values:

Value Name	Set Value to...
VVM_SystemServer_0 ¹	The IP address of the Cisco Unity Server
VVM_SystemServer_VmwsProtocol_0	HTTPS
VVM_SystemServer_VmwsPort_0	443

1. The last character in the value names described in this table can be 0 or 1 depending on whether the server is a primary or secondary server.

- Step 2** Download a certificate for secure access to Cisco Unity. For more information, see [Downloading the IIS Certificate from Cisco Unity, page 3-19](#).
- Step 3** Install the certificate on the client computer, see [Enabling LDAP Over SSL, page 3-11](#).

Downloading the IIS Certificate from Cisco Unity

Procedure

- Step 1** Start a browser on the Cisco Unity server.
- Step 2** Use the HTTPS protocol to access the URL of the Cisco Unity server.

You can access the URL structured as follows:

`https://<localhost>`

For example, access:

<https://unityserver/>

- Step 3** Select **View Certificate** on the security dialog box.
- Step 4** Select the **Details** tab.
- Step 5** Select **Copy to File**.
- Step 6** Select **DER encoded binary X.509 (.CER)**, then select **Next**.
- Step 7** Enter a filename for the certificate, then select **Next**.
- Step 8** Verify the details of your certificate on the Completing the Certificate Export Wizard screen, then select **Finish**.

What To Do Next

[Enabling LDAP Over SSL, page 3-11](#)

Configuring Secure Voicemail Access to a Cisco Unity Connection Server

Procedure

- Step 1** Set the following registry values:

Value Name	Set Value to...
VVM_Mailstore_Server_0 ¹	The IP address of the Cisco Unity Connection server
VVM_Mailstore_ImapProtocol_0	TLS
VVM_Mailstore_ImapPort_0	7993
VVM_Mailstore_EncryptedConnection	True

1. The last character in the first three value names described in this table can be 0 or 1 depending on whether the server is a primary or secondary server.

- Step 2** Download a certificate for secure access to Cisco Unity Connection. For more information, see [Downloading the Tomcat Certificate from Cisco Unity Connection, page 3-20](#).
- Step 3** Install the certificate on the client computer, see [Enabling LDAP Over SSL, page 3-11](#).

Downloading the Tomcat Certificate from Cisco Unity Connection

Procedure

- Step 1** Select **Security > Certificate Management** in Cisco Unified Operating System Administration.
- Step 2** Find the Tomcat certificate.
- Step 3** Select the **tomcat.der** link.

Step 4 Select **Download**, then save the tomcat.der file to your computer.

What To Do Next

[Enabling LDAP Over SSL, page 3-11](#)

Installing Security Certificates on Client Computers

Procedure

Step 1 Put the certificate file into the folder where you store your security certificates.

Step 2 Use the SECURITY_CertificateDirectory registry key value name to specify the folder where the certificates are stored.

Related Topics

- [Specifying Security Certificate Value Names, page 3-6](#)



CHAPTER 4

Installing Cisco Unified Communications Integration for Microsoft Office Communicator

Revised: July 7, 2011

- [Removing Cisco Unified Video Advantage, page 4-1](#)
- [Cisco UC Integration for Microsoft Office Communicator Deployment, page 4-1](#)
- [Information to Provide to Users After Installation, page 4-4](#)

Removing Cisco Unified Video Advantage

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



Tip

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

Cisco UC Integration for Microsoft Office Communicator Deployment



Note

Before you deploy Cisco UC Integration for Microsoft Office 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.

The Cisco UC Integration for Microsoft Office Communicator installation application installs the following components:

- User interface for Cisco UC Integration for Microsoft Office Communicator.

- The client-related components of the Client Services Framework.
- Click to Call functionality (optional).

The Cisco UC Integration for Microsoft Office Communicator application is provided in two separate installation formats as follows:

- Cisco UC Integration for Microsoft Office Communicator executable file.
- Cisco UC Integration for Microsoft Office Communicator Windows Installer (MSI) file.

This section describes the installation formats and the deployment options.

- [Executable File, page 4-2](#)
- [Windows Installer \(MSI\) File, page 4-3](#)
- [Deployment Options, page 4-3](#)

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 UC Integration for Microsoft Office 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 UC Integration for Microsoft Office 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 UC Integration for Microsoft Office 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 Microsoft .Net Framework 3.5 Service Pack 1 in advance of the Cisco UC Integration for Microsoft Office Communicator installation to save time and avoid any internet access issues. For more information about the minimum required version of .Net Framework, see the *Release Notes for Cisco Unified Communications Integration for Microsoft Office Communicator*.

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 UC Integration for Microsoft Office Communicator.

**Note**

If you choose to install the MSI file, you must install the prerequisite software prior to installing Cisco UC Integration for Microsoft Office Communicator.

The prerequisite software that you must install prior to installing the Cisco UC Integration for Microsoft Office 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 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)

The prerequisite software is available from the Microsoft website.

Deployment Options

You can deploy the Cisco UC Integration for Microsoft Office Communicator installation application in one of the following ways:

- [Automated Mass Deployment, page 4-3](#)
- [Standalone Installation, page 4-4](#)

Automated Mass Deployment

The mass deployment options for installing Cisco UC Integration for Microsoft Office 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

You can install Cisco UC Integration for Microsoft Office Communicator on each individual client computer or users can install the application on their own computers. You deploy the administrator configuration settings.


Note



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

Upgrading Cisco UC Integration for Microsoft Office Communicator

To upgrade Cisco UC Integration for Microsoft Office Communicator, you do not need to uninstall Cisco UC Integration for Microsoft Office Communicator. When you install a newer version, the installation application uninstalls the previous version of Cisco UC Integration for Microsoft Office Communicator, then installs the new version.

Information to Provide to Users After Installation

When your installation of Cisco UC Integration for Microsoft Office Communicator is complete, you can provide the information in the following table to your users:

Provide...	Explanation
Sign-in information.	Depending on whether or not the phone service, voicemail service, contact service and web conference service credentials are synchronized, users might need to select  in the Cisco UC pane and enter their credentials for each service. For more information, see Specifying Account Credential Synchronization Value Names , page 3-10.
Instructions for using the application.	Provide users with information about how to access the online help, as follows <ol style="list-style-type: none"> 1. Select  in the Microsoft Office Communicator title bar. 2. Select Tools > FAQ on Cisco UC. You can also provide users with the <i>Frequently Asked Questions: Cisco Unified Communications Integration for Microsoft Office Communicator</i> , which contains the same information as the online help.

