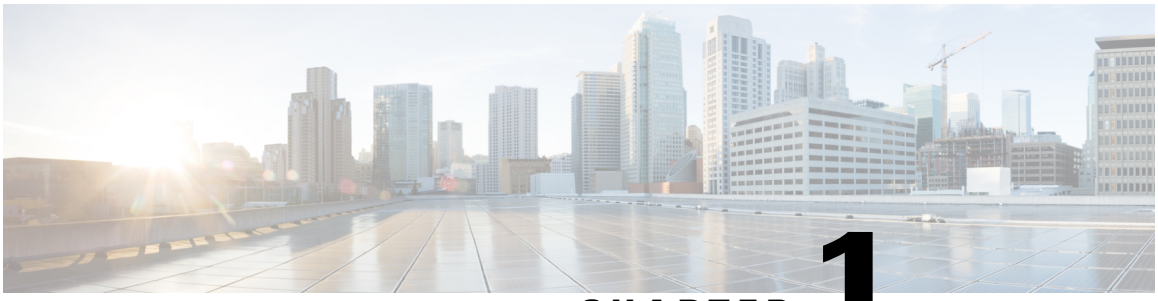
Administration Guide for Cisco UC Integration for Microsoft Lync Release 9.2(1)

First Published: May 28, 2013

Last Modified: June 12, 2013

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

CONTENTS



CHAPTER 1

Introduction

Important **This document is a draft that may include information on functionality not yet part of the client or be missing information that will be included in future updates. Please direct any documentation feedback to the Community forums.**

This section provides an introduction to Cisco UC Integration for Microsoft Lync.

Cisco UC Integration for Microsoft Lync

Cisco UC Integration for Microsoft Lync is a Microsoft Windows desktop application that provides access to Cisco Unified Communications from Microsoft Lync. The solution extends the presence and instant messaging capabilities of Microsoft Lync by providing access to a broad set of Cisco Unified Communications capabilities; including software phone standards-based video, unified messaging, conferencing, desktop phone control and phone presence.

Key features of Cisco UC Integration for Microsoft Lync include:

- Make and receive video calls using the Cisco Precision Video engine.
- Make and receive phone calls through Cisco Unified Communications Manager.
- Drag and drop and right-click integration with the Microsoft Lync contact list.
- Instant Messaging and Presence integration with Microsoft Lync.
- Mute, hold, and transfer during calls.
- Software phone or desktop phone mode selection.
- Communications history of missed, placed, and received calls.
- Audio and visual notification of incoming calls.

- Ad hoc conferencing.
- Visual voicemail.
- Click to Call from the Microsoft Outlook and Excel Ribbon and Internet Explorer.

Documentation Resources

About This Document

The guide provides information to help you complete the following tasks:

- Plan a successful deployment.
- Set up your deployment environment.
- Configure and deploy the application.
- Review supported environments and software.
- Review audio, video, and network requirements.

Additional Documentation

See the Cisco UC Integration for Microsoft Lync documentation and support site for additional resources. This site can be accessed at: http://www.cisco.com/en/US/products/ps11390/tsd_products_support_series_home.html. Documentation and resources for the Cisco Virtualization Experience Media Engine can be accessed at: http://www.cisco.com/en/US/products/ps12862/tsd_products_support_series_home.html.

Community Resources

Cisco provides different community resources where you can engage with support representatives or join other community members in product discussions.

Cisco product conversation and sharing site

Join other community members in discussing features, functions, licensing, integration, architecture, challenges, and more. Share useful product resources and best practices.
https://communities.cisco.com/community/technology/collaboration/product

Cisco support community

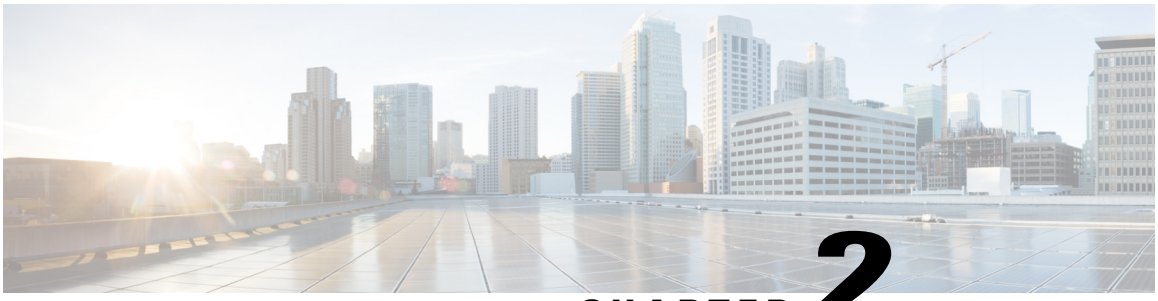
Visit the Cisco support community for IT installation, implementation, and administrative questions.
https://supportforums.cisco.com/community/netpro/collaboration-voice-video

Cisco support and downloads

Find a wealth of product support resources, download application software, and find bugs based on product and version.
http://www.cisco.com/cisco/web/support/index.html

Cisco expert corner

Engage, collaborate, create, and share with Cisco experts. The Cisco expert corner is a collection of resources that various experts contribute to the community, including videos, blogs, documents, and webcasts.
https://supportforums.cisco.com/community/netpro/expert-corner#view=ask-the-experts



CHAPTER 2

Deployment Architecture Overview

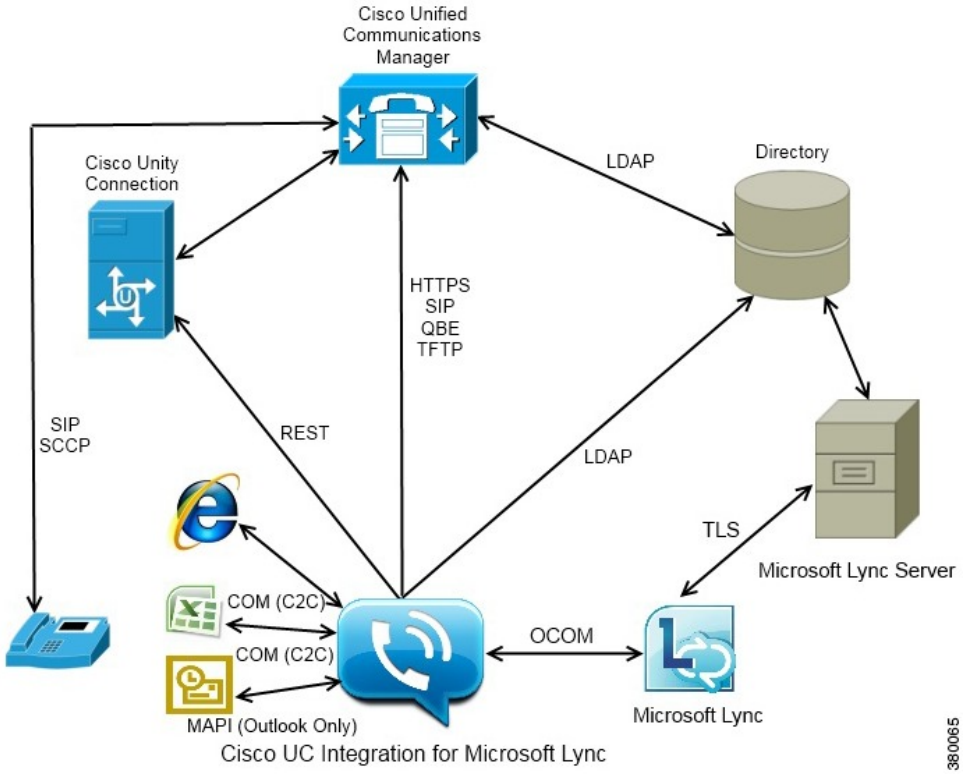
This section contains information on the Cisco UC Integration for Microsoft Lync deployment architecture.

Deployment Architecture

This section describes the Cisco UC Integration for Microsoft Lync deployment architecture.

Deployment Diagram

The following diagram illustrates the architecture of a typical Cisco UC Integration for Microsoft Lync deployment.



Deployment Components

The following list describes the components of a typical deployment:

Desk phone

Connects to Cisco Unified Communications Manager for signaling and configuration.

Cisco Unity Connection

Provides voicemail capabilities.

Cisco Unified Communications Manager

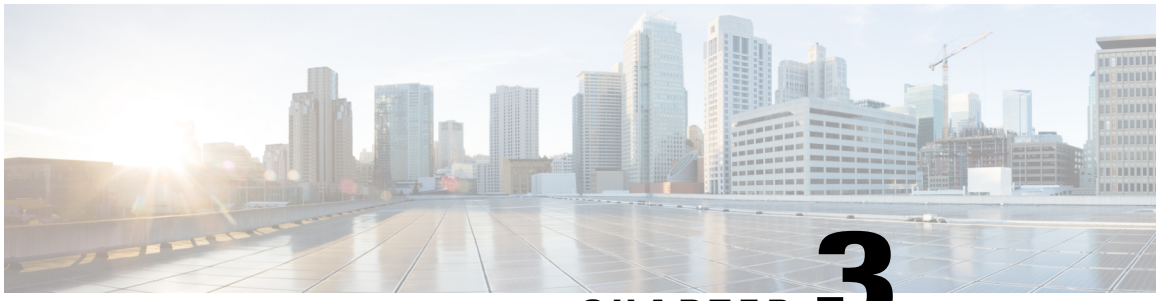
- Provides audio and video call management capabilities.
- Provides user and device configuration settings.
- Connects to the directory for user synchronization and user authentication.

Directory

One of the following types of directory:

- Microsoft Active Directory
- LDAP directory

As an alternative to a standalone directory, you can use Cisco Unified Communications Manager User Data Service as your directory source after you synchronize your directory to Cisco Unified Communications Manager.



CHAPTER 3

Planning

This section provides information on planning for a deployment.

Hardware Requirements

Installed RAM

1.87 GB RAM on Microsoft Windows XP 32 bit with Service Pack 3
2 GB RAM on Microsoft Windows 7

Free physical memory

128 MB

Free disk space

256 MB

CPU speed and type

Mobile AMD Sempron Processor 3600+ 2 GHz
Intel Core2 CPU T7400 @ 2. 16 GHz

GPU

Directx 9 on Microsoft Windows XP 32 bit with Service Pack 3
Directx 11 on Microsoft Windows 7

I/O ports

USB 2.0 for USB camera and audio devices.

Software Requirements

Supported Microsoft Lync versions

- Microsoft Lync 2010
- Microsoft Lync 2013

  Microsoft Lync 2013 is supported with the following caveats at this time:

  - Drag and drop from the Microsoft Lync contact list is not supported.
  - Click to Call from Microsoft Office 2013 is not supported.
  - Escalation from a Microsoft Lync group chat session to a voice or video call is not supported.
  - Microsoft Lync 2013 update KB2760512 must be installed.

Note Microsoft Lync 2013 64 bit is not supported.

Supported operating systems

- Microsoft Windows 7 32 bit
- Microsoft Windows 7 64 bit
- Microsoft Windows XP 32 bit with Service Pack 3

Supported servers

- Cisco Unified Communications Manager version 7.1(4) or later
- Cisco Unity Connection version 8.5 or later

Supported directories

- Microsoft Active Directory 2003
- Microsoft Active Directory 2008
- Cisco Unified Communications Manager User Data Service

  UDS is supported on Cisco Unified Communications Manager version 8.6.2 or later.
- OpenLDAP

Restriction Directory integration with OpenLDAP requires you to define specific parameters in a Cisco UC Integration for Microsoft Lync configuration file. See *LDAP Directory Servers* for more information.

Microsoft Internet Explorer

Cisco UC Integration for Microsoft Lync requires Microsoft Internet Explorer 7.0, 8.0, or 9.0. The application uses the Microsoft Internet Explorer rendering engine to display HTML content.

Support for Microsoft Office (Click to Call)

- Microsoft Office 2007 32 bit
- Microsoft Office 2010 32 bit

Note Microsoft Lync 2013 is installed with Microsoft Office 2013 but Click to Call is not supported.

Network Requirements

ICMP requests

Cisco UC Integration for Microsoft Lync sends Internet Control Message Protocol (ICMP) requests to the TFTP server. These requests enable the client to determine if it can connect to Cisco Unified Communications Manager. You must configure firewall settings to allow ICMP requests from the client. If your firewall does not allow ICMP requests, the application cannot establish a connection to Cisco Unified Communications Manager.

Ports and protocols

Cisco UC Integration for Microsoft Lync uses the ports and protocols listed in the following table. If you plan to deploy a firewall between the application and a server, configure the firewall to allow these ports and protocols.

Port	Protocol	Description
Inbound		

Port	Protocol	Description
16384 to 32766	UDP	Receives Real-Time Transport Protocol (RTP) media streams for audio and video. You set these ports in Cisco Unified Communications Manager.
Outbound		
69	UDP	Trivial File Transfer Protocol (TFTP) service
6970	HTTP	TFTP service to download client configuration
443	TCP (HTTPS)	Cisco Unity Connection for voicemail
7080	TCP (HTTPS)	Cisco Unity Connection for notifications of voice messages
389	UDP / TCP	LDAP directory server
636	LDAPS	LDAP directory server (secure)
3268	TCP	Global Catalog server
3269	LDAPS	Global Catalog server (secure)
2748	TCP	CTI gateway
5060	UDP / TCP	Session Initiation Protocol (SIP) call signaling
5061	TCP	Secure SIP call signaling
8443	HTTPS	Web access to Cisco Unified Communications Manager and includes connections for the following: • Cisco Unified Communications Manager IP Phone (CCMCIP) server for assigned devices. • User Data Service (UDS)
16384 to 32766	UDP	RTP media streams for audio and video
53	UDP / TCP	Domain Name System (DNS) traffic
3804	TCP	Locally Significant Certificates (LSC) for IP phones This is the listening port for Cisco Unified Communications Manager Certificate Authority Proxy Function (CAPF) enrollment.