Provide...	Explanation
Information about how to tune computers for maximum video performance.	<p data-bbox="618 260 1209 296">Setting the CPU Speed to Maximum Performance</p> <p data-bbox="618 302 1524 499">The power settings of your computer, particularly a laptop, can affect the video capabilities of your system. The power settings allow users to reduce CPU speed and performance to save battery life. This can also reduce the video capabilities of a computer. For optimum video performance, you should set the power scheme to the maximum performance to ensure that the CPU speed is also operating at maximum performance.</p> <p data-bbox="618 506 771 541"><u>Windows XP</u></p> <ol data-bbox="618 548 1485 678" style="list-style-type: none"> <li data-bbox="618 548 1242 583">1. Open the Control Panel and select Power Options. <li data-bbox="618 590 1015 625">2. Select the Power Schemes tab. <li data-bbox="618 632 1485 678">3. Select Maximum Performance from the Power schemes drop-down list. <p data-bbox="618 684 792 720"><u>Windows Vista</u></p> <ol data-bbox="618 726 1461 846" style="list-style-type: none"> <li data-bbox="618 726 1461 804">1. Open the Control Panel and select System and Maintenance > Power Options. <li data-bbox="618 810 1088 846">2. Select the High Performance option. <p data-bbox="618 852 750 888"><u>Windows 7</u></p> <ol data-bbox="618 894 1518 1024" style="list-style-type: none"> <li data-bbox="618 894 1518 930">1. Open the Control Panel and select System and Security > Power Options. <li data-bbox="618 936 1015 972">2. Select Show additional plans. <li data-bbox="618 978 1088 1024">3. Select the High Performance option. <hr/> <p data-bbox="618 1031 1258 1066">Setting Your Graphics Hardware to Full Acceleration</p> <p data-bbox="618 1073 771 1108"><u>Windows XP</u></p> <ol data-bbox="618 1115 1234 1287" style="list-style-type: none"> <li data-bbox="618 1115 1153 1150">1. Open the Control Panel and select Display. <li data-bbox="618 1157 925 1192">2. Select the Settings tab. <li data-bbox="618 1199 1234 1234">3. Select Advanced and select the Troubleshoot tab. <li data-bbox="618 1241 1161 1287">4. Set the Hardware acceleration slider to Full. <p data-bbox="618 1293 792 1329"><u>Windows Vista</u></p> <ol data-bbox="618 1335 1469 1539" style="list-style-type: none"> <li data-bbox="618 1335 1469 1413">1. Open the Control Panel and select Appearance and Personalization > Personalization > Display Settings. <li data-bbox="618 1419 966 1455">2. Select Advanced Settings. <li data-bbox="618 1461 1307 1497">3. Select the Troubleshoot tab and select Change Settings. <li data-bbox="618 1503 1161 1539">4. Set the Hardware acceleration slider to Full. <p data-bbox="618 1545 750 1581"><u>Windows 7</u></p> <ol data-bbox="618 1587 1469 1749" style="list-style-type: none"> <li data-bbox="618 1587 1469 1665">1. Open the Control Panel and select Appearance and Personalization > Display > Change Display Settings > Advanced Settings. <li data-bbox="618 1671 1307 1707">2. Select the Troubleshoot tab and select Change Settings. <li data-bbox="618 1713 1161 1749">3. Set the Hardware acceleration slider to Full. <p data-bbox="618 1755 1518 1898">Note To support this setting, you may need to update the driver for your video adapter. For information about how to obtain an updated driver for your video adapter, contact the manufacturer of your video adapter or the manufacturer of your computer.</p>

■ Information to Provide to Users After Installation

Provide...	Explanation
Internal company support for the application.	Provide your users with the names of people to contact for assistance if they encounter problems with the application.
Tip regarding the removal of a protective strip from the camera lens.	Some personal computers with built-in cameras are shipped with a protective plastic strip over the lens. To avoid issues with poor video quality, users must remove the plastic strip from the lens.



CHAPTER 5

Support for Microsoft Business Productivity Online Standard Suite

Revised: July 7, 2011

Cisco UC Integration for Microsoft Office Communicator supports environments where a Microsoft Office Communications Server is hosted within the Microsoft Business Productivity Online Standard Suite (BPOS).

The following sections provide an overview of the configuration consideration when you deploy the Cisco UC Integration for Microsoft Office Communicator in an environment that is hosted by BPOS:

- [Requirements for Using Cisco UC Integration for Microsoft Office Communicator with BPOS, page 5-1](#)
- [Architecture of Cisco UC Integration for Microsoft Office Communicator in a BPOS Environment, page 5-2](#)
- [User Phone Numbers Must Use +E.164 Formatting, page 5-2](#)
- [User Authentication, page 5-3](#)
- [Using Cisco UC Integration for Microsoft Office Communicator with Microsoft Exchange in a BPOS Environment, page 5-3](#)

Requirements for Using Cisco UC Integration for Microsoft Office Communicator with BPOS

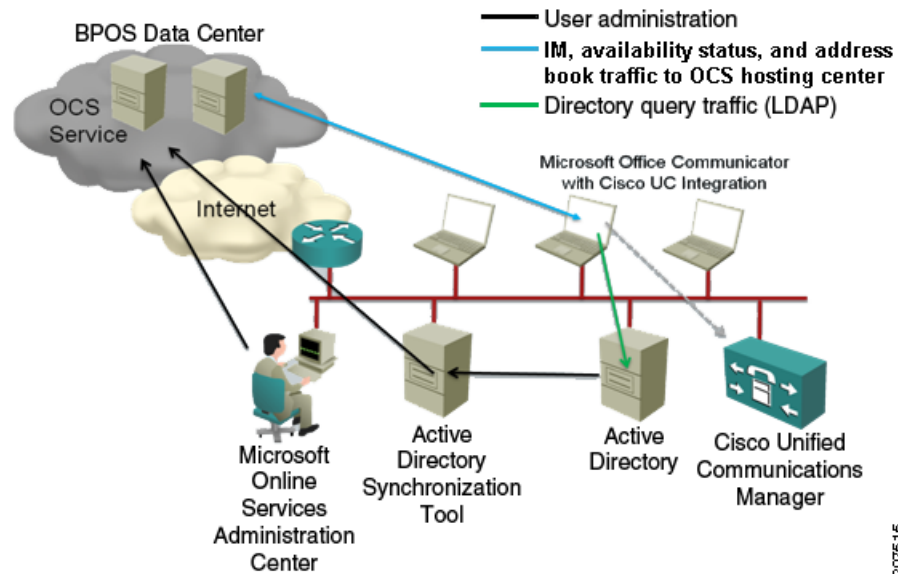
You can use Cisco UC Integration for Microsoft Office Communicator with Microsoft Office Communicator and BPOS if the following conditions are met:

- The Active Directory server required by the Cisco UC Integration for Microsoft Office Communicator, and used as an LDAP server is located within the enterprise network.
- The BPOS user accounts are synchronized from the Active Directory user accounts in the enterprise. You can use the following tools to do this:
 - Active Directory Synchronization Tool.
 - Microsoft Online Services Administration Center. You add the user accounts manually with this tool.
- All phone numbers in the BPOS environment are defined in +E.164 format.
- Cisco UC Integration for Microsoft Office Communicator supports the version of Microsoft Office Communicator that is being used. For more information about the supported versions of Microsoft Office Communicator, see the *Release Notes for Cisco Unified Communications Integration for Microsoft Office Communicator* at the following location:

http://www.cisco.com/en/US/products/ps9829/prod_release_notes_list.html

Architecture of Cisco UC Integration for Microsoft Office Communicator in a BPOS Environment

The following illustration shows how the Cisco UC Integration for Microsoft Office Communicator operates in a BPOS environment:



The Cisco UC Integration for Microsoft Office Communicator has no direct interaction with the hosted Microsoft Office Communicator servers. All interaction happens through the Microsoft Office Communicator application programming interfaces (APIs).