Supported Codecs

Supported Audio Codecs

- g.722.1
  - g.722.1 32k
  - g.722.1 24k

Note g.722.1 is supported on Cisco Unified Communications Manager 8.6.1 or later.

- g.711
  - g.711 A-law
  - g.711 u-law
- g.729a

Supported Video Codecs

- H.264/AVC

Phones, headsets, and cameras

CTI supported devices

Cisco UC Integration for Microsoft Lync supports the same CTI devices as Cisco Unified Communications Manager version 8.6(1). See the *CTI supported device matrix* table in the *CTI Supported Devices* topic at the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/tapi_dev/8_6_1/supporteddevices.html

Headsets and speakers

Plantronics Blackwire C420	Plantronics Voyager Pro UC B230
Plantronics Blackwire C610	Plantronics Voyager Pro UC BT300
Plantronics Blackwire C620	Jabra BIZ 2400
Plantronics C220UC	Jabra BIZ 620
Plantronics C420	Jabra Go 6470
Plantronics Calisto P420	Jabra PRO 930
Plantronics Calisto P800 series headset	Jabra Speak 410

Plantronics DSP400	Jabra-8120
Plantronics W740	Jabra GN2000
Plantronics WO200/A	Jabra PRO 9470
Plantronics WO300	Polycom CX100 Speakerphone
Plantronics Voyager Pro UC WG200/B	-

Plantronics Blackwire C310	Plantronics Voyager 510SL
Plantronics Blackwire C320	Plantronics Voyager Pro UC B230
Plantronics Blackwire C420	Plantronics DSP 400
Plantronics Blackwire C435	Plantronics Savi 740
Plantronics Blackwire C610	Plantronics Savi 440
Plantronics Blackwire C620	Jabra GN2000 CIPC Mono
Plantronics Blackwire C710	Jabra GN2000 CIPC Duo
Plantronics Blackwire C720	Jabra Go 6470
Plantronics Calisto P240 series	Jabra Pro 930
Plantronics Calisto P420	Jabra Speak 410
Plantronics Calisto P610 series	Jabra BIZ 2400
Plantronics Calisto P800 series	Polycom CX100 Speakerphone
Plantronics Voyager Pro UC WG200/B	-

Cameras

Microsoft LifeCam 6000	Tandberg Precision HD devices
Logitech Pro 9000	Cisco VTIII, resolution up to VGA
Logitech C920	-

Cisco AnyConnect

Cisco AnyConnect refers to a server-client infrastructure that enables the application to connect securely to your corporate network from remote locations such as Wi-Fi or mobile data networks.

The Cisco AnyConnect environment includes the following components:

Cisco Adaptive Security Appliance (ASA)

Provides a service to secure remote access.

Cisco AnyConnect Secure Mobility Client

Establishes an secure connection to Cisco Adaptive Security Appliance from the user's computer.

Cisco UC Integration for Microsoft Lync supports secure remote access with the following:

- Cisco AnyConnect Secure Mobility Client 2.5
- Cisco AnyConnect Secure Mobility Client 3.1

See the Cisco AnyConnect documentation for information and procedures on the configuration of this infrastructure. It is located here: http://www.cisco.com/en/US/products/ps10884/tsd_products_support_series_home.html.

Audio and Video Performance Reference

Attention The following data is based on testing in a lab environment. This data is intended to provide an idea of what you can expect in terms of bandwidth usage. The content in this topic is not intended to be exhaustive or to reflect all media scenarios that might affect bandwidth usage.

Bit Rates for Audio, Video, and Presentation Video

The following table describes bit rates for audio:

Codec	RTP payload in kilobits (kbits) per second	Actual bitrate (kbits per second)	Notes
g.722.1	24/32	54/62	High quality compressed
g.711	64	80	Standard uncompressed
g.729a	8	38	Low quality compressed

Bit Rates for Video

The following table describes bit rates for video with `g.711` audio:

Resolution	Pixels	Measured bit rate (kbits per second) with g.711 audio
w144p	256 x 144	156
w288p This is the default size of the video rendering window.	512 x 288	320
w448p	768 x 448	570
w576p	1024 x 576	890
720p	1280 x 720	1300

Notes about the preceding table:

- This table does not list all possible resolutions.
- The measured bit rate is the actual bandwidth used (RTP payload + IP packet overhead).

Bit Rates for Presentation Video

The following table describes the bit rates for presentation video:

Pixels	Estimated wire bit rate at 2 fps (kbits per second)	Estimated wire bit rate at 8 fps (kbits per second)
720 x 480	41	164
704 x 576	47	188
1024 x 768	80	320
1280 x 720	91	364
1280 x 800	100	400

Notes about the preceding table:

- The application captures at 8 fps and transmits at 2 to 8 fps.
- The values in this table do not include audio.

Maximum Negotiated Bit Rate

You specify the maximum payload bit rate in Cisco Unified Communications Manager in the **Region Configuration** window. This maximum payload bit rate does not include packet overhead, so the actual bit rate used is higher than the maximum payload bit rate you specify.

The following table describes how the application allocates the maximum payload bit rate:

Desktop sharing session	Audio	Interactive video (Main video)	Presentation video (Desktop sharing video)
No	The application uses the maximum audio bit rate	The application allocates the remaining bit rate as follows: The maximum video call bit rate minus the audio bit rate.	-
Yes	The application uses the maximum audio bit rate	The application allocates half of the remaining bandwidth after subtracting the audio bit rate.	The application allocates half of the remaining bandwidth after subtracting the audio bit rate.

Performance Expectations for Bandwidth

The application separates the bit rate for audio and then divides the remaining bandwidth equally between interactive video and presentation video. The following table provides information to help you understand what performance you should be able to achieve per bandwidth:

Upload speed	Audio	Audio + Interactive video (Main video)	Audio + Presentation video (Desktop sharing video)	Audio + Interactive video + Presentation video
125 kbps under VPN	At bandwidth threshold for g.711. Sufficient bandwidth for g.729a and g.722.1.	Insufficient bandwidth for video.	Insufficient bandwidth for video.	Insufficient bandwidth for video.
384 kbps under VPN	Sufficient bandwidth for any audio codec.	w288p (512 x 288) at 30 fps	1280 x 800 at 2+ fps	w144p (256 x 144) at 30 fps + 1280 x 720 at 2+ fps
384 kbps in an enterprise network	Sufficient bandwidth for any audio codec.	w288p (512 x 288) at 30 fps	1280 x 800 at 2+ fps	w144p (256 x 144) at 30 fps + 1280 x 800 at 2+ fps
1000 kbps	Sufficient bandwidth for any audio codec.	w576p (1024 x 576) at 30 fps	1280 x 800 at 8 fps	w288p (512 x 288) at 30 fps + 1280 x 800 at 8 fps
2000 kbps	Sufficient bandwidth for any audio codec.	w720p30 (1280 x 720) at 30 fps	1280 x 800 at 8 fps	w288p (1024 x 576) at 30 fps + 1280 x 800 at 8 fps

Note that VPN increases the size of the payload, which increases the bandwidth consumption.

Video Rate Adaptation

The application uses video rate adaptation to negotiate optimum video quality. Video rate adaptation dynamically increases or decreases video bit rate throughput to handle real-time variations on available IP path bandwidth.

Users should expect video calls to begin at lower resolution and scale upwards to higher resolution over a short period of time. The application saves history so that subsequent video calls should begin at the optimal resolution.

Cisco Options Package Files

Review the different Cisco Options Package (COP) files that you might require to deploy the application.

COP File	Description	Cisco Unified Communications Manager Versions
ciscocm.installcsfdevicetype.cop.sgn	Adds the CSF device type to Cisco Unified Communications Manager. For more information, see *Software Requirements*.	7.1.3
cmterm-bfcp-e.8-6-2.cop.sgn	Enables CSF devices to support BFCP video desktop sharing. For more information, see *Apply COP File for BFCP Capabilities*.	8.6.2 only
ciscocm.addcsfsupportfield.cop.sgn	Adds the **CSF Support Field** field for group configuration files. For more information, see *Create Group Configurations*.	8.6.x and lower
cmterm-cupc-dialrule-wizard-0.1.cop.sgn	Publishes application dial rules and directory lookup rules to Cisco UC Integration for Microsoft Lync. For more information, see *Publish Dial Rules*.	All supported versions

Directory Integration

Deployment of the application requires directory integration. Two types of directory integration are supported:

- Enhanced Directory Integration (EDI)
- Cisco Unified Communications Manager User Data Service (UDS)

EDI Directory Integration

Enhanced Directory Integration (EDI) uses native Microsoft Windows APIs to retrieve contact data from Microsoft Active Directory.

EDI Configuration

Cisco UC Integration for Microsoft Lync will automatically discover the directory service and connect to a Global Catalog if it has been installed on a workstation that is registered to an Active Directory domain. This connection can be customized in the configuration file as follows:

- Attribute mappings

  See *Attribute Mapping Parameters*.

- Connection settings

  See *Directory Connection Parameters*.

- Query settings

See *Directory Query Parameters*.

- Contact photo resolution

  See *Contact Photo Parameters*.

- Contact resolution

  See *Contact Resolution*.

Retrieving Attributes from the Directory

Cisco UC Integration for Microsoft Lync can connect to a Global Catalog or Domain Controller to retrieve Active Directory attributes. Use the following information when determining how the application will receive attributes in your network.

Global Catalog

Cisco UC Integration for Microsoft Lync connects to a Global Catalog server by default . If you use the default settings, you must ensure that all attributes reside on your Global Catalog server.

You can replicate attributes to a Global Catalog server using an appropriate tool such as the Microsoft Active Directory Schema snap-in.

Note Replicating attributes to your Global Catalog server generates traffic between Active Directory servers in the domain.

See the appropriate Microsoft documentation for instructions on replicating attributes to a Global Catalog server with the Active Directory Schema snap-in.

Domain Controller

You can configure Cisco UC Integration for Microsoft Lync to connect to a Domain Controller if you:

- Do not want to connect to a Global Catalog server.
- Do not want to replicate attributes to a Global Catalog server.

Note The application queries only a single domain if you configure it to connect to a Domain Controller.

Specify 1 as the value of the ConnectionType parameter to configure the application to connect to a Domain Controller. See *Directory Connection Parameters* for more information.

Indexing Attributes

Ensure you index any attributes you use for contact resolution on your directory.

If you use the default attribute mappings, ensure the following attributes are indexed:

- sAMAccountName
- telephoneNumber

Additionally, ensure you index the following attributes for secondary number queries:

- otherTelephone
- mobile
- homePhone

Note By default secondary number queries are enabled in the application. You can disable secondary number queries with the DisableSecondaryNumberLookups parameter.

UDS Directory Integration

UDS is an interface on Cisco Unified Communications Manager that provides contact resolution. You synchronize contact data into Cisco Unified Communications Manager from Microsoft Active Directory or another LDAP directory source. Cisco UC Integration for Microsoft Lync automatically retrieves that contact data directly from Cisco Unified Communications Manager using the UDS interface.

Enable Integration with UDS

To enable integration with UDS, you perform the following steps:

1. Create your directory source in Cisco Unified Communications Manager.
2. Synchronize the contact data to Cisco Unified Communications Manager.
3. Specify UDS as the value of the DirectoryServerType parameter in your Cisco UC Integration for Microsoft Lync configuration file.

Contact data resides in Cisco Unified Communications Manager after the synchronization occurs. The application automatically connects to UDS and performs all contact resolution. You do not need to perform any other server configuration tasks to use UDS.

Contact Photo Retrieval

You must configure the application to retrieve contact photos if you integrate with UDS. For more information, see *Contact Photo Retrieval*.

Contact Resolution with Multiple Clusters

For contact resolution with multiple Cisco Unified Communications Manager clusters, you should synchronize all users on the corporate directory to each Cisco Unified Communications Manager cluster. You should then provision a subset of those users on the appropriate Cisco Unified Communications Manager cluster.

For example, your organization has 40,000 users. 20,000 users reside in North America. 20,000 users reside in Europe. Your organization has the following Cisco Unified Communications Manager clusters for each location:

- cucm-cluster-na for North America
- cucm-cluster-eu for Europe

In this example, you should synchronize all 40,000 users to both clusters. You then provision the 20,000 users in North America on cucu-cluster-na and the 20,000 users in Europe on cucm-cluster-eu.

When users in Europe call users in North America, the application retrieves the contact details for the user in Europe from cucu-cluster-na.

When users in North America call users in Europe, the application retrieves the contact details for the user in North America from cucu-cluster-eu.

Supported LDAP Directory Services

Cisco UC Integration for Microsoft Lync supports the following directory services:

- Microsoft Active Directory 2003
- Microsoft Active Directory 2008
- OpenLDAP
- Active Directory Lightweight Directory Service (AD LDS) or Active Directory Application Mode (ADAM)

Cisco UC Integration for Microsoft Lync supports the following specific integration scenarios with OpenLDAP, AD LDS, and ADAM:

- OpenLDAP integration using anonymous or authenticated bings.
- AD LDS or ADAM integration using anonymous binds, authentication with the Microsoft Windows principal user, or authentication with the AD LDS principal user.

Evaluate your directory service to determine the characteristics of the schema before configuring Cisco UC Integration for Microsoft Lync.

Domain Name System Configuration

Cisco UC Integration for Microsoft Lync must connect to a directory service that can access information for all users in the organization. The application typically retrieves the domain name from the USERDNSDOMAIN environment variable on the user's workstation. This value allows Cisco UC Integration for Microsoft Lync to locate either the Global Catalog or LDAP service in the domain.

Note The application automatically connects to the Global Catalog. The application must be configured to locate an LDAP service.

In some instances, the value of the USERDNSDOMAIN environment variable does not resolve to the DNS domain name that corresponds to the domain name of the entire forest. For example, an instance where this configuration occurs is when an organization uses a sub-domain or resource domain. In such a configuration, the USERDNSDOMAIN environment variable resolves to a child domain, not the parent domain. The result of this type of configuration is that the application cannot access information for all users in the organization.

If the USERDNSDOMAIN environment variable resolves to a child domain, you can use one of the following configuration options to connect to a service in the parent domain:

- Configure the application to use the FQDN of the parent domain.

To perform this configuration, you specify the FQDN of the parent domain as the value of the PrimaryServerName parameter.

- Configure your DNS server to direct the application to a server that can access all users in the organization when it requests a Global Catalog or LDAP service.
- Ensure that the Global Catalog or LDAP service has access to all users in the organization.

For more information about configuring your DNS server, see the following Microsoft documentation:

- *Configuring DNS for the Forest Root Domain*
- *Assigning the Forest Root Domain Name*
- *Deploying a GlobalNames Zone*
- *Support for DNS Namespace planning in Microsoft server products*

Quality of Service Configuration

You can configure group policies in Microsoft Windows so that clients automatically apply Differentiated Services Code Point (DSCP) values to media streams.

The policies you configure should match the application, the UDP protocol, and a source port range. In most cases, you should configure one policy to apply DSCP values to the audio call port range and another policy to apply DSCP values to the video call port range.

See the *Policy-based Quality of Service (QoS)* topic in the Microsoft Windows Server 2008 documentation for more information.

Cisco Media Services Interface

Cisco Media Services Interface provides a Microsoft Windows service that works with Cisco Prime Collaboration Manager and Cisco Medianet-enabled routers to ensure that the application can send audio-visual media on your network with minimum latency and packet loss. The application checks for this service before sending audio-visual media on the network. Flow information is provided to the Cisco Media Services Interface by the application if it is installed. The service then signals the network so that routers classify the flow and provide priority to the application traffic. Audio-visual media is sent normally across the network if this service is not installed.

You must install Cisco Media Services Interface separately and ensure your network is enabled for Cisco Medianet. You must also install Cisco Prime Collaboration Manager and routers enabled for Cisco Medianet.

Port Ranges on Cisco Unified Communications Manager

Cisco Unified Communications Manager lets you define one port range for Cisco UC Integration for Microsoft Lync . The application divides this port range equally and uses the lower half for audio calls and the upper half for video calls. For example, if you define a port range of 1000 to 3000, the application uses a port range of 1000 to 2000 for audio calls and a port range of 2000 to 3000 for video calls.

Part ranges are set on the **SIP Profile Configuration** window for the appropriate SIP profile on Cisco Unified Communications Manager.

To access the **SIP Profile Configuration** window, select **Device** > **Device Settings** > **SIP Profile**.

The **Start Media Port** field defines the lowest port available. The **Stop Media Port** field defines the highest port available. See the *SIP Profile Configuration* topic in the Cisco Unified Communications Manager documentation for more information.

CHAPTER 4

Server Setup

This section provides task-based information to guide you through the server setup process.

Note Providing information on every task involved in installing and configuring Cisco Unified Communications Manager is beyond the scope of this document. The purpose of this chapter is to provide a high-level workflow of the tasks you should complete to set up your environment. See the appropriate documentation for Cisco Unified Communications Manager to review detailed information and ensure you complete the installation and configuration tasks specific to your deployment.

Prerequisites

You must install and configure Cisco Unified Communications Manager before you begin any tasks in this section.

Review the Setup Process

This topic provides a high-level overview of the process to set up your environment with Cisco Unified Communications Manager.

Procedure

Step 1 Add a directory to your environment.
Adding a directory to your environment does the following:

- Populates the Cisco Unified Communications Manager database with user data that resides on your directory server.
- Provides Cisco Unified Communications Manager with users in your environment who you can add to profiles and to whom you can provision capabilities.

Step 2 Set up unified communications.

a) Create software phone devices.
b) Create desk phone devices.

Step 3 (Optional) Set up voicemail.

Add a Directory to Your Environment

Adding a directory to your environment populates the Cisco Unified Communications Manager database with user data that resides on your directory server. Completing this task provides Cisco Unified Communications Manager with users in your environment who you can add to profiles and to whom you can provision capabilities.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **System** > **LDAP** > **LDAP System**.
The **LDAP System Configuration** window opens.

Step 3 Locate the **LDAP System Information** section.

Step 4 Select **Enable Synchronizing from LDAP Server**.

Step 5 Select the appropriate values from the following drop-down lists:

- **LDAP Server Type**
- **LDAP Attribute for User ID**

Step 6 Select **System** > **LDAP** > **LDAP Directory**.

Step 7 Select **Add New**.
The **LDAP Directory** window opens.

Step 8 Specify the required details on the **LDAP Directory** window.
See the LDAP integration topics in the *Cisco Unified Communications Manager Administration Guide* for more information about the values and formats you can specify.

Step 9 Select **Save**.

Step 10 Select **Peform Full Sync Now**.

Note The amount of time it takes for the synchronization process to complete depends on the number of users that exist in your directory. If you synchronize a large directory with thousands of users, you should expect the process to take some time.

User data from your directory server is synchronized to the Cisco Unified Communications Manager database. Cisco Unified Communications Manager then synchronizes the user data to the Cisco Unified Presence database.

What to Do Next

Verify that users from your directory are available on Cisco Unified Communications Manager and Cisco Unified Presence.

If users from your directory are returned in the list of available users, you have successfully added a directory to your environment.

Related Topics

Configuring Cisco Unified Communication Manager Directory Integration
LDAP Directory Configuration
Integrating the LDAP Directory

Create a Service Profile

You create a service profile that contains the configuration settings for the services you add on Cisco Unified Communications Manager. You add the service profile to the end user configuration for your Cisco UC Integration for Microsoft Lync users. Cisco UC Integration for Microsoft Lync can then retrieve settings for available services from the service profile.

Before You Begin

Review the following prerequisites before completing this task:

- Service Profile creation is only available in Cisco Unified Communications Manager 9.0.1 and later.
- Review the *Service profile setup* section of the *Cisco Unified Communications Manager Administration Guide* for specific details about creating service profiles.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management** > **User Settings** > **Service Profile**.
The **Find and List Service Profiles** window opens.

Step 3 Select **Add New**.
The **Service Profile Configuration** window opens.

Step 4 Enter settings on the **Service Profile Configuration** window as follows:

a) Specify a unique name for the service profile in the **Name** field.
b) Specify an optional description in the **Description** field.
c) Select **Make this the default service profile for the system**, if appropriate.

Step 5 Select **Save**.

Create Software Phone Devices

Software phones provide capabilities for Cisco UC Integration for Microsoft Lync to send and receive audio and video through a computer.

Create SIP Profiles

The first step in creating a software phone device is to create a SIP profile so that you can enable video desktop sharing. You cannot edit or configure the default SIP profile. You must create a new SIP profile.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Device Settings** > **SIP Profile**.
The **Find and List SIP Profiles** window opens.

Step 3 Do one of the following to create a new SIP profile:

- Find the default SIP profile and create a copy that you can edit.
- Select **Add New** and create a new SIP profile.

Related Topics

SIP Profile Configuration

Video Desktop Sharing

Binary Floor Control Protocol (BFCP) provides video desktop sharing capabilities for CSF devices. Cisco Unified Communications Manager handles the BFCP packets users transmit when using video desktop sharing capabilities. BFCP presentation sharing is automatically enabled on Cisco Unified Communications Manager version 9.0(1) and higher.

Note

- Cisco Unified Communications Manager supports BFCP presentation sharing on 8.6(1) and higher only.
- Cisco UC Integration for Microsoft Lync supports video desktop sharing on software phone devices. It cannot be enabled for desktop phones.

Tip You must enable BFCP on the SIP trunk to allow video desktop sharing capabilities between nodes in a Cisco Unified Communications Manager cluster. Do the following to enable BFCP on the SIP trunk:

1. Select **Allow Presentation Sharing using BFCP** in the **Trunk Specific Configuration** section of the SIP profile.
2. Select the SIP profile from the **SIP Profile** drop-down list on the CSF device configuration.

Related Topics

Presentation Sharing with the Binary Floor Control Protocol

Create CSF Devices

Complete this procedure for every CSF device.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Phone**
The **Find and List Phones** window opens.

Step 3 Select **Add New**.

Step 4 Select **Cisco Unified Client Services Framework** from the **Phone Type** drop-down list and then select **Next**.
The **Phone Configuration** window opens.

Step 5 Specify a name for the CSF device in the **Device Name** field.
You should use the **CSF*username*** format for CSF device names. For example, you need to create a device name for Tanya Adams whose username is **tadams**. Tanya's device name should be **CSFtadams**.

Step 6 Specify configuration settings on the **Phone Configuration** window as appropriate.
See the *Phone Configuration Settings* topic in the Cisco Unified Communications Manager documentation for more information about the configuration settings on the **Phone Configuration** window.

Step 7 Select **Allow Presentation Sharing using BFCP** in the **Protocol Specific Information** section to enable video desktop sharing for versions of Cisco Unified Communications Manager older than 9.0.1.
Video desktop sharing is enabled by default in Cisco Unified Communications Manager 9.0.1 and later.

Step 8 Select **Save**.

A message is displayed to confirm successful configuration. The **Associate Information** section becomes available on the **Phone Configuration** window.

What to Do Next

Add a directory number to the device and save the configuration.

Add a Directory Number to the Device

You must add directory numbers to devices in Cisco Unified Communications Manager. This topic provides instructions on adding directory numbers using the **Device** > **Phone** menu option after you create your device. Under this menu option, only the configuration settings that apply to the phone model or CTI route point display. See the Cisco Unified Communications Manager documentation for more information about different options to configure directory numbers.

Procedure

Step 1 Locate the **Association Information** section on the **Phone Configuration** window.

Step 2 Select **Add a new DN**.
The **Directory Number Configuration** window opens.

Step 3 Specify a directory number in the **Directory Number** field.

Step 4 Specify all other required configuration settings as appropriate.

Step 5 Associate end users with the directory number as follows:

a) Locate the **Users Associated with Line** section.
b) Select **Associate End Users**.
The **Find and List Users** dialog box opens.
c) Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.
d) Select the appropriate users from the list.
e) Select **Add Selected**.
The selected users are added to the voicemail profile.

Step 6 Select **Save**.

Step 7 Select **Apply Config**.
The **Apply Configuration** window opens.

Step 8 Follow the prompts on the **Apply Configuration** window to apply the configuration.

Set Up Secure Phone Capabilities

You can optionally set up secure phone capabilities for CSF devices. Secure phone capabilities provide secure SIP signaling, secure media streams, and encrypted device configuration files.

Configure the Security Mode

To use secure phone capabilities, you must configure the Cisco Unified Communications Manager security mode using the Cisco CTL Client. You cannot use secure phone capabilities with the nonsecure security mode. At a minimum, you must use mixed mode security.

Mixed mode security:

- Allows authenticated, encrypted, and nonsecure phones to register with Cisco Unified Communications Manager.
- Cisco Unified Communications Manager supports both RTP and SRTP media.
- Authenticated and encrypted devices use secure port 5061 to connect to Cisco Unified Communications Manager.

See the *Cisco Unified Communications Manager Security Guide* for instructions on configuring mixed mode with the Cisco CTL Client.

Create a Phone Security Profile

The first step to setting up secure phone capabilities is to create a phone security profile that you can apply to the device.

Before You Begin

Configure the Cisco Unified Communications Manager security to use mixed mode.

Procedure

Step 1 Select **System** > **Security** > **Phone Security Profile**.

Step 2 Select **Add New**.

Step 3 Select **Cisco Unified Client Services Framework** from the **Phone Security Profile Type** drop-down list and then select **Next**.
The **Phone Security Profile Configuration** window opens.

Configure the Phone Security Profile

After you add a phone security profile, you must configure it to suit your requirements.

Procedure

Step 1 Specify a name for the phone security profile in the **Name** field on the **Phone Security Profile Configuration** window.

Step 2 Specify values for the phone security profile as follows:

Device Security Mode

Select one of the following:

- **Authenticated**
- **Encrypted**

Transport Type

Leave the default value of **TLS**.

TFTP Encrypted Config

Select this checkbox to encrypt the CSF device configuration file that resides on the TFTP server.

Authentication Mode

Select **By Authentication String**.

Key Size (Bits)

Select the appropriate key size for the certificate.

Note Key size refers to the bit length of the public and private keys that the client generates during the CAPF enrollment process. The client has been tested using authentication strings with 1024 bit length keys. The client requires more time to generate 2048 bit length keys than 1024 bit length keys. As a result, if you select 2048, you should expect it to take longer to complete the CAPF enrollment process.