The Cisco UC Integration for Microsoft Office Communicator uses LDAP to interact with an enterprise-based Active Directory server. The Cisco UC Integration for Microsoft Office Communicator also interacts with Cisco Unified Communications Manager for voice and video media services.

User Phone Numbers Must Use +E.164 Formatting

When you call a contact, the Cisco UC Integration for Microsoft Office Communicator mostly gets contact phone numbers from the Microsoft Office Communicator address book. In a BPOS environment, the address book is downloaded from the BPOS service.

To populate the address book with the phone numbers of the Microsoft Office Communicator users, the OCS address book service in the BPOS data center must enter the phone numbers into address book files correctly.

The OCS address book service only enters +E.164-formatted phone numbers into the address book. Phone numbers that are not in this format are excluded from the address book. All phone numbers provided to the BPOS service *must* be in +E.164 format.

For more information about the +E.164 standard and Cisco UC Integration for Microsoft Office Communicator, see the *Installation Guide for Cisco Unified Communications Integration for Microsoft Office Communicator* at the following URL:

http://www.cisco.com/en/US/products/ps10317/tsd_products_support_series_home.html

**Note**

Do not use spaces in +E.164 phone numbers.

User Authentication

The Microsoft Online Services Sign In tool performs Microsoft Office Communicator authentication. This tool manages the Microsoft Office Communicator sign-in process.

The Cisco UC Integration for Microsoft Office Communicator sign-in process is authenticated using Cisco Unified Communications Manager and/or Active Directory, depending on how the authentication is set up. The BPOS environment does not change the default authentication process for the Cisco UC Integration for Microsoft Office Communicator.

**Note**

If your organization uses a dedicated BPOS environment your users might not be required to use the Microsoft Online Services Sign in tool with Microsoft Office Communicator.

Using Cisco UC Integration for Microsoft Office Communicator with Microsoft Exchange in a BPOS Environment

The BPOS service can also provide a Microsoft Exchange service. The Cisco UC Integration for Microsoft Office Communicator includes an option that users can select to save conversation history in Microsoft Outlook. This option has been tested with an Outlook client integrated into a BPOS-hosted Exchange server.

The Cisco UC Integration for Microsoft Office Communicator can also operate in an environment where OCS is hosted within BPOS, and Exchange is hosted within the enterprise data center.



CHAPTER 6

Troubleshooting Cisco Unified Communications Integration for Microsoft Office Communicator

Revised: July 7, 2011

- [Setting Logging Levels Before You Create a Problem Report, page 6-1](#)
- [Moving a Device to Another Cluster, page 6-2](#)
- [How to Resolve General Problems with the Integration, page 6-3](#)
- [How to Resolve Synchronization Problems, page 6-10](#)
- [How to Resolve Availability Status Problems, page 6-11](#)
- [How to Resolve Click to Call Problems, page 6-13](#)
- [How to Resolve Instant Message Window Problems, page 6-16](#)
- [How to Resolve Voicemail Problems, page 6-17](#)
- [How to Resolve Video Problems, page 6-17](#)
- [How to Resolve Camera Problems, page 6-18](#)
- [How to Resolve LDAP Problems, page 6-19](#)

Setting Logging Levels Before You Create a Problem Report

By default, when you start Cisco UC Integration for Microsoft Office Communicator and Client Services Framework, the logging level is set to Default.

If you want to report a problem with Cisco UC Integration for Microsoft Office Communicator, you must set the logging level in Cisco UC Integration for Microsoft Office Communicator to Verbose before you create the problem report. To set the logging level, select the Options button in the Cisco UC pane, select **Verbose** as the logging level, then select **OK**.

To obtain logs for Cisco UC Integration for Microsoft Office Communicator from a user, ask the user to create a problem report and send the report to you. For information about how to create a problem report, see the FAQ help or the user documentation for Cisco UC Integration for Microsoft Office Communicator at the following URL:

http://www.cisco.com/en/US/products/ps10317/products_user_guide_list.html

Alternatively, you can view the log files in the following locations:

Operating System	Log File Location
Windows XP	<drive>:\Documents and Settings\<username>\Local Settings\Application Data\Cisco\Unified Communications\Cucimoc\Logs
Windows Vista Windows 7	<drive>:\Users\<username>\AppData\Local\Cisco\Unified Communications\Cucimoc\Logs

Moving a Device to Another Cluster

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, you must update the CTL file for the device list of servers in the new cluster.

Procedure

Step 1 Delete the contents of the appropriate folder as described in the following table:

Operating System	Folder
Windows XP	<drive>:\Documents and Settings\<username>\Application Data\Cisco\Unified Communications\Client Services Framework\Security\sec
Windows Vista Windows 7	<drive>:\Users\<username>\AppData\Roaming\Cisco\Unified Communications\Client Services Framework\Security\sec

Step 2 Delete the contents of the appropriate folder as described in the following table:

Operating System	Folder
Windows XP	<drive>:\Documents and Settings\<username>\Application Data\Cisco\Unified Communications\Client Services Framework\Config
Windows Vista Windows 7	<drive>:\Users\<username>\AppData\Roaming\Cisco\Unified Communications\Client Services Framework\Config

Step 3 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.

How to Resolve General Problems with the Integration

- [How to Resolve Synchronization Problems, page 6-10](#)
- [Cisco UC Integration for Microsoft Office Communicator Is Slow To Start, page 6-5](#)
- [Users Cannot See the Cisco UC Integration for Microsoft Office Communicator Menu Items, page 6-5](#)
- [Cisco Unified IP Phone 7931G Users Cannot Control Desk Phone from Cisco UC Integration for Microsoft Office Communicator, page 6-5](#)
- [Audio Devices Are Selected Incorrectly, page 6-6](#)
- [Cisco UC Pane Takes a Long Time to Connect, page 6-6](#)
- [Cisco UC Pane Stops Responding If Windows Security Fails, page 6-6](#)
- [Incorrect Caller Name Displayed for Shared Lines, page 6-7](#)
- [Users with More Than One Directory Number Not Added to Conference Call, page 6-7](#)
- [CAST Connection from IP Phone Times Out, page 6-8](#)
- [Users Lose Control of the Active Call on the Desk Phone, page 6-8](#)
- [Users Cannot See the Participant List for the Conference Call, page 6-8](#)
- [Participant List for the Conference Call is Incorrect, page 6-8](#)
- [Numbers Published by Users in Microsoft Office Communicator Not Recognized, page 6-8](#)
- [Cisco UC Integration for Microsoft Office Communicator Menu Items Available but Not Functional, page 6-9](#)
- [Call Ends Unexpectedly, page 6-9](#)
- [Users Can Only Control One Line on Phones Configured for Multiple Lines, page 6-9](#)
- [Cannot See All Calls in Progress on Cisco Unified IP Phone 9900, 8900, and 6900 Model Series, page 6-9](#)
- [Conversation History Events Marked as Unread, page 6-10](#)

Cisco UC Integration for Microsoft Office Communicator Fails to Start

Problem The Cisco UC Integration for Microsoft Office Communicator fails to start, displaying a general exception error.

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

Possible Cause	Description
1	<p>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:</p> <ul style="list-style-type: none"> 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	<p>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:</p> <ul style="list-style-type: none"> 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\Cucimoc\Logs
- Windows Vista and Windows 7** - <drive>:\Users\<username>\AppData\Local\Cisco\Unified Communications\Cucimoc\Logs

Solution To resolve this issue, do the following:

- Open the **Control Panel**.
- Select **Regional and Language Options**.
- Select the **Regional Options** tab.
- In the Standards and formats section, select a different language from the drop-down list. For example, select **English (Australia)**.
- Select **Apply**.
- In the Standards and formats section, select **English (United States)** from the drop-down list.
- Select **Apply** again, then select **OK**.

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


Cisco UC Integration for Microsoft Office Communicator Is Slow To Start

Problem When users start the Cisco UC Integration for Microsoft Office Communicator, more than a minute might pass before the Cisco UC Integration user interface is displayed. This occurs when the user cannot create an SSL connection to Verisign, the Digital Signature Certificate Authority for Cisco. This problem typically occurs if the user is in an organization that uses web proxies, content filtering, or strict web access controls.

By default, .NET Framework applications validate the certificate of the publisher before the user interface is displayed. The application creates an SSL connection to Verisign. If the application cannot connect to Verisign, the standard HTTP timeout of 60 seconds occurs. After this timeout, the application starts and validation of the certificate is deferred.

Solution Open the Internet Options item in your Control Panel. Select the **Advanced** tab, and uncheck **Check for publisher's certificate revocation** in the Security section.

Users Cannot See the Cisco UC Integration for Microsoft Office Communicator Menu Items

Problem When users select  in the Microsoft Office Communicator title bar, then select Tools, the following menu items are missing:

- FAQ on Cisco UC
- Select Phone for Cisco UC
- Create Problem Report
- Server Status and Notifications
- About Cisco UC
- Sign Out of Cisco UC
- Start Cisco UC
- Stop Cisco UC

This problem occurs if the computer has no network connection.

Solution Close Microsoft Office Communicator, connect to a network, then restart Microsoft Office Communicator.

Cisco Unified IP Phone 7931G Users Cannot Control Desk Phone from Cisco UC Integration for Microsoft Office Communicator

Problem Users who have a Cisco Unified IP Phone 7931G cannot use their desk phone from Cisco UC Integration for Microsoft Office Communicator.


Solution Set the value of the Outbound Call Rollover field to **No Rollover** in Cisco Unified Communications Manager, as follows:

-
- Step 1** Select **Device > Phone** in Cisco Unified Communications Manager Administration.
 - Step 2** Search for the Cisco Unified IP Phone 7931G phone of the user in the Find and List Phones window.
 - Step 3** Select the Cisco Unified IP Phone 7931G phone.

- Step 4** Select **No Rollover** from the Outbound Call Rollover list box in the Protocol Specific Information section.
- Step 5** Select **Save**.
-

Audio Devices Are Selected Incorrectly

Problem Users might experience audio device selection issues. For example, audio might be played on the computer speakers, but the headset microphone is the active microphone, rather than the microphone on the computer.

Cisco UC Integration for Microsoft Office Communicator does not support the Default option in the Microsoft Office Communicator Set Up Audio and Video feature. Ensure that users select the Custom option when they configure the audio devices for Cisco UC Integration for Microsoft Office Communicator. To do this, the user must select  in the Microsoft Office Communicator title bar, then select **Tools > Setup Audio and Video**. For more information, see the FAQ help or the user documentation for Cisco UC Integration for Microsoft Office Communicator at the following URL:

http://www.cisco.com/en/US/products/ps10317/products_user_guide_list.html

Cisco UC Pane Takes a Long Time to Connect

Problem When a user starts Microsoft Office Communicator, the “Connecting...” message is displayed, but the application does not connect to the Cisco UC pane within five minutes.

Solution Host Intrusion Protection Software (HIPS) software might unexpectedly terminate the cucimoc.exe process. Start the Task Manager, then check if the cucimoc.exe process is running. If the process is not running, check if there is HIPS software running on your computer. Disabling HIPS software might help to resolve this problem. For information about HIPS software updates that might resolve this issue, please contact your HIPS vendor.

The exact cause of the process termination is not clear. Please report such incidents to Cisco support to help to determine the root cause of the problem and to help identify a solution.

Cisco UC Pane Stops Responding If Windows Security Fails

Problem Cisco Unified Communications Integration for Microsoft Office Communicator uses Windows security to secure communication between the Cisco UC pane in Microsoft Office Communicator and Cisco Unified Communications Integration for Microsoft Office Communicator itself. If Windows security fails, the Cisco UC pane displays the following error:

“Could not start the Cisco UC pane. A windows authentication error occurred, please contact your administrator”

Solution This failure is typically due to the inability of the client computer to connect to a domain controller. This can be caused by the following issues:

- Name resolution failure: The DNS server of the client computer is not available, or is not configured correctly, and the client computer cannot find a domain controller.

- Network connectivity failure: The client computer cannot connect to a domain controller because of a network failure or a firewall. For example, the client computer is not connected to the corporate network and the user has not established a VPN connection. In this scenario, depending on your environment, Microsoft Office Communicator might be able to connect but Cisco Unified Communications Integration for Microsoft Office Communicator cannot connect.

If the cause of failure is resolved, you must reload the Cisco UC pane to trigger it to attempt to connect to Cisco Unified Communications Integration for Microsoft Office Communicator again.

To reload the Cisco UC pane, sign out of Microsoft Office Communicator, then sign in again. Alternatively, restart Microsoft Office Communicator.

Incorrect Caller Name Displayed for Shared Lines

Problem When users are configured in Cisco Unified Communications Manager to share a line, the incorrect caller name might be displayed in notification windows or in the conversations window.

Solution This is expected behavior. In Cisco Unified Communications Manager, caller names are sent to the phones when the phones are initially configured. However, Cisco UC Integration for Microsoft Office Communicator must search for the caller name in Active Directory.

If lines are shared, when Cisco UC Integration for Microsoft Office Communicator performs a search based on the phone number, the caller name in the first set of results returned that is the closest match to the Cisco Unified Communications Manager caller name is displayed. When shared lines are not configured, there is usually only one match in Active Directory for the phone number and the caller name associated with this number is displayed.

Users with More Than One Directory Number Not Added to Conference Call

Problem When a user tries to add a participant to a conference call, the participant is not added to the conference call but remains in a normal phone call with the user who tried to add them to the conference.

Solution This issue typically occurs when participants in a conference call have shared lines configured. The issue occurs in the following circumstances:

- A participant in the conference call has more than one directory number configured in Cisco Unified Communications Manager.
- One of the directory numbers of that participant is missing from Active Directory.
- There is another participant who also has more than one directory number. This participant has the *same directory number* configured in the Active Directory that the first participant is missing from Active Directory.

Either of these participants might not be added to the conference call, but remain in a one-to-one call with the host of the conference call.