SIP Phone Port

Leave the default value.
The client always uses port 5061 to connect to Cisco Unified Communications Manager when you apply a secure phone profile. The port that you specify in this field only takes effect if you select **Non Secure** as the value for **Device Security Mode**.

Step 3 Select **Save**.

Configure CSF Devices

Add the phone security profile to the devices and complete other configuration tasks for secure phone capabilities.

Procedure

Step 1 Open the CSF device configuration window.

a) Select **Device** > **Phone**.
The **Find and List Phones** window opens.

b) Specify the appropriate filters in the **Find Phone where** field and then select **Find** to retrieve a list of devices.

c) Select the CSF device from the list.

The **Phone Configuration** window opens.

Step 2 Select **Allow Control of Device from CTI** in the **Device Information** section.

Step 3 Select **Save**.

Step 4 Locate the **Protocol Specific Information** section.

Step 5 Select the phone security profile from the **Device Security Profile** drop-down list.

Step 6 Select **Save**.

At this point in the secure phone set up, existing users can no longer use their CSF devices. You must complete the secure phone set up for users to be able to access their CSF devices.

What to Do Next

Specify the certificate settings and generate the authentication string for users.

Specify Certificate Settings

Specify certificate settings in the CSF device configuration and generate the authentication strings that you provide to users.

Procedure

Step 1 Locate the **Certification Authority Proxy Function (CAPF) Information** section on the **Phone Configuration** window.

Step 2 Specify values as follows:

Certificate Operation

Select **Install/Upgrade**.

Authentication Mode

Select **By Authentication String**.

Key Size (Bits)

Select the same key size that you set in the phone security profile.

Operation Completes By

Specify an expiration value for the authentication string or leave as default.

Step 3 Select **Save**.

Step 4 Create the authentication string.
You can do one of the following:

- Select **Generate String** in the **Certification Authority Proxy Function (CAPF) Information** section.
- Enter a custom string in the **Authentication String** field.

What to Do Next

Provide users with the authentication string.

Provide Users with Authentication Strings

Users must specify the authentication string in the client interface to access their CSF devices and securely register with Cisco Unified Communications Manager.

When users enter the authentication string in the client interface, the CAPF enrollment process begins.

Note The time it takes for the enrollment process to complete can vary depending on the specifications of the user's computer and the current load for Cisco Unified Communications Manager. It can take up to one minute for the client to complete the CAPF enrollment process.

The client displays an error if:

- Users enter an incorrect authentication string.

  Users can attempt to enter authentication strings again to complete the CAPF enrollment. However, if a user continually enters an incorrect authentication string, the client might reject any string the user enters, even if the string is correct. In this case, you must generate a new authentication string on the user's CSF device and then provide it to the user.

- Users do not enter the authentication string before the expiration time you set in the **Operation Completes By** field.

  In this case, you must generate a new authentication string on the user's CSF device. The users must then enter that authentication string before the expiration time.

Important When you configure the end users in Cisco Unified Communications Manager, you must add them to the following user groups:

- **Standard CCM End Users**
- **Standard CTI Enabled**

Users must not belong to the following user group:

Standard CTI Secure Connection

Secure Phone Details

Secure Connections

If you enable secure phone capabilities, then:

- SIP connections between CSF devices and Cisco Unified Communications Manager are over TLS.

- If you select **Authenticated** as the value for the **Device Security Mode** field on the phone security profile, the SIP connection is over TLS using NULL-SHA encryption.
- If you select **Encrypted** as the value for the **Device Security Mode** field on the phone security profile, the SIP connection is over TLS using AES 128/SHA encryption.

- Mutual TLS ensures that only CSF devices with the correct certificates can register to Cisco Unified Communications Manager. Likewise, CSF devices can register only to Cisco Unified Communications Manager instances that provide the correct certificate.

If you enable secure phone capabilities for users, their CSF device connections to Cisco Unified Communications Manager are secure. If the other end point also has a secure connection to Cisco Unified Communications Manager, then the call can be secure. However, if the other end point does not have a secure connection to Cisco Unified Communications Manager, then the call is not secure.

Encrypted Media

If you select **Encrypted** as the value for the **Device Security Mode** field on the phone security profile, the client uses Secure Realtime Transport Protocol (SRTP) to offer encrypted media streams as follows:

Media Stream	Encryption
Main video stream	Can be encrypted
Main audio stream	Can be encrypted
Presentation video stream Refers to video desktop sharing using BFCP.	Not encrypted
BFCP application stream Refers to BFCP flow control.	Not encrypted

The ability to encrypt media depends on if the other end points also encrypt media, as in the following examples:

- You enable media encryption for user A and user B. In other words, **Device Security Mode** is set to **Encrypted** on the phone security profile for the users' CSF devices.
- You do not enable media encryption for user C. In other words, **Device Security Mode** is set to **Authenticated** on the phone security profile for the user's CSF device.
- User A calls user B. The client encrypts the main video stream and audio stream.
- User A calls user C. The client does not encrypt the main video stream and audio stream.
- User A, user B, and user C start a conference call. The client does not encrypt the main video stream or audio stream for any user.

Note The client displays a lock icon when it can use SRTP for encrypted media streams to other secured clients or conference bridges.

However, not all versions of Cisco Unified Communications Manager provide the ability to display the lock icon. If the version of Cisco Unified Communications Manager you are using does not provide this ability, the client cannot display a lock icon even when it sends encrypted media.

Stored Files

The client stores the following files for secure phone capabilities:

- Certificate trust list (`.tlv`)
- Locally significant certificate (`.lsc`)
- Private key for the CSF device (`.key`)

The client downloads and stores certificate trust lists whenever you configure Cisco Unified Communications Manager security as mixed mode. Certificate trust lists enable the client to verify the identity of Cisco Unified Communications Manager servers.

The client saves the locally significant certificates and private keys after users successfully enter the authentication code and complete the enrollment process. The locally significant certificate and private key enable the client to establish mutual TLS connections with Cisco Unified Communications Manager.

Note The client encrypts the private key before saving it to the file system.

The client stores these files in the following folder:
`%User_Profile%\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF\Security`

Because the client stores the files in the user's `Roaming` folder, users can log in to any Microsoft Windows account on the Windows domain to register their CSF devices.

Conference Calls

On conference, or multi-party, calls, the conferencing bridge must support secure phone capabilities. If the conferencing bridge does not support secure phone capabilities, calls to that bridge are not secure. Likewise, all parties must support a common encryption algorithm for the client to encrypt media on conference calls.

CSF device security reverts to the lowest level available on multi-party calls. For example, user A, user B, and user C join a conference call. User A and user B have CSF devices with secure phone capabilities. User C has a CSF device without secure phone capabilities. In this case, the call is not secure for all users.

Sharing Secure CSF Devices between Clients

Clients that do not support secure phone capabilities cannot register to secure CSF devices.

Multiple Users on a Shared Microsoft Windows Account

Multiple users can have unique credentials for the client and share the same Windows account. However, the secure CSF devices are restricted to the Windows account that the users share. Users who share the same Windows account cannot make calls with their secure CSF devices from different Windows accounts.

You should ensure that multiple users who share the same Windows account have CSF devices with unique names. Users cannot register their CSF devices if they share the same Windows account and have CSF devices with identical names, but connect to different Cisco Unified Communications Manager clusters.

For example, user A has a CSF device named CSFcompanyname and connects to cluster 1. User B has a CSF device named CSFcompanyname and connects to cluster 2. In this case, a conflict occurs for both CSF devices. Neither user A or user B can register their CSF devices after both users log in to the same Windows account.

Multiple Users on a Shared Computer

The client caches the certificates for each user's secure CSF device in a location that is unique to each Windows user. When a user logs in to their Windows account on the shared computer, that user can access only the secure CSF device that you provision to them. That user cannot access the cached certificates for other Windows users.

Create Desk Phone Devices

Cisco UC Integration for Microsoft Lync users can use their computers to control desk phone and place audio calls. This topic describes how to create desk phone devices on Cisco Unified Communications Manager.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Phone**.
The **Find and List Phones** window opens.

Step 3 Select **Add New**.

Step 4 Select the appropriate device from the **Phone Type** drop-down list and then select **Next**.
The **Phone Configuration** window opens.

Step 5 Complete the following steps in the **Device Information** section:

a) Enter a meaningful description in the **Description** field.
The client displays device descriptions to users. If users have multiple devices of the same model, the descriptions help users tell the difference between multiple devices.

b) Select **Allow Control of Device from CTI**.
If you do not select **Allow Control of Device from CTI**, users cannot control the desk phone.

Step 6 Complete the following steps to enable desk phone video capabilities:

a) Locate the **Product Specific Configuration Layout** section.

b) Select **Enabled** from the **Video Capabilities** drop-down list.

Note If possible, you should enable desk phone video capabilities on the device configuration. However, certain phone models do not include the **Video Capabilities** drop-down list at the device configuration level. In this case, you should open the **Common Phone Profile Configuration** window and then select **Enabled** from the **Video Calling** drop-down list.

See *Desk Phone Video Configuration* for more information about desk phone video.

Step 7 Specify all other configuration settings on the **Phone Configuration** window as appropriate.
See the Cisco Unified Communications Manager documentation for more information about the configuration settings on the **Phone Configuration** window.

Step 8 Select **Save**.
An message displays to inform you if the device is added successfully. The **Association Information** section becomes available on the **Phone Configuration** window.

What to Do Next

Add a directory number to the device and apply the configuration.

Desk Phone Video Configuration

Desk phone video capabilities let users receive video transmitted to their desk phone devices on their computers.

Set Up Desk Phone Video

To set up desk phone video, you must complete the following steps:

1 Physically connect the computer to the computer port on the desk phone device.

You must physically connect the computer to the desk phone device through the computer port so the application can establish a connection to the device. You cannot use desk phone video capabilities with wireless connections to desk phone devices.

Tip If users have both wireless and wired connections available, they should configure Microsoft Windows so that wireless connections do not take priority over wired connections. See the following Microsoft documentation for more information: *An explanation of the Automatic Metric feature for Internet Protocol routes*.

2 Enable the desk phone device for video in Cisco Unified Communications Manager.

See the *Create Desk Phone Devices* topic for instructions.

3 Install Cisco Media Services Interface on the computer.

Cisco Media Services Interface provides the Cisco Discover Protocol (CDP) driver that enables the application to do the following:

- Discover the desk phone device.
- Establish and maintain a connection to the desk phone device using the CAST protocol.

Note Download the **Cisco Media Services Interface** installation program from Cisco.com.

Desk Phone Video Considerations

Review the following considerations and limitations before you provision desk phone video capabilities:

- Cisco UC Integration for Microsoft Lync does not support desk phone video capabilities on Microsoft Windows Vista.
- You cannot use desk phone video capabilities on devices if video cameras are attached to the devices, such as a Cisco Unified IP Phone 9971. You can use desk phone video capabilities if you remove video cameras from the devices.
- You cannot use desk phone video capabilities with devices that do not support CTI.
- Video desktop sharing, using the BFCP protocol, is not supported with desk phone video.
- It is not possible for endpoints that use SCCP to receive video only. SCCP endpoints must send and receive video. Instances where SCCP endpoints do not send video result in audio only calls.
- 7900 series phones must use SCCP for desk phone video capabilities. 7900 series phones cannot use SIP for desk phone video capabilities.
- If a user initiates a call from the keypad on a desk phone device, the call starts as an audio call on the desk phone device. Cisco UC Integration for Microsoft Lync then escalates the call to video. For this reason, you cannot make video calls to devices that do not support escalation, such as H.323 endpoints. To use desk phone video capabilities with devices that do not support escalation, users should initiate calls from Cisco UC Integration for Microsoft Lync.
- A compatibility issue exists with Cisco Unified IP Phones that use firmware version SCCP45.9-2-1S. You must upgrade your firmware to version SCCP45.9-3-1 to use desk phone video capabilities.
- Some antivirus or firewall applications, such as Symantec EndPoint Protection, block inbound CDP packets, which disables desk phone video capabilities. You should configure your antivirus or firewall application to allow inbound CDP packets.

  The following article provides additional details about this issue: http://www.symantec.com/docs/TECH105234

If you encounter an error that indicates desk phone video capabilities are unavailable or the desk phone device is unknown, do the following:

1. Ensure you enable the desk phone device for video in Cisco Unified Communications Manager.
2. Reset the physical desk phone.
3. Exit Cisco UC Integration for Microsoft Lync.
4. Run services.msc on the computer where you installed Cisco UC Integration for Microsoft Lync.
5. Restart Cisco Media Services Interface.
6. Restart Cisco UC Integration for Microsoft Lync.

Add a Directory Number to the Device

You must add directory numbers to devices in Cisco Unified Communications Manager. This topic provides instructions on adding directory numbers using the **Device** > **Phone** menu option after you create your device. Under this menu option, only the configuration settings that apply to the phone model or CTI route point

display. See the Cisco Unified Communications Manager documentation for more information about different options to configure directory numbers.

Procedure

Step 1 Locate the **Association Information** section on the **Phone Configuration** window.

Step 2 Select **Add a new DN**.
The **Directory Number Configuration** window opens.

Step 3 Specify a directory number in the **Directory Number** field.

Step 4 Specify all other required configuration settings as appropriate.

Step 5 Associate end users with the directory number as follows:

a) Locate the **Users Associated with Line** section.
b) Select **Associate End Users**.
The **Find and List Users** dialog box opens.
c) Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.
d) Select the appropriate users from the list.
e) Select **Add Selected**.
The selected users are added to the voicemail profile.