If a user has more than one directory number configured, then the corresponding Active Directory registry value must be set also. To resolve this issue, ensure that all users who have more than one directory number have all of their numbers configured in Active Directory. The field in the Active Directory to which you need to add the numbers is defined in the following registry key value name:

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

CAST Connection from IP Phone Times Out

Problem When attempting to start a CAST connection from an IP phone, the connection times out.

Solution To resolve this issue, check to ensure that:

- The IP phone is configured as an SCCP phone in Cisco Unified Communications Manager.
- The IP phone is enabled for video capabilities in Cisco Unified Communications Manager.
- The video icon is displayed in the lower right corner of the LCD screen on the IP phone.
- The client computer that is running Cisco UC Integration for Microsoft Office Communicator is tethered to the IP phone.
- Cisco Unified Video Advantage is not running. Cisco Unified Video Advantage should not be running, see [Removing Cisco Unified Video Advantage, page 4-1](#) for more information.

For more information about how to perform the checks outlined above, see [Configuring Failover to Cisco Unified Survivable Remote Site Telephony \(SRST\), page 2-18](#).

Users Lose Control of the Active Call on the Desk Phone

Problem A user can no longer control the active call on the desk phone.

Solution If a user docks, undocks, hibernates, resumes, or suspends the computer while a call is in progress on the desk phone, the call remains active, but the user cannot control the call from the computer. This is expected behavior.

Users Cannot See the Participant List for the Conference Call

Problem If users have a conference call that involves users in different clusters, some users might not be able to see the participant list for the conference call. Instead, the conference call resembles a call between two users.

Solution This is expected behavior.

Participant List for the Conference Call is Incorrect

Problem If you use Cisco Unified Communications Manager 6.1(3), in conference calls the names of the participants are incorrect in the participant list.

Solution This is expected behavior.

Numbers Published by Users in Microsoft Office Communicator Not Recognized

Problem If users use Microsoft Office Communicator to publish numbers to other Microsoft Office Communicator users, Cisco Unified Communications Integration for Microsoft Office Communicator does not recognize numbers published in this way.

Solution This is expected behavior.

Cisco UC Integration for Microsoft Office Communicator Menu Items Available but Not Functional

Problem If the Cisco UC pane is stopped, the Cisco Unified Communications Integration for Microsoft Office Communicator menu items on the Tools menu in Microsoft Office Communicator are available but are not functional.

Solution This is expected behavior.

Call Ends Unexpectedly

Problem If a user receives a call from Cisco Unified MeetingPlace, then puts the call on hold, and resumes the call several times in quick succession, the call might end.

Solution This is expected behavior in all releases of Cisco Unified MeetingPlace earlier than 8.0.

Users Can Only Control One Line on Phones Configured for Multiple Lines

Problem Cisco UC Integration for Microsoft Office Communicator can only control one call session button on a phone that is configured for multiple lines.

Solution Cisco UC Integration for Microsoft Office Communicator can control the first line in the list of lines returned by the Cisco Unified Communications Manager CTI service. You cannot change which line is controlled when the lines are partitioned. You *can* change which line is controlled by Cisco UC Integration for Microsoft Office Communicator if the lines are not partitioned, that is, they have different directory numbers.

Cannot See All Calls in Progress on Cisco Unified IP Phone 9900, 8900, and 6900 Model Series

Problem Cisco UC Integration for Microsoft Office Communicator monitors only one call session button on the desk phone that is associated with it. The Cisco Unified IP Phone 9900, 8900, and 6900 model series allow simultaneous calls on multiple call session buttons. Any call operations that happen on buttons other than the one that Cisco UC Integration for Microsoft Office Communicator monitors are not reflected in the Cisco UC Integration for Microsoft Office Communicator user interface.

If you place or answer a call on a call session button that is not the one that Cisco UC Integration for Microsoft Office Communicator monitors, the call does appear in the Cisco UC pane.

Solution You cannot use Cisco UC Integration for Microsoft Office Communicator to control calls on the buttons that Cisco UC Integration for Microsoft Office Communicator does not monitor.

The impact of JAL and DTAL operations on a call that Cisco UC Integration for Microsoft Office Communicator controls depends on whether the operation moves a call to a monitored call session button.

If a JAL operation moves a call to a monitored call session button, the call transitions to a conference call. If a JAL operation moves a call to an unmonitored button, the call disappears from the Cisco UC Integration for Microsoft Office Communicator user interface. Cisco UC Integration for Microsoft Office Communicator cannot control the call.

Similarly, a DTAL operation moves a call to a monitored call session button, Cisco UC Integration for Microsoft Office Communicator can control the call, but if the call moves to an unmonitored button, Cisco UC Integration for Microsoft Office Communicator cannot control the call.

Conversation History Events Marked as Unread

Problem When a user upgrades from Cisco UC Integration for Microsoft Office Communicator Release 7.x to Release 8.0, all events in their conversation history are marked as unread.

Solution This is expected behavior. To fix this, select all of the events in your conversation history and mark them as read.

How to Resolve Synchronization Problems

- [Users See “Cannot Synchronize...” Error Message, page 6-10](#)
- [Users See “Cannot Synchronize... Communicator 2007” Error Message, page 6-10](#)

Users See “Cannot Synchronize...” Error Message

Problem Microsoft Office Communicator users see the following error message:

“Cannot synchronize with the corporate address book because the file could not be found.”

Solution Install a security certificate for the default web site in Internet Information Services (IIS). For more information about this issue, see the following URLs:

- <http://support.microsoft.com/kb/939530>
- <http://support.microsoft.com/kb/299875>

Users See “Cannot Synchronize... Communicator 2007” Error Message

Problem Microsoft Office Communicator users see the following error message:

“You cannot synchronize the corporate address book when you use Communicator 2007 to log on to Communications Server 2007.

Cannot synchronize with the corporate address book. This may be because the proxy server setting in your web browser does not allow access to the address book. If the problem persists, contact your system administrator.”

Solution Set the correct permissions in IIS. For more information about this issue, see the following URL:

<http://support.microsoft.com/kb/953113>

Solution Ensure that the password for the RTCComponentService user account has not expired. If the password has expired, reset the password, and check **Password Never Expires**.

Solution Ensure that the security certificates are configured properly. For more information on this topic, see the following URL:

<http://www.windowsecurity.com/articles/Client-Certificate-Authentication-IIS6.html>

How to Resolve Availability Status Problems

- [“Inactive” and “Away” Availability Statuses and Custom Availability Statuses](#), page 6-11
- [“On the Phone” Availability Status Not Available in Some Locales](#), page 6-11
- [Availability Status Incorrect for Previously-Called Contacts](#), page 6-12
- [Availability Status Incorrect After a Call Ends](#), page 6-12
- [Availability Status Is Reset from “Do Not Disturb” to “Available”](#), page 6-13
- [Availability Status Does Not Return to Initial Status After Call Ends](#), page 6-13

“Inactive” and “Away” Availability Statuses and Custom Availability Statuses

Problem Users might observe some unusual availability statuses.

Solution This is expected behavior. Microsoft Office Communicator provides the availability information in Cisco UC Integration for Microsoft Office Communicator. In particular circumstances, Cisco UC Integration for Microsoft Office Communicator provides custom phone availability status information which can result in unusual availability statuses.