Step 6 Select **Save**.

Step 7 Select **Apply Config**.
The **Apply Configuration** window opens.

Step 8 Follow the prompts on the **Apply Configuration** window to apply the configuration.

Enable Video Rate Adaptation

Cisco UC Integration for Microsoft Lync uses video rate adaptation to negotiate optimum video quality. Video rate adaptation dynamically increases or decreases video quality based on network conditions.

To use video rate adaptation, you must enable Real-Time Transport Control Protocol (RTCP) on Cisco Unified Communications Manager.

Note RTCP is enabled on software phone devices by default. However, you must enable RTCP on desk phone devices.

Enable RTCP on Common Phone Profiles

You can enable RTCP on a common phone profile to enable video rate adaptation on all devices that use the profile.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Device Settings** > **Common Phone Profile**.
The **Find and List Common Phone Profiles** window opens.

Step 3 Specify the appropriate filters in the **Find Common Phone Profile where** field and then select **Find** to retrieve a list of profiles.

Step 4 Select the appropriate profile from the list.
The **Common Phone Profile Configuration** window opens.

Step 5 Locate the **Product Specific Configuration Layout** section.

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

Step 7 Select **Save**.

Enable RTCP on Device Configurations

You can enable RTCP on specific device configurations instead of a common phone profile. The specific device configuration overrides any settings you specify on the common phone profile.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Phone**.
The **Find and List Phones** window opens.

Step 3 Specify the appropriate filters in the **Find Phone where** field and then select **Find** to retrieve a list of phones.

Step 4 Select the appropriate phone from the list.
The **Phone Configuration** window opens.

Step 5 Locate the **Product Specific Configuration Layout** section.

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

Step 7 Select **Save**.

Add a Remote Destination

Remote destinations represent the available CTI controllable devices.

You should add a remote destination through the **Cisco Unified CM Administration** interface if you plan to provision users with dedicated CTI remote devices. This task ensures that users can automatically control their phones and place calls when they start the application.

If you plan to provision users with CTI remote devices along with software phone devices and desk phone devices, you should not add a remote destination through the **Cisco Unified CM Administration** interface. Users can enter remote destinations through the client interface.

Note

- The application supports only one remote destination per user. You should not add two or more remote destinations for a user.
- Cisco Unified Communications Manager does not verify if it can route remote destinations that you add through the **Cisco Unified CM Administration** interface. For this reason, you must ensure that Cisco Unified Communications Manager can route the remote destinations you add.
- Cisco Unified Communications Manager automatically applies application dial rules to all remote destination numbers for CTI remote devices. For more information about application dial rules, see *Dial Plan Mapping*.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Phone**.
The **Find and List Phones** window opens.

Step 3 Specify the appropriate filters in the **Find Phone where** field to and then select **Find** to retrieve a list of phones.

Step 4 Select the CTI remote device from the list.
The **Phone Configuration** window opens.

Step 5 Locate the **Associated Remote Destinations** section.

Step 6 Select **Add a New Remote Destination**.
The **Remote Destination Information** window opens.

Step 7 Specify JabberRD in the **Name** field.

Restriction You must specify JabberRD in the **Name** field. The application uses only the JabberRD remote destination. If you specify a name other than JabberRD, users cannot access that remote destination.

The application automatically sets the JabberRD name when users add remote destinations through the client interface.

Step 8 Enter the destination number in the **Destination Number** field.

Step 9 Specify all other values as appropriate.
See the *Remote destination configuration settings* topic in the Cisco Unified Communications Manager documentation for more information.

Step 10 Select **Save**.

What to Do Next

Complete the following steps to verify the remote destination and apply the configuration to the CTI remote device:

1 Repeat the steps to open the **Phone Configuration** window for the CTI remote device.

2 Locate the **Associated Remote Destinations** section.

3 Verify the remote destination is available.

4 Select **Apply Config**.

Note The **Device Information** section on the **Phone Configuration** window contains a **Active Remote Destination** field.

When users select a remote destination in Cisco UC Integration for Microsoft Lync, it displays as the value of **Active Remote Destination**.

none displays as the value of **Active Remote Destination** if:

- Users do not select a remote destination in the application.
- Users exit or are not signed in to the application.

Add a CTI Service

The CTI service enables Cisco UC Integration for Microsoft Lync users to control devices.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management** > **User Settings** > **UC Service**.
The **Find and List UC Services** window opens.

Step 3 Select **Add New**.
The **UC Service Configuration** window opens.

Step 4 In the **Add a UC Service** section, select **CTI** from the **UC Service Type** drop-down list.

Step 5 Select **Next**.

Step 6 Provide details for the instant messaging and presence service as follows:

a) Specify a name for the service in the **Name** field.
The name you specify displays when you add services to profiles. Ensure the name you specify is unique, meaningful, and easy to identify.

b) Specify an optional description in the **Description** field.

c) Specify the CTI service address in the **Host Name/IP Address** field.

d) Specify the port number for the CTI service in the **Port** field.

Step 7 Select **Save**.

Apply CTI Service

After you add a CTI service on Cisco Unified Communications Manager, you must apply it to a service profile so that Cisco UC Integration for Microsoft Lync can retrieve the settings.

Before You Begin

Create a service profile.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management** > **User Settings** > **Service Profile**.
The **Find and List Service Profiles** window opens.

Step 3 Find and select your service profile.
The **Service Profile Configuration** window opens.

Step 4 In the **CTI Profile** section, select up to three services from the following drop-down lists:

- **Primary**
- **Secondary**
- **Tertiary**

Step 5 Select **Save**.

Related Topics

Service profile setup

Configure User Associations

You must associate users with software phone and desk phone devices on Cisco Unified Communications Manager. Associating users with devices allows the users to access those devices and send or receive audio and video calls.

In addition to associating users with devices, you must also add users to the appropriate user groups.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management** > **End User**.
The **Find and List Users** window opens.

Step 3 Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.

Step 4 Select the appropriate user from the list.

The **End User Configuration** window opens.

Step 5 Locate the **Device Information** section.

Step 6 Select **Device Association**.
The **User Device Association** window opens.

Step 7 Select the devices to which you want to associate the user.

Step 8 Select **Save Selected/Changes**.

Step 9 Select **User Management** > **End User** and return to the **Find and List Users** window.

Step 10 Find and select the same user from the list.
The **End User Configuration** window opens.

Step 11 Locate the **Permissions Information** section.

Step 12 Select **Add to User Group**.
The **Find and List User Groups** dialog box opens.

Step 13 Select the groups to which you want to assign the user.
At a minimum you should assign the user to the following groups:

- **Standard CCM End Users**
- **Standard CTI Enabled**

Certain phone models require additional groups, as follows:

- Cisco Unified IP Phone 9900 or 8900 series, select **Standard CTI Allow Control of Phones supporting Connected Xfer and conf**.
- Cisco Unified IP Phone 6900 series, select **Standard CTI Allow Control of Phones supporting Rollover Mode**.

Step 14 Select **Add Selected**.
The **Find and List User Groups** window closes.

Step 15 Select **Save** on the **End User Configuration** window.

Reset Devices

You should reset devices after you add software phones and desk phones and associate users with those devices.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Phone**.

The **Find and List Phones** window opens.

Step 3 Specify the appropriate filters in the **Find Phone where** field and then select **Find** to retrieve a list of devices.

Step 4 Select the appropriate device from the list.
The **Phone Configuration** window opens.

Step 5 Locate the **Association Information** section.

Step 6 Select the appropriate directory number configuration.
The **Directory Number Configuration** window opens.

Step 7 Select **Reset**.
The **Device Reset** dialog box opens.

Step 8 Select **Reset**.

Step 9 Select **Close** to close the **Device Reset** dialog box.

Dial Plan Mapping

You configure dial plan mapping on Cisco Unified Communications Manager to ensure that dialing rules on Cisco Unified Communications Manager match dialing rules on your directory.

Review the *Dial Rules Overview* topic in the Cisco Unified Communications Manager documentation for more information on configuring dial plan mapping.

Application Dial Rules

Application dial rules automatically add or remove digits in phone numbers that users dial. Application dialing rules manipulate numbers that users dial from the application.

For example, you can configure a dial rule that automatically adds the digit 9 to the start of a 7 digit phone number to provide access to outside lines.

Directory Lookup Dial Rules

Directory lookup dial rules transform caller ID numbers into numbers that Cisco UC Integration for Microsoft Lync can lookup in the directory. Each directory lookup rule you define specifies which numbers to transform based on the initial digits and the length of the number.

For example, you can create a directory lookup rule that automatically removes the area code and two digit prefix digits from 10 digit telephone numbers. An example of this type of rule is to transform 4089023139 into 23139.

Publish Dial Rules

Cisco Unified Communications Manager versions 8.5 and lower do not automatically publish dial rules to the client. For this reason, you must deploy a COP file to publish your dial rules.This COP file copies your dial rules from the Cisco Unified Communications Manager database to an XML file on your TFTP server. The client can then download that XML file and access your dial rules.

Before You Begin

1. Create your dial rules in Cisco Unified Communications Manager.
2. Download the Cisco UC Integration for Microsoft Lync administration package from Cisco.com.
3. Copy `cmterm-csf-dialrule-wizard-0.1.cop.sgn` from the Cisco UC Integration for Microsoft Lync administration package to your file system.

Procedure

Step 1 Open the **Cisco Unified OS Administration** interface.

Step 2 Select **Software Upgrades** > **Install/Upgrade**.

Step 3 Specify the location of `cmterm-csf-dialrule-wizard-0.1.cop.sgn` in the **Software Installation/Upgrade** window.

Step 4 Select **Next**.

Step 5 Select `cmterm-csf-dialrule-wizard-0.1.cop.sgn` from the **Available Software** list.

Step 6 Select **Next** and then select **Install**.

Step 7 Restart the TFTP service.

Step 8 Open the dial rules XML files in a browser to verify that they are available on your TFTP server.

a) Navigate to `http://tftp_server_address:6970/CUPC/AppDialRules.xml`.

b) Navigate to `http://tftp_server_address:6970/CUPC/DirLookupDialRules.xml`.

If you can access AppDialRules.xml and DirLookupDialRules.xml with your browser, the client can download your dial rules.

Step 9 Repeat the preceding steps for each Cisco Unified Communications Manager instance that runs a TFTP service.

What to Do Next

After you repeat the preceding steps on each Cisco Unified Communications Manager instance, restart Cisco UC Integration for Microsoft Lync.

Set Up Voicemail

Setting up voicemail enables users to receive voice mail messages and redirect incoming audio calls to the voicemail service. As part of the task of setting up voicemail, you can also configure a mailstore to enable visual voicemail in the client.

Add a Voicemail Service

Allow users to receive voice messages.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management** > **User Settings** > **UC Service**.
The **Find and List UC Services** window opens.

Step 3 Select **Add New**.
The **UC Service Configuration** window opens.

Step 4 In the **Add a UC Service** section, select **Voicemail** from the **UC Service Type** drop-down list.

Step 5 Select **Next**.

Step 6 Specify details for the voicemail service as follows:

Product Type

Select **Unity Connection**.

Name

Enter a descriptive name for the server, for example, PrimaryVoicemailServer.

Description

Enter an optional description.

Hostname/IP Address

Enter the address of the voicemail server in one of the following formats:

- Hostname
- IP Address
- FQDN

Port

Enter the port to connect to the voicemail server.

Protocol Type

Select the appropriate protocol.

Step 7 Select **Save**.

What to Do Next

Add the voicemail service to your service profile.

Apply Voicemail Service

After you add a voicemail service on Cisco Unified Communications Manager, you must apply it to a service profile so that the client can retrieve the settings.

Before You Begin

Create a service profile if none already exist or you require a separate service profile for voicemail.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management** > **User Settings** > **Service Profile**.
The **Find and List Service Profiles** window opens.

Step 3 Find and select your service profile.
The **Service Profile Configuration** window opens.

Step 4 Configure the **Voicemail Profile** section as follows:

a) Select up to three services from the following drop-down lists:

- **Primary**
- **Secondary**
- **Tertiary**

b) To synchronize credentials with the voicemail service, select **Unified CM - IM and Presence** from the **Credentials source for voicemail service** drop-down list.
Unified CM - IM and Presence uses the instant messaging and presence credentials to log in to the voicemail service. As a result, users do not need to enter their credentials for voicemail services in the client.

Note Do not select **Web conferencing**. This option uses the conferencing credentials to log in to the voicemail service. You cannot currently synchronize with conferencing credentials.

Step 5 Select **Save**.

Add a Mailstore Service

The mailstore service provides users with visual voicemail capabilities.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management** > **User Settings** > **UC Service**.
The **Find and List UC Services** window opens.

Step 3 Select **Add New**.

The **UC Service Configuration** window opens.

Step 4 In the **Add a UC Service** section, select **MailStore** from the **UC Service Type** drop-down list.

Step 5 Select **Next**.

Step 6 Provide details for the mailstore service as follows:

Name

Enter a descriptive name for the server, for example, PrimaryMailStoreServer.

Description

Enter an optional description.

Hostname/IP Address

Enter the address of the mailstore server in one of the following formats:

- Hostname
- IP Address
- FQDN

Port

Enter the port to connect to the mailstore server.

Protocol Type

Select the appropriate protocol.

Step 7 Select **Save**.