The following table lists the circumstances that result in these unusual availability statuses:

Initial Availability Status	Event	Availability Status Is Updated To...
Inactive	Call starts	<i>Inactive On the Phone</i>
Away	Call starts	Availability status is not updated.
Inactive On the Phone	All calls end	<i>Inactive</i> , followed by the availability status before the call started. For example, the status might be <i>Inactive Available</i> .
Away, and Cisco UC Integration for Microsoft Office Communicator automatically set the status to On the Phone	All calls end	<i>Inactive</i> , followed by the availability status before the call started. For example, the status might be <i>Inactive Available</i> .

“On the Phone” Availability Status Not Available in Some Locales

Problem Users cannot see the custom availability status “On the Phone” when they select the presence button in Microsoft Office Communicator. Other users see the availability status of this user as “Busy”. This problem occurs on computers that use the following Microsoft locales:

Language	Locale ID
Chinese (Taiwan)	1028
Spanish - Spain (Traditional Sort)	1034

This problem occurs on computers on which Microsoft Office Communicator was installed using a standalone installer for each language. In this case, the locale ID is not stored in the system registry, so Microsoft Office Communicator uses the locale ID of the computer.

Users who share the same OCS server cannot use a mixture of the locale IDs above and the following locale IDs:

Language	Locale ID
Chinese (Default Chinese-Simplified)	2052
Spanish - Modern Sort (Default Spanish)	3082

Solution You can change the locale IDs of the custom availability status file as follows:

-
- Step 1** Search the uc-client log files on the computer for the following string:
CurrentCulture LCID
The locale ID that the computer is using is in brackets ([]) after the string.
- Step 2** Locate the cisco-presence-states-config.xml file in the installation folder, then open the file.
- Step 3** If the current locale ID identified in [Step 1](#) is 1028, change the value of the LCID attribute of the <activity> element in cisco-presence-states-config.xml from 2052 to 1028.
If the current locale ID is 1034, change the value of the LCID attribute from 3082 to 1034.
- Step 4** Ask the user to sign out of Microsoft Office Communicator, then sign in again.
-

Related Topics

- [How to Resolve General Problems with the Integration, page 6-3](#)

Availability Status Incorrect for Previously-Called Contacts

Problem If you have previously called a contact, their availability status appears as “Unknown” in the conversation history window and Select Contacts dialog box.

Solution This problem occurs because the contact has been cached. If your system does not use +E.164 number formatting, enable wildcard searches.

For more information about how to enable wildcard searches, see [Configuring Value Names for the Client Services Framework Client Integration, page 3-2](#).

Availability Status Incorrect After a Call Ends

Problem After a user ends a call, the availability status displayed for the user is inaccurate. For example, the availability status might be “Busy” after the user ends the call.

Solution If users select in Microsoft Office Communicator to update the availability status from the Outlook calendar information, the availability status can be inaccurate. Users need to reset the availability status after they end a call.

Availability Status Is Reset from “Do Not Disturb” to “Available”

Problem If Cisco Unified Presence is deployed in your Cisco Unified Communications system, your phone application might reset the availability status of your phone from Do Not Disturb to Available.

Solution This can occur on the following events:

- You are using your computer for phone calls, and use the Cisco UC pane to switch to use your desk phone for phone calls.
- You are using your desk phone for phone calls, and use the Cisco UC pane to switch to use your computer for phone calls.
- You exit Cisco UC Integration for Microsoft Office Communicator Cisco UC Integration for Microsoft Office Communicator, that is, you sign out of the Cisco UC pane.

For example, if you set your availability status to Do Not Disturb, sign out of Microsoft Office Communicator, then sign in again, the availability status of your phone is reset automatically to Available.

Availability Status Does Not Return to Initial Status After Call Ends

Problem The availability status does not always return to the initial availability status after a call ends.

Solution Microsoft Office Communicator provides the availability information in Cisco UC Integration for Microsoft Office Communicator. Cisco UC Integration for Microsoft Office Communicator updates the availability status of users after calls start and end as shown in the following table:

Initial Status	Status After Call Starts	Status When All Calls End
Busy	On the Phone	Available
In a Meeting	On the Phone	In a Meeting, if the meeting is still in progress. Otherwise, the status is Available.

How to Resolve Click to Call Problems

- [Users Cannot See “Call” or “Call with Edit” in Microsoft Excel 2003 or Word 2003, page 6-14](#)
- [Users Cannot See “Call” or “Call with Edit” in Microsoft Word 2003 or Word 2007, page 6-14](#)
- [Users Cannot See “Call” or “Call with Edit” in Microsoft Excel, Outlook, PowerPoint, or Word, page 6-15](#)
- [Users Cannot See “Additional Actions” Menu in Microsoft Outlook Contacts, page 6-15](#)

Users Cannot See “Call” or “Call with Edit” in Microsoft Excel 2003 or Word 2003

Problem After you perform a complete installation of Cisco UC Integration for Microsoft Office Communicator, the “Call” and “Call with Edit” menu items for the click-to-call feature do not appear in Microsoft Excel 2003 or Word 2003.

Solution The DLL file mscoree.dll has been disabled. To enable mscoree.dll, perform the following steps:

-
- Step 1** Select **Help > About Microsoft <application>** in the application where the problem occurs.
 - Step 2** Select **Disabled Items**.
 - Step 3** Select mscoree.dll.
 - Step 4** Select **Enable**.
 - Step 5** Close the application, then open the application again.
-

Users Cannot See “Call” or “Call with Edit” in Microsoft Word 2003 or Word 2007

Problem The “Call” and “Call with Edit” menu items for the click-to-call feature do not appear, or several instances appear in Word 2003 or Word 2007. The menu items appear correctly in Excel 2003 or Excel 2007.

Solution Replace your normal template file as follows:

-
- Step 1** Close Word.
 - Step 2** Delete the Word normal template file as indicated in the following table:

Version	Filename	File Location
Word 2003	Normal.dot	<drive>:\Documents and Settings\<username>\Application Data\Microsoft\Templates
Word 2007	Normal.dotm	<drive>:\Documents and Settings\<username>\Application Data\Microsoft\Templates

- Step 3** Open Word.
The normal template file is recreated automatically.
-

Related Topics

- [How to Resolve General Problems with the Integration, page 6-3](#)

Users Cannot See “Call” or “Call with Edit” in Microsoft Excel, Outlook, PowerPoint, or Word

Problem The “Call” and “Call with Edit” menu items for the click-to-call feature do not appear in Microsoft Excel, Outlook, PowerPoint, or Word. This problem can occur in either 2003 or 2007 versions of these applications.

Solution Set the value of LoadBehavior to 3 in the appropriate registry key as shown in the following table, then restart the application.

Application	Architecture	Registry Key
Excel 2003 or 2007	32-bit	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Excel\Addins\CiscoClickToCall.Connect
	64-bit	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\Excel\Addins\CiscoClickToCall.Connect
Outlook 2003 or 2007	32-bit	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Outlook\Addins\CiscoClickToCallContacts.Connect
	64-bit	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\Outlook\Addins\CiscoClickToCallContacts.Connect
PowerPoint 2003	32-bit	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\PowerPoint\Addins\CiscoClickToCall.Connect
	64-bit	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\PowerPoint\Addins\CiscoClickToCall.Connect
Word 2003 or 2007	32-bit	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Word\Addins\CiscoClickToCall.Connect
	64-bit	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\Word\Addins\CiscoClickToCall.Connect

Users Cannot See “Additional Actions” Menu in Microsoft Outlook Contacts

Problem When users right-click on a contact in the Microsoft Outlook Contacts folder, the Additional Actions menu is not displayed.

Solution Restart Outlook as follows:

Procedure

-
- Step 1** Close Outlook.
- Step 2** Start the Task Manager.
- Step 3** End the Outlook process.
The name of the Outlook process is OUTLOOK.EXE or OUTLOOK*32.EXE.
- Step 4** Restart Outlook.
-

How to Resolve Instant Message Window Problems

- [Instant Message Window Closes When You Try to Call a Contact Who Has No Number in LDAP, page 6-16](#)
- [Instant Message Window Displayed When Users Select the Place a Call Menu Item, page 6-16](#)
- [Meeting URL Displayed in the Instant Message Window Does Not Work, page 6-16](#)

Instant Message Window Closes When You Try to Call a Contact Who Has No Number in LDAP

Problem The instant message window closes automatically when you do the following:

1. Open instant message window with a contact who has no number in LDAP.
2. Do not type any text in the window.
3. Right-click the contact, then select **Place a Call**.

Solution This is expected behavior.

Instant Message Window Displayed When Users Select the Place a Call Menu Item

Problem When users right-click on a contact in the Microsoft Office Communicator Contact List, Instant Message Window, or Search Box, then select **Place a Call**, an instant message window is displayed briefly.

Solution This is expected behavior.

Meeting URL Displayed in the Instant Message Window Does Not Work

Problem When users are invited to a meeting, they receive an instant message in Microsoft Office Communicator with a URL to join the meeting. If the meeting URL contains an underscore character (_) at the start of the URL, the URL does not work.

Solution This is expected behavior if the OCS server is configured to enable the security setting where all URLs are preceded by an underscore (_) character.

How to Resolve Voicemail Problems

- Deleted Voice Messages Might Appear as Not Deleted, page 6-17

Deleted Voice Messages Might Appear as Not Deleted

Problem If the voicemail system uses Cisco Unity with Microsoft Exchange 2007, when users delete voice messages using Cisco UC Integration for Microsoft Office Communicator, the deleted messages are not moved to the Deleted Items folder in the Exchange mailbox. In this situation, when a user views the Exchange mailbox using a client such as Outlook or Thunderbird, the deleted messages are shown in the Inbox, sometimes with a strikethrough to indicate that the messages are deleted. When a user accesses the voicemail Inbox using the Cisco Unity Telephone User Interface (TUI), the deleted messages appear as saved messages.

Solution This is expected behavior. Microsoft Exchange 2007 does not support the IMAP UIDPLUS extensions that Cisco Unified Client Services Framework relies on.

How to Resolve Video Problems

- Users Cannot Use Video Features on Their Computers When They Use Their Desk Phone, page 6-17
- Users Cannot See Video in Ad-Hoc Conference Calls, page 6-18

For more information about video problems, see the release notes for the product at the following URL:
http://www.cisco.com/en/US/products/ps10317/prod_release_notes_list.html

Users Cannot Use Video Features on Their Computers When They Use Their Desk Phone

Problem When users have selected to use their desk phone for phone calls, they might not be able to use video on their calls, even when the phone is configured for video. A warning icon appears in the status bar on the Cisco UC pane. If a user selects the Menu button from the Microsoft Office Communicator title bar, then selects **Tools > Server Status and Notifications**, the following error is displayed in the Server Status tab as the value of the Status field in the Desk Phone (CAST) entry:

“CSF can't detect phone - no phone attached.”

Solution To resolve this problem, check the following, in the order shown below:

1. The camera or built-in camera is functioning correctly. Check that the camera is attached correctly to the computer.
2. The computer is tethered to the desk phone.
3. The desk phone is running SCCP firmware. SIP firmware does not support video when Cisco UC Integration for Microsoft Office Communicator is set to use the desk phone for phone calls.
4. In Cisco Unified Communications Manager Administration, ensure that the Video Capabilities option is set to Enabled for the desk phone.

5. Symantec Endpoint Protection might be blocking the addresses used by Cisco Discovery Protocol (CDP). To resolve this problem, create a rule in Symantec Network Threat Protection (NTP) to allow the following MAC addresses:

01-00-0c-cc-cc-cc

01-00-0c-cc-cc-cd

For more information about how to create this rule, see the following URL:

<http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2008062616331948>

Users Cannot See Video in Ad-Hoc Conference Calls

Problem Users cannot see video in an ad-hoc conference call.

Solution This could be as a result of the Minimum Video Capable Participants To Allocate Video Conference setting in Cisco Unified Communications Manager.

Related Topics

- [\(Optional\) Specifying a Minimum Number of Video-Capable Participants for Ad-Hoc Conferences, page 2-15](#)

How to Resolve Camera Problems


- [Camera Troubleshooting Tips, page 6-18](#)
- [Some Cameras Zoom In Suddenly During a Call, page 6-18](#)

For more information about video problems, see the release notes for the product at the following URL:

http://www.cisco.com/en/US/products/ps10317/prod_release_notes_list.html

Camera Troubleshooting Tips

The following are some general tips to avoid camera issues:

- Ensure that you installed the correct driver for the camera that you use.
- To configure the camera that you want to use with Cisco UC Integration for Microsoft Office Communicator, select  in the Microsoft Office Communicator title bar, then select **Tools > Set Up Audio and Video**. The tool allows you to preview the video output from the camera. You can use the Webcam Settings to change the video properties, such as, brightness and contrast.

Some Cameras Zoom In Suddenly During a Call

Problem During a call, the camera sometimes zooms in suddenly. This problem may occur on cameras that support the autofocus feature, as the camera tries to regain focus of the image.

Solution Place the call on hold and resume the call to see if the image is restored correctly.

How to Resolve LDAP Problems

- [How Do I Determine Which LDAP Server OCS Is Using?](#), page 6-19
- ["Host/Network reports server unavailable"](#), page 6-19

How Do I Determine Which LDAP Server OCS Is Using?

Problem I do not know which Lightweight Directory Access Protocol (LDAP) server the Office Communications Server (OCS) is using.

Solution To resolve this issue, perform the following steps:

1. Log in to the OCS 2007 R2.
2. Select **Start > Administrative Tools > Active Directory Sites and Services**.
3. Browse to Sites.
4. Select the site name.
5. Select **Servers**. The name of the LDAP Server is listed as a node.

"Host/Network reports server unavailable"

Problem The Server Status tab in Cisco UC Integration for Microsoft Office Communicator displays the following error in the Status field of the LDAP section:

"Host/network reports server unavailable"

Solution Check the values of the following Client Services Framework registry keys:

- LDAP_UserLogonDomain
- LDAP_SearchBaseDN_1, LDAP_SearchBaseDN_2, LDAP_SearchBaseDN_3, LDAP_SearchBaseDN_4, and LDAP_SearchBaseDN_5

For more information about the correct values for these registry keys, see [Specifying LDAP Value Names](#), page 3-7.