What to Do Next

Add the mailstore service to your service profile.

Apply Mailstore Service

After you add a mailstore service on Cisco Unified Communications Manager, you must apply it to a service profile so that the client can retrieve the settings.

Before You Begin

Create a service profile if none already exist or you require a separate service profile for the mailstore service.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management** > **User Settings** > **Service Profile**.

The **Find and List Service Profiles** window opens.

Step 3 Find and select your service profile.
The **Service Profile Configuration** window opens.

Step 4 Configure the **MailStore Profile** section as follows:

a) Select up to three services from the following drop-down lists:

- **Primary**
- **Secondary**
- **Tertiary**

b) Specify appropriate values for the following fields:

- **Inbox Folder**
- **Trash Folder**
- **Polling Interval**

c) Select the **Allow dual folder mode** if your mailstore supports IMAP UIDPLUS extensions.

Step 5 Select **Save**.

Configure Retrieval and Redirection

Configure retrieval so that users can access voice mail messages in the client interface. Configure redirection so that users can send incoming calls to voice mail. You configure retrieval and redirection on Cisco Unified Communications Manager.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Configure the voicemail pilot.

a) Select **Advanced Features** > **Voice Mail** > **Voice Mail Pilot**.
The **Find and List Voice Mail Pilots** window opens.

b) Select **Add New**.
The **Voice Mail Pilot Configuration** window opens.

c) Specify the appropriate details on the **Voice Mail Pilot Configuration** window.

d) Select **Save**.

Step 3 Add the voicemail pilot to the voicemail profile.

a) Select **Advanced Features** > **Voice Mail** > **Voice Mail Profile**.
The **Find and List Voice Mail Mail Profiles** window opens.

b) Specify the appropriate filters in the **Find Voice Mail Profile where Voice Mail Profile Name** field and then select **Find** to retrieve a list of profiles.

c) Select the appropriate profile from the list.
The **Voice Mail Pilot Configuration** window opens.

d) Select the voicemail pilot from the **Voice Mail Pilot** drop-down list.

e) Select **Save**.

Step 4 Specify the voicemail profile in the directory number configuration.

a) Select **Device** > **Phone**.
The **Find and List Phones** window opens.

b) Specify the appropriate filters in the **Find Phone where** field and then select **Find** to retrieve a list of devices.

c) Select the appropriate device from the list.
The **Phone Configuration** window opens.

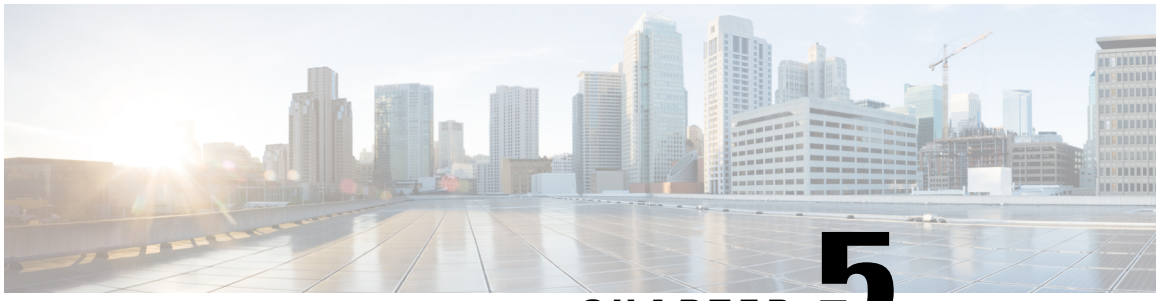
d) Locate the **Association Information** section.

e) Select the appropriate device number.
The **Directory Number Configuration** window opens.

f) Locate the **Directory Number Settings** section.

g) Select the voicemail profile from the **Voice Mail Profile** drop-down list.

h) Select **Save**.



CHAPTER 5

Client Installation

Review the options for installation and learn about different methods for installing Cisco UC Integration for Microsoft Lync. Understand the requirements for successful deployments before you start the installation procedure.

Installation Overview

You can install the client on the following operating systems:

- Microsoft Windows 7 32 bit
- Microsoft Windows 7 64 bit
- Microsoft Windows XP 32 bit with Service Pack 3

Note Cisco UC Integration for Microsoft Lync does not require the Microsoft .NET Framework or any Java modules.

For more information about installation requirements, see the Hardware Requirements and Software Requirements topics.

Note Restart Microsoft Outlook after installing Cisco UC Integration for Microsoft Lync to ensure Click to Call functionality initializes properly.

Installation Options

Cisco UC Integration for Microsoft Lync provides an MSI installation package that gives you the following options for installation:

Install through the Command Line

You can install Cisco UC Integration for Microsoft Lync in a command line window using arguments to specify installation properties.

Choose this option if you plan to install multiple instances across an organization.

For more information, see Use the Command Line.

Repackage the MSI

You can use a program such as Microsoft Orca to customize the Cisco UC Integration for Microsoft Lync installation package. Repackaging the MSI lets you open the default installation package, specify the required installation properties, and then save a custom installation package.

Choose this option if you plan to distribute an installation package with the same installation properties.

For more information, see Transform the Installer.

Run the MSI Manually

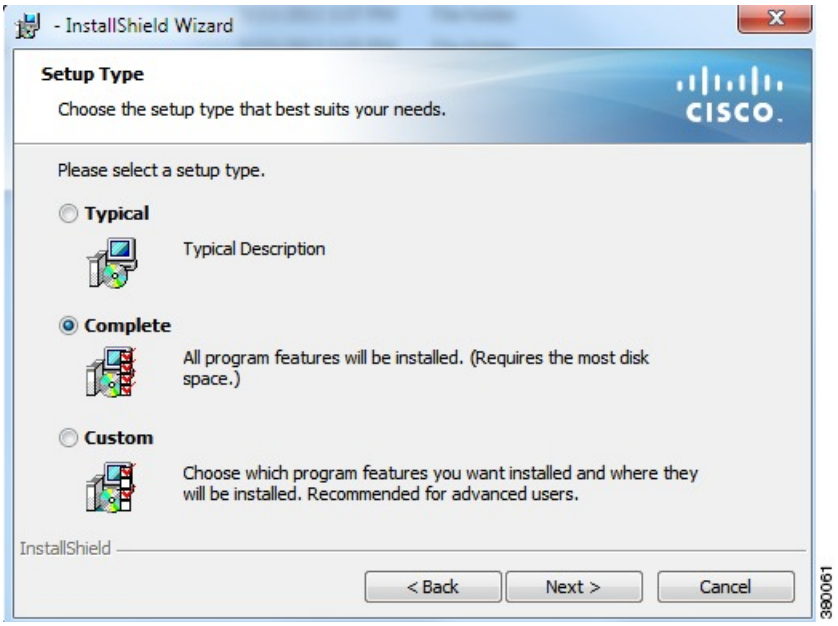
You can run the MSI manually on the file system of the client computer and then specify connection properties when you start Cisco UC Integration for Microsoft Lync for the first time.

Choose this option if you plan to install a single instance for testing or evaluation purposes.

For more information, see Run the MSI Manually.

Click to Call Installation

Ensure the application is installed using the **Complete** installer option to install Click to Call functionality. The **Typical** option does not include Click to Call functionality. The **Custom** option provides the ability to exclude Click to Call.



Use the Command Line

You can specify command line arguments to apply properties to Cisco UC Integration for Microsoft Lync during installation.

Before You Begin

Prepare Cisco UC Integration for Microsoft Lync for deployment with your software configuration management program.

Procedure

Step 1 Open a command line window.

Step 2 Enter the following command:

```
msiexec.exe /i CUCILyncSetup.msi
```

Step 3 Specify the appropriate command line arguments as parameter=value pairs in the command line window. The following are example commands to install Cisco UC Integration for Microsoft Lync:

Installation Example
`msiexec.exe /i CUCILyncSetup.msi LANGUAGE=1033 /quiet` Where: LANGUAGE=1033 specifies English as the language. /quiet specifies a silent installation.

See *Command Line Arguments* for more information about the command line arguments.

Step 4 Run the command to install Cisco UC Integration for Microsoft Lync.

Command Line Arguments

The following table describes the command line arguments you can use to install Cisco UC Integration for Microsoft Lync:

Argument	Value	Description
TFTP	IP address Hostname FQDN	Specifies the address of your TFTP server. Set one of the following as the value: **Hostname** For example, hostname **IP address** For example, 123.45.254.1 **Fully qualified domain name** For example, hostname.domain.com
CTI	IP address Hostname FQDN	Specifies the address of your CTI server. This argument is required only if the address of your CTI server is not the same as the address of your TFTP server. If both server addresses are the same, you do not need to specify this argument.
CCMCIP	IP address Hostname FQDN	Specifies the address of your CCMCIP server. This argument is required only if the address of your CCMCIP server is not the same as the address of your TFTP server. If both server addresses are the same, you do not need to specify this argument.

Argument	Value	Description
LANGUAGE	LCID in decimal	Defines the Locale ID (LCID), in decimal, of the language that Cisco UC Integration for Microsoft Lync uses. The value must be an LCID in decimal that corresponds to a supported language. For example, you can specify one of the following: • 1033 specifies English. • 1036 specifies French. • 1034 specifies Spanish. • 2052 specifies Chinese - China. This argument is optional. If you do not specify a value, Cisco UC Integration for Microsoft Lync uses the system locale language as the default. See the *Supported Languages* topic for a full list of the languages you can specify.

LOG_DIRECTORY	Directory path	Specifies a custom directory location for log files. The directory location is specified using the template `LOG_DIRECTORY=<directory_location>`. Directory paths containing spaces must be placed in double quotes.
		The following is an example of using this parameter:
		`msiexec /i CUCILyncSetup.msi LOG_DIRECTORY=C:\CUCILyncCustomLogDirectory`
		This following is an example of using this parameter for a silent installation:
		`msiexec /i CUCILyncSetup.msi LOG_DIRECTORY=C:\CUCILyncCustomLogDirectory /quiet`

FORGOT_PASSWORD_URL	URL	Specifies the URL to which users are directed if they forget, or need to reset, their passwords. You do not need to specify this argument to enable the functionality. However, you should provide a valid URL to ensure users can obtain new passwords.

Argument	Value	Description
TFTP_FILE_NAME	Filename	Specifies a unique name for the global configuration file on your TFTP server. You should specify a value for this argument if your global configuration file does not use the default name of `jabber-config.xml`. You can specify either an unqualified or fully qualified filename as the value. The name you specify as the value for this argument overrides any other global configuration files on your TFTP server. This argument is optional.
CLEAR	1	Specifies if Cisco UC Integration for Microsoft Lync overrides any existing bootstrap file from previous installations. Cisco UC Integration for Microsoft Lync saves the arguments and values you set during installation to the bootstrap file, `jabber-bootstrap.properties`. Cisco UC Integration for Microsoft Lync then loads settings from the bootstrap file at startup. **Specify this argument** If you specify this argument, the following occurs during installation: 1 Cisco UC Integration for Microsoft Lync deletes any existing bootstrap file. 2 Cisco UC Integration for Microsoft Lync creates a new bootstrap file. **Do not specify this argument** If you do not specify this argument, Cisco UC Integration for Microsoft Lync checks for existing bootstrap files during installation. • If no bootstrap file exists, Cisco UC Integration for Microsoft Lync creates a bootstrap file during installation. • If a bootstrap file exists, Cisco UC Integration for Microsoft Lync does not override that bootstrap file and preserves the existing settings.

Argument	Value	Description
		Note If you are reinstalling Cisco UC Integration for Microsoft Lync, you should consider the following: • Cisco UC Integration for Microsoft Lync does not preserve settings from existing bootstrap files. If you specify CLEAR, you must also specify all other installation arguments as appropriate. • Cisco UC Integration for Microsoft Lync does not save your installation arguments to an existing bootstrap file. If you want to change the values for installation arguments, or specify additional installation arguments, you must specify CLEAR to override the existing settings. To override existing bootstrap files, specify CLEAR in the command line as follows: `msiexec.exe /i CUCILyncSetup.msi CLEAR=1`

Supported languages

The following table lists the languages that Cisco UC Integration for Microsoft Lync supports:

- Arabic
- Chinese - China
- Chinese - Taiwan
- Czech
- Danish
- Dutch
- English
- French
- Finnish
- German
- Greek
- Hebrew
- Italian
- Japanese

- Korean
- Norwegian
- Polish
- Portuguese - Brazil
- Portuguese - Portugal
- Russian
- Swedish
- Spanish
- Turkish

Note Cisco UC Integration for Microsoft Lync does not support Locale IDs for all sub-languages. For example, if you specify French - Canada, Cisco UC Integration for Microsoft Lync uses French - France.

As of this release, Cisco UC Integration for Microsoft Lync supports the Locale IDs for Chinese - China and Chinese - Taiwan only. Cisco UC Integration for Microsoft Lync does not support any other Locale IDs for Chinese sub-languages. For example, if you specify Chinese - Singapore, Cisco UC Integration for Microsoft Lync uses English.

See the following documentation for more information about Locale IDs:

- *Microsoft Windows Locale Code Identifier (LCID) Reference*
- *Locale IDs Assigned by Microsoft*

Repackage the MSI

You can repackage `CUCILyncSetup.msi` to create a custom MSI that contains the installation properties you require.

Use Custom Installers

You use the `CUCILyncProperties.mst` transform file to modify `CUCILyncSetup.msi` and create custom installers.

Restriction You must remove all language codes from the custom installer except for 1033 (English).

Microsoft Orca does not retain any language files in custom installers except for the default, which is 1033. If you do not remove all language codes from the custom installer, you cannot run the installer on any operating system where the language is other than English.

Note Applying transform files does not alter the digital signatures of `CUCILyncSetup.msi`.

Before You Begin

1. Download the Cisco UC Integration for Microsoft Lync administration package from Cisco.com.
2. Copy `CUCILyncProperties.mst` from the administration package to your file system.
3. Download and install Microsoft Windows SDK for Windows 7 and .NET Framework 4 from the Microsoft website.

   You use Microsoft Orca to create custom versions of `CUCILyncSetup.msi`. Microsoft Orca is available as part of the Microsoft Windows SDK for Windows 7 and .NET Framework 4.

Procedure

Step 1 Start Microsoft Orca.

Step 2 Open `CUCILyncSetup.msi` in Microsoft Orca.

a) Select **File** > **Open**.
b) Browse to the location of `CUCILyncSetup.msi` on your file system.
c) Select `CUCILyncSetup.msi` and then select **Open**.

`CUCILyncSetup.msi` opens in Microsoft Orca. The list of tables for the installer opens in the **Tables** pane.

Step 3 Remove all language codes except for 1033 (English).

a) Select **View** > **Summary Information**.
The **Edit Summary Information** window displays.
b) Locate the **Languages** field.
c) Delete all language codes except for 1033.
d) Select **OK**.

English is set as the language for your custom installer.

Step 4 Apply `CUCILyncProperties.mst`.

a) Select **Transform** > **Apply Transform**.
b) Browse to the location of `CUCILyncProperties.mst` on your file system.
c) Select `CUCILyncProperties.mst` and then select **Open**.

Step 5 Select **Property** from the list of tables in the **Tables** pane.
The list of properties for `CUCILyncSetup.msi` opens in the right panel of the application window.

`CUCILyncProperties.mst` applies the following properties:

- LANGUAGE
- TFTP_FILE_NAME
- FORGOT_PASSWORD_URL

These properties correspond to the command line arguments and have the same values. See *Command Line Arguments* for descriptions of each property and the values you can specify.

Step 6 Specify values for the properties as appropriate or drop any properties you do not require.

Step 7 Enable your custom installer to save embedded streams.

a) Select **Tools** > **Options**.
b) Select the **Database** tab.
c) Select **Copy embedded streams during 'Save As'**.
d) Select **Apply** and then **OK**.

Step 8 Save your custom installer.

a) Select **File** > **Save Transformed As**.
b) Select a location on your file system to save the installer.
c) Specify a name for the installer and then select **Save**.

What to Do Next

Prepare your custom installer for deployment with your software configuration management program.

Related Topics

Microsoft Windows SDK for Windows 7 and .NET Framework 4

Create Custom Transform Files

Custom transform files contain properties and values that you can apply to installers. For example, you can create one transform file that sets the default language of Cisco UC Integration for Microsoft Lync to French during installation and another transform file that sets the default language to Spanish. You can then apply each transform file to `CUCILyncSetup.msi` and create two installers, one for each language.

Procedure

Step 1 Start Microsoft Orca.

Step 2 Open `CUCILyncSetup.msi` and then apply `CUCILyncProperties.mst`.
See *Transform the Installer* for more information.

Step 3 Specify values for the appropriate installer properties.

Step 4 Generate and save the transform file.

a) Select **Transform** > **Generate Transform**.
b) Select a location on your file system to save the transform file.
c) Specify a name for the transform file and select **Save**.

The transform file you created is saved as *`file_name`*`.mst`. You can apply this transform file to modify the properties of `CUCILyncSetup.msi`.

Deploy with Group Policy

Install Cisco UC Integration for Microsoft Lync with Group Policy using the Microsoft Group Policy Management Console (GPMC) on Microsoft Windows Server.

Note To install Cisco UC Integration for Microsoft Lync with Group Policy, all computers or users to which you plan to deploy Cisco UC Integration for Microsoft Lync must be in the same domain.

Before You Begin

Complete the following steps to set a language code in the installation package:

1. Start Microsoft Orca.

   Microsoft Orca is available as part of the Microsoft Windows SDK for Windows 7 and .NET Framework 4 that you can download from the Microsoft website.

2. Open `CUCILyncSetup.msi`.
   a. Select **File** > **Open**.
   b. Browse to the location of `CUCILyncSetup.msi` on your file system.
   c. Select `CUCILyncSetup.msi` and then select **Open**.
3. Select **View** > **Summary Information**.
4. Locate the **Languages** field.
5. Set the Locale ID that corresponds to the installation language.

   For example, set 1033 as the Locale ID to specify English as the installation language.
6. Select **OK**.
7. Save the installation package.

   You must enable embedded streams if you select **File** > **Save As** to save the installation package.
   1. Select **Tools** > **Options** and then select the **Database** tab.
   2. Select **Copy embedded streams during 'Save As'**.
   3. Select **Apply** and then **OK**.

Procedure

Step 1 Copy the installation package to a software distribution point for deployment.
All computers or users to which you plan to deploy Cisco UC Integration for Microsoft Lync must be able to access the installation package on the distribution point.

Step 2 Select **Start** > **Run** and then enter the following command:
`GPMC.msc`

The **Group Policy Management** console opens.

Step 3 Create a new group policy object.

a) Right-click on the appropriate domain in the left pane.
b) Select **Create a GPO in this Domain, and Link it here**.
The **New GPO** window opens.
c) Enter a name for the group policy object in the **Name** field.
d) Leave the default value or select an appropriate option from the **Source Starter GPO** drop-down list and then select **OK**.
The new group policy displays in the list of group policies for the domain.

Step 4 Set the scope of your deployment.

a) Select the group policy object under the domain in the left pane.
The group policy object displays in the right pane.
b) Select **Add** in the **Security Filtering** section of the **Scope** tab.
The **Select User, Computer, or Group** window opens.
c) Specify the computers and users to which you want to deploy Cisco UC Integration for Microsoft Lync.

Step 5 Specify the installation package.

a) Right-click the group policy object in the left pane and then select **Edit**.
The **Group Policy Management Editor** opens.
b) Select **Computer Configuration** and then select **Policies** > **Software Settings**.
c) Right-click **Software Installation** and then select **New** > **Package**.
d) Enter the location of the installation package next to **File Name**; for example, `\\server\software_distribution`.

Important You must enter a Uniform Naming Convention (UNC) path as the location of the installation package. If you do not enter a UNC path, Group Policy cannot deploy Cisco UC Integration for Microsoft Lync.

e) Select the installation package and then select **Open**.
f) In the **Deploy Software** dialog box, select **Assigned** and then **OK**.

Group Policy installs Cisco UC Integration for Microsoft Lync on each computer the next time each computer starts.

Cisco Media Services Interface

Cisco Media Services Interface provides a Microsoft Windows service that works with Cisco Prime Collaboration Manager and Cisco Medianet-enabled routers to ensure that Cisco UC Integration for Microsoft Lync can send audio media and video media on your network with minimum latency or packet loss. This section contains information on Cisco Media Services Interface and using it for traffic marking and desktop phone video.

Traffic Marking

Cisco UC Integration for Microsoft Lync can use Cisco Media Services Interface to provide flow information. Cisco UC Integration for Microsoft Lync checks for Cisco Media Services Interface before sending audio media or video media.

- If the service exists on the computer, Cisco UC Integration for Microsoft Lync provides flow information to Cisco Media Services Interface.

  The service then signals the network so that routers classify the flow and provide priority to the Cisco UC Integration for Microsoft Lync traffic.
- If the service does not exist, Cisco UC Integration for Microsoft Lync does not use it and sends audio media and video media as normal.

Note Cisco UC Integration for Microsoft Lync checks for Cisco Media Services Interface for each audio call or video call.

Desk Phone Video Capabilities

You must install Cisco Media Services Interface to enable desk phone video capabilities. Cisco Media Services Interface provides a driver that enables Cisco UC Integration for Microsoft Lync to do the following:

- Discover the desk phone device.
- Establish and maintain a connection to the desk phone device using the CAST protocol.

Before You Begin

To install Cisco Media Services Interface for traffic marking, you must do the following:

- Install Cisco Prime Collaboration Manager.
- Install routers or switches enabled for Cisco Medianet where appropriate.
- Configure your network to handle the metadata attributes that Cisco Media Services Interface applies to applications.

  Note that not all devices on your network must support Cisco Medianet. The first hop should prioritize traffic based on the metadata attributes from Cisco Media Services Interface. As the traffic traverses the network, all other devices should also prioritize that traffic unless you configure policies on those devices to handle the traffic differently. See the Medianet Knowledge Base Portal for detailed information on configuring your network.

Important

- Cisco UC Integration for Microsoft Lync supports Cisco Media Services Interface version 3.2.2 or later.

Procedure

Step 1 Download the **Cisco Media Services Interface** installation program from the Cisco UC Integration for Microsoft Lync download site on Cisco.com.

Step 2 Install Cisco Media Services Interface on each computer on which you install Cisco UC Integration for Microsoft Lync.
See the appropriate Cisco Medianet documentation for installing Cisco Media Services Interface.

Uninstall Cisco UC Integration for Microsoft Lync

You can uninstall Cisco UC Integration for Microsoft Lync using either the command line or the Microsoft Windows control panel. This topic describes how to uninstall Cisco UC Integration for Microsoft Lync using the command line.

To uninstall Cisco UC Integration for Microsoft Lync with the command line, you can use the MSI or the product code. You should use the MSI if it is available on the file system. However, if the MSI is not available on the file system, you should use the product code.

Procedure

Step 1 Open a command line window.

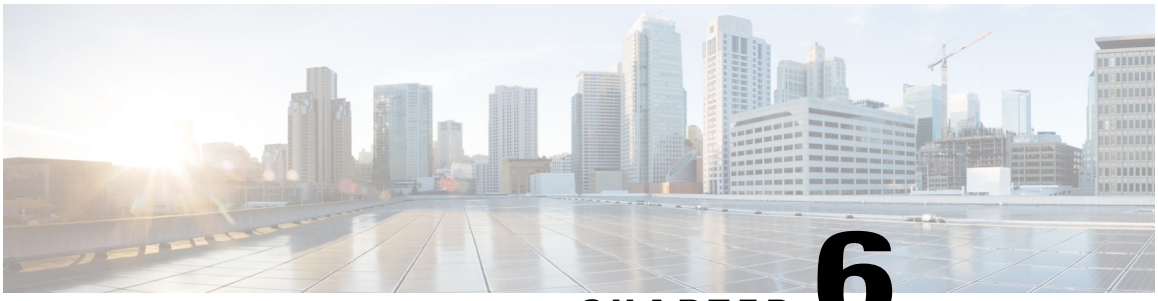
Step 2 Enter one of the following commands to uninstall Cisco UC Integration for Microsoft Lync:

Option	Command

Uninstall with the MSI	`msiexec.exe /x path_to_CUCILyncSetup.msi`
	The following is an example command to uninstall Cisco UC Integration for Microsoft Lync with the MSI:
	`msiexec.exe /x C:\Windows\Installer\CUCILyncSetup.msi /quiet`
	Where /quiet specifies a silent uninstall.

Uninstall with the product code	`msiexec.exe /x product_code`
	The following is an example command to uninstall Cisco UC Integration for Microsoft Lync with the product code:
	`msiexec.exe /x 45992224-D2DE-49BB-B085-6524845321C7 /quiet`
	Where /quiet specifies a silent uninstall.
	To find the product code for Cisco UC Integration for Microsoft Lync, do the following:
	1 Open the Microsoft Windows registry editor.
	2 Locate the following registry key: **HKEY_CLASSES_ROOT\Installer\Products**
	3 Select **Edit** > **Find**.
	4 Enter Cisco UC Integration for Microsoft Lync in the **Find what** text box in the **Find** window and select **Find Next**.
	5 Locate the **ProductIcon** registry key.
	The product code is specified in the value data of the **ProductIcon** registry key as follows:
	`C:\Windows\Installer\{product_code}\ARPPRODUCTICON.exe`.
	Note The product code changes with each version of Cisco UC Integration for Microsoft Lync.

The command removes Cisco UC Integration for Microsoft Lync from the computer.



CHAPTER 6

Configuration

Cisco UC Integration for Microsoft Lync retrieves configuration settings from XML files that reside on your TFTP server. This section helps you to understand when you should create a custom configuration and learn about the different types of configuration files you can create.

Global Configuration Files

Global configuration files apply to all Cisco UC Integration for Microsoft Lync users. Cisco UC Integration for Microsoft Lync downloads the global configuration file from your TFTP server during the login sequence.

Global Configuration File Names

The default name for the global configuration file is `jabber-config.xml`. However, you can specify a unique name for the global configuration file during deployment using the following command line argument:

TFTP_FILE_NAME

See the installation chapter for more information about the command line arguments.

Group Configuration Files

Group configuration files apply to subsets of Cisco UC Integration for Microsoft Lync users. Group configuration files take priority over global configuration files.

Cisco UC Integration for Microsoft Lync retrieves group configuration files after users sign in to their phone account in the client for the first time. Cisco UC Integration for Microsoft Lync then prompts the users to sign out. During the second login sequence, Cisco UC Integration for Microsoft Lync downloads the group configuration file from your TFTP server.

Cisco UC Integration for Microsoft Lync loads group configuration files as follows:

Users are not signed in

1. Users sign in.
2. Users sign out.
3. Users sign in and then Cisco UC Integration for Microsoft Lync loads the group configuration settings.