"The server has rejected the provided credentials"

Problem The Server Status tab in Cisco UC Integration for Microsoft Office Communicator displays the following error in the Status field of the LDAP section:

"The server has rejected the provided credentials"

Solution Check the following:

- The value of the Client Services Framework registry key LDAP_UserLogonDomain.
- The values of the Client Services Framework registry keys LDAP_SearchBaseDN_1, LDAP_SearchBaseDN_2, LDAP_SearchBaseDN_3, LDAP_SearchBaseDN_4, and LDAP_SearchBaseDN_5.
- The values of the LDAP_AttributeName_* registry keys. These values should be set to the corresponding values on the LDAP server.

- The credentials entered for the Corporate directory in the Accounts section of the Cisco UC options dialog box in Cisco UC Integration for Microsoft Office Communicator.

For more information about the correct values for these registry keys, see [Specifying LDAP Value Names](#), page 3-7.



APPENDIX **A**

Normalization Rules for OCS

Revised: July 7, 2011

If you do not define phone numbers in +E.164 format for each user in your Active Directory, you must perform other actions to ensure that the numbers in your Active Directory are processed into the Office Communications Server (OCS) address book in a form that Cisco Unified Communications Manager dialing rules can process to dial a number.

If all the numbers in your Active Directory are in +E.164 format, you do not need to configure OCS normalization rules. This is the easiest way to deploy Cisco UC Integration for Microsoft Office Communicator.

If the numbers in your Active Directory are not in +E.164 format, then you must configure OCS normalization rules to ensure that Microsoft Office Communicator downloads +E.164-formatted numbers from OCS.

This is necessary because OCS requires +E.164-formatted numbers, unless you configure normalization rules. For information about this topic, see the following URL:

<http://technet.microsoft.com/en-us/library/bb964002.aspx>



Note

Configuring OCS normalization rules can be an error-prone task, especially for international and enterprise dial plans.

Related Topics

- [Dial Plan Options for Cisco UC Integration for Microsoft Office Communicator, page 2-4](#)
- [Dialing Rules Required for Cisco UC Integration for Microsoft Office Communicator, page 2-5](#)



APPENDIX **B**

Enabling Display of Photos in Notification Windows, the Conversations Window, and Contact Cards

Revised: July 7, 2011

- [Adding the Active Directory Schema Snap-In, page B-1](#)
- [Creating the photoUri Attribute, page B-2](#)
- [Setting a Default Value for the photoUri Attribute Using ADSI Edit, page B-2](#)
- [Configuring IIS to Display Photos, page B-4](#)
- [Verifying the User Object, page B-4](#)

Adding the Active Directory Schema Snap-In

Procedure

- Step 1** Execute the following command:
`regsvr32 schmmgmt.dll`
- Step 2** Execute the following command to start Microsoft Management Console:
`mmc`
- Step 3** In Microsoft Management Console, select **File > Add/Remove Snap-in**.
- Step 4** Select **Active Directory Schema**, then select **Add**.
- Step 5** Select **Close** on the Add Standalone Snap-in dialog box, then select **OK** on the Add/Remove Snap-in dialog box.
-

What to Do Next

- [Creating the photoUri Attribute, page B-2](#)

Creating the photoUri Attribute

Procedure

- Step 1** Start the Active Directory Schema administrative tool.
- Step 2** Right-click the **Attribute** container, then select **New > Attribute** from the pop-up menu.
- Step 3** To create the photoUri attribute, complete the fields on the properties dialog box as follows:

Field	Description
Description	Enter "photoUri".
Common Name	Enter "photoUri".
X500 OID	Enter the object ID.
Syntax	Enter "Case Insensitive String".
Allow this attribute to be shown in advanced view	Select this option.
Attribute is active	Select this option.
Attribute is copied when duplicating a user	Select this option.

- Step 4** Select **OK**.
- Step 5** Open the **Classes** container in the Active Directory Schema administrative tool, right-click **user**, then select **Properties** from the pop-up menu.
- Step 6** Select **Attributes**, then select **Add**.
- Step 7** Select **photoUri** from the list on the Select Schema Object dialog box, then select **OK**.

What to Do Next

- [Setting a Default Value for the photoUri Attribute Using ADSI Edit, page B-2](#)

Setting a Default Value for the photoUri Attribute Using ADSI Edit

Before You Begin

If you cannot run the ADSI Edit application, you must enable the ADSI Edit application before you perform this procedure.

Procedure

- Step 1** Execute the following command to start the Active Directory Service Interface (ADSI) editor:
adsiedit.msc
- Step 2** Open the organizational unit (OU) you require, right-click the user you require, then select **Properties**.

- Step 3** Select the **photoUri** attribute, then select **Edit**.
- Step 4** Enter the URL for the photo for the user in the Value field. For example, enter a URL similar to the following:

http://www.example.com/photos/mweinstein.jpg



Note If you plan to use a script to populate the default value, enter a space character in the Value field. You cannot run a script if there is no default value.

- Step 5** Select **OK**.
- Step 6** After you configure IIS to display photos, you can verify that you can view the photo by accessing the URL you entered.
-

Related Topics

- [Enabling the ADSI Edit Application, page B-3](#)
- [Configuring IIS to Display Photos, page B-4](#)

Enabling the ADSI Edit Application

If you cannot run the ADSI Edit application, you must perform the following procedure.

Procedure

- Step 1** Execute the following command:
- ```
regsvr32 adsiedit.dll
```
- Step 2** Execute the following command to start the ADSI editor:
- ```
adsiedit.msc
```
- Step 3** If the application still does not start, obtain the adsiedit.dll file, then run the command in Step 1 from the folder where the adsiedit.dll file is located.
-

Related Topics

- [Setting a Default Value for the photoUri Attribute Using ADSI Edit, page B-2](#)

What to Do Next

- [Configuring IIS to Display Photos, page B-4](#)

Configuring IIS to Display Photos

Procedure

- Step 1** Start Internet Information Services Manager.
- Step 2** Select the computer name in the left pane, then select **Web Sites**.
- Step 3** Right-click **Default Web Site**, then select **New > Virtual Directory**.
- Step 4** Follow the instructions in the wizard to create the virtual directory, and enter the local folder where the photos are located. You can now access the photos from the URL structured as follows:

`http://<domain-name>/<virtual-directory>/<photo-filename>`

For example, you can access a photo with a URL similar to the following:

`http://www.example.com/photos/mweinstein.jpg`

What to Do Next

- [Verifying the User Object, page B-4](#)

Verifying the User Object

Procedure

- Step 1** Execute the following command:
- ldp**
- Step 2** Select **Connection > Connect**, then select **OK**.
- Step 3** Select **Connection > Bind**, enter your username and password, then select **OK**.
- Step 4** Select **View > Tree**, select the BaseDN, then select **OK**.
- Step 5** Open the BaseDN node, then double-click on the user you require.
- Step 6** Verify that the photo information is present for the user.
-