Users are signed in and use software phones for calls

1. Users are signed in and using their software phones for calls.
2. Users sign out.
3. Users sign in and then Cisco UC Integration for Microsoft Lync loads the group configuration settings.

Users are signed in and use desk phones for calls

1. Users are signed in and using their desk phones for calls.
2. Users sign out.
3. Users sign in and then Cisco UC Integration for Microsoft Lync loads the group configuration settings.

   If users select the option to use software phones for calls before they sign out, Cisco UC Integration for Microsoft Lync notifies the users to sign out and then sign in again to load the group configuration settings.

Group Configuration File Names

You specify the name of the group configuration files in the **Cisco Support Field** on the CSF device configuration in Cisco Unified Communications Manager.

If you remove the name of the group configuration file in the CSF device configuration on Cisco Unified Communications Manager, Cisco UC Integration for Microsoft Lync detects the change, prompts the users to sign out, and loads the global configuration file. You can remove the name of the group configuration file in the CSF device configuration by deleting the entire `configurationFile=group_configuration_file_name.xml` string or by deleting the group configuration filename from the string.

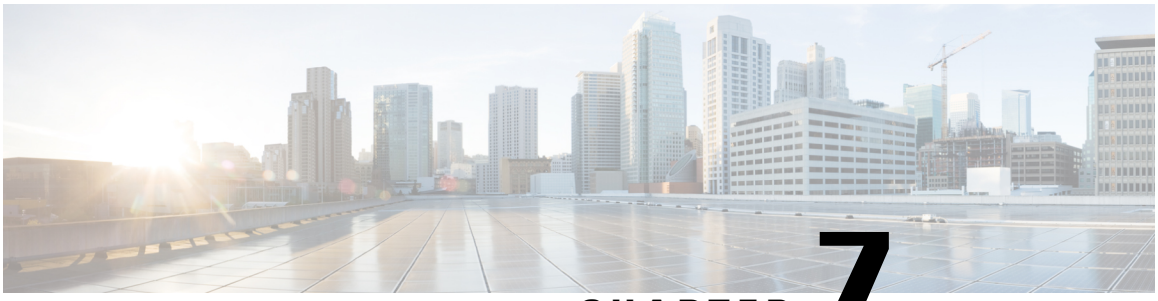
If users have desk phone devices only, use the following command line argument to specify unique names configuration files for different groups:

TFTP_FILE_NAME

See the Installation chapter for more information about the command line arguments.

Configuration File Requirements

- Configuration filenames are case sensitive. Use lowercase letters in the filename to prevent errors and to ensure Cisco UC Integration for Microsoft Lync can retrieve the file from the TFTP server.
- You must use utf-8 encoding for the configuration files.
- Cisco UC Integration for Microsoft Lync cannot read configuration files that do not have a valid XML structure. Ensure you check the structure of your configuration file for closing elements and that elements are nested correctly. Review the examples of configuration files in this chapter for more information.
- Your XML can contain only valid XML character entity references. For example, use `&` instead of `&`. If your XML contains invalid characters, Cisco UC Integration for Microsoft Lync cannot parse the configuration file.
  Open your configuration file in Microsoft Internet Explorer to determine if any characters or entities are not valid. If Internet Explorer displays the entire XML structure, your configuration file does not contain invalid characters or entities. If Internet Explorer displays only part of the XML structure, your configuration file most likely contains invalid characters or entities.



CHAPTER 7

Deployment Configuration

This section describes the parameters used to configure deployments for your corporate environment.

Create Group Configurations

Cisco UC Integration for Microsoft Lync retrieves the names of group configuration files from the CSF device configuration on Cisco Unified Communications Manager.

Restriction If you do not configure CSF devices for users, you cannot apply group configurations to those users.

Before You Begin

You must complete the following steps on Cisco Unified Communications Manager version 8.6.x or lower:

1. Download the Cisco UC Integration for Microsoft Lync administration package from Cisco.com.
2. Copy `ciscocm.addcsfsupportfield.cop` from the administration package to your file system.
3. Deploy `ciscocm.addcsfsupportfield.cop` on Cisco Unified Communications Manager.

   See the Cisco Unified Communications Manager documentation for instructions on deploying COP files.

The **Cisco Support Field** field is available for CSF devices in the **Desktop Client Settings** section on the **Phone Configuration** window in Cisco Unified Communications Manager.

Procedure

Step 1 Create an XML group configuration file with any text editor.
The group configuration file can have any appropriate name; for example, `cucilync-groupa-config.xml`.

- Use lowercase letters in the filename.
- Use utf-8 encoding.

Step 2 Define the required configuration parameters in the group configuration file.

Important If the structure of your configuration file is not valid, Cisco UC Integration for Microsoft Lync cannot read the settings you define. See the sample XML in this chapter for an example of the structure your configuration file must have.

Step 3 Host the group configuration file on your TFTP server.

a) Open the **Cisco Unified OS Administration** interface.
b) Select **Software Upgrades** > **TFTP File Management**.
c) Select **Upload File**.
d) Select **Browse** in the **Upload File** section.
e) Select the group configuration file on the file system.
f) Do not specify a value in the **Directory** text box in the **Upload File** section.
If you specify a value for the **Directory** text box, make a note of the value. You must specify the path and filename when you specify the group configuration file in the CSF device configuration on Cisco Unified Communications Manager.
g) Select **Upload File**.

Step 4 Specify the name of the group configuration file in the **Cisco Support Field** field.

Timesaver Use the Bulk Administration Tool for multiple users.

a) Open the **Cisco Unified CM Administration** interface.
b) Select **Device** > **Phone**.
c) Find and select the appropriate CSF device to which the group configuration applies.
d) Locate the **Product Specific Configuration Layout** section of the **Phone Configuration** window.
e) Locate the **Desktop Client Settings** section.
f) Enter `configurationfile=`*`group_configuration_file_name.xml`* in the **Cisco Support Field** field; for example, `configurationfile=cucilync-groupa-config.xml`

Note Use a semicolon to delimit multiple entries in the **Cisco Support Field** field. However, do not specify multiple group configuration files. If you specify multiple group configuration files, Cisco UC Integration for Microsoft Lync uses the first group configuration available.

If you host the group configuration file on your TFTP server in a location other than the default directory, you must specify the path and the filename in the **Cisco Support Field** field; for example, `configurationfile=/customFolder/cucilync-groupa-config.xml`.

g) Select **Save**.

Create Global Configurations

This topic provides a high-level overview of the steps to create a global configuration file and explains how to host the file on your TFTP server.

Procedure

Step 1 Create a file named `jabber-config.xml` with any text editor.

Remember
- Use lowercase letters in the filename.
- Use utf-8 encoding.

Step 2 Define the required configuration parameters in `jabber-config.xml`.

Important If the structure of your configuration file is not valid, Cisco UC Integration for Microsoft Lync cannot read the settings you define. See the sample XML in this chapter for an example of the structure your configuration file must have.

Step 3 Host `jabber-config.xml` on your TFTP server.

a) Open the **Cisco Unified OS Administration** interface on Cisco Unified Communications Manager.
b) Select **Software Upgrades** > **TFTP File Management**.
c) Select **Upload File**.
d) Select **Browse** in the **Upload File** section.
e) Select `jabber-config.xml` on the file system.
f) Do not specify a value in the **Directory** text box in the **Upload File** section.
Leave the value of the **Directory** text box empty to host `jabber-config.xml` in the default directory of your TFTP server.
If you host `jabber-config.xml` in a directory other than the default directory, you must specify the path and filename as the value of the following command line argument during deployment: TFTP_FILE_NAME.
g) Select **Upload File**.

Restart Your TFTP Server

You must restart your TFTP server before Cisco UC Integration for Microsoft Lync can access the configuration files.

Procedure

Step 1 Open the **Cisco Unified Serviceability** interface on Cisco Unified Communications Manager.

Step 2 Select **Tools** > **Control Center - Feature Services**.

Step 3 Select **Cisco Tftp** from the **CM Services** section.

Step 4 Select **Restart**.
A window displays to prompt you to confirm the restart.

Step 5 Select **OK**.
The **Cisco Tftp Service Restart Operation was Successful** status displays.

Step 6 Select **Refresh** to ensure the **Cisco Tftp** service starts successfully.

What to Do Next

To verify that the configuration file is available on your TFTP server, open the configuration file in any browser. Typically, you can access the global configuration file at the following URL:
`http://tftp_server_address:6970/jabber-config.xml`

Configuration File Structure

XML Structure

The following XML snippet shows the basic structure of a configuration file:

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
 <Client>
  <parameter_name>value</parameter_name>
 </Client>
 <Options>
  <parameter_name>value</parameter_name>
 </Options>
 <Policies>
  <parameter_name>value</parameter_name>
 </Policies>
 <Phone>
  <parameter_name>value</parameter_name>
 </Phone>
</config>
```

The following table describes the elements in the basic structure of a configuration file:

Element	Description
<?xml version="1.0" encoding="utf-8"?>	XML declaration. Your configuration file must conform to the standard XML format.

Element	Description
config	Root element of the configuration XML that contains the available configuration groups. The root element must also contain the version attribute.
Client	Parent element that contains client configuration parameters.
Directory	Parent element that contains directory configuration parameters.
Options	Parent element that contains user option configuration parameters for user options.
Policies	Parent element that contains policy configuration parameters.

Client Parameters

Parameter	Value	Description
PrtLogServerUrl	URL	Specifies the custom script for submitting problem reports. For more information about problem reports, see *Configure Problem Reporting*.

Client Configuration Example

The following is an example client configuration:

```
<Client>
 <PrtLogServerUrl>http://server_name.cisco.com/cucilync/prt/my_script.php</PrtLogServerUrl>
</Client>
```

Directory Attribute Mapping Parameters

You can change the default attribute mappings for Cisco UC Integration for Microsoft Lync. For example, by default, Cisco UC Integration for Microsoft Lync maps the BusinessPhone parameter to the telephoneNumber attribute in your directory. The result of this mapping is that Cisco UC Integration for Microsoft Lync retrieves the value of the telephoneNumber attribute from your directory for a particular user. Cisco UC Integration for Microsoft Lync then displays this value as the user's work phone in that user's profile. If your organization uses an attribute other than telephoneNumber for business phone numbers, you should change the mapping in the configuration file.

The following table describes the parameters for mapping directory attributes:

Parameter	Default Value
CommonName	cn
DisplayName	displayName

Parameter	Default Value
Firstname	givenName
Lastname	sn
EmailAddress	mail
SipUri	msRTCSIP-PrimaryUserAddress
PhotoSource	thumbnailPhoto
BusinessPhone	telephoneNumber
MobilePhone	mobile
HomePhone	homePhone
OtherPhone	otherTelephone
Title	title
CompanyName	company
UserAccountName	sAMAccountName
DomainName	userPrincipalName
Location	co
Nickname	nickname
PostalCode	postalCode
State	st
StreetAddress	streetAddress

Directory Connection Parameters

The following table describes parameters for configuring your directory connection:

Parameter	Value	Description
ConnectionType	0 1	Specifies if Cisco UC Integration for Microsoft Lyncconnects to a Global Catalog server or Domain Controller. **0** Connect to a Global Catalog server. This is the default value. **1** Connect to a Domain Controller server.

Parameter	Value	Description
PrimaryServerName	Fully qualified domain name IP address	Specifies the fully qualified domain name or IP address of the primary server connection for directory access. You must specify this parameter if Cisco UC Integration for Microsoft Lync cannot automatically discover the primary server.
SecondaryServerName	Fully qualified domain name IP address	Specifies the fully qualified domain name or IP address of the backup server connection for directory access. You must specify this parameter if Cisco UC Integration for Microsoft Lync cannot automatically discover the backup server.
ServerPort1	Port number	Specifies the primary server port. You must specify this parameter if Cisco UC Integration for Microsoft Lync cannot automatically discover the primary server.
ServerPort2	Port number	Specifies the backup server port. You must specify this parameter if Cisco UC Integration for Microsoft Lync cannot automatically discover the backup server.
UseWindowsCredentials	0 1	Specifies if Cisco UC Integration for Microsoft Lync uses Microsoft Windows user names and passwords. **0** Use credentials you specify as the values for the ConnectionUsername and ConnectionPassword parameters. **1** Use Microsoft Windows credentials. This is the default value.

Parameter	Value	Description
ConnectionUsername	Username	Specifies a username to connect to the directory server. **Important** The client transmits and stores this username as plain text. Using this parameter is not a secure method of authenticating with the directory server. In most deployment scenarios, you do not need to specify a username to connect to the directory server. This parameter enables you to authenticate with a directory server that requires a well-known or public set of credentials. You should include this parameter in the client configuration only if it is not possible to authenticate with the directory server with the user's credentials.
ConnectionPassword	Password	Specifies a password to connect to the directory server. **Important** The client transmits and stores this password as plain text. Using this parameter is not a secure method of authenticating with the directory server. In most deployment scenarios, you do not need to specify a password to connect to the directory server. This parameter enables you to authenticate with a directory server that requires a well-known or public set of credentials. You should include this parameter in the client configuration only if it is not possible to authenticate with the directory server with the user's credentials.
UseSSL	0 1	Specifies if Cisco UC Integration for Microsoft Lync uses SSL for secure connections to the directory. **0** Disable SSL. This is the default value. **1** Enable SSL.

Parameter	Value	Description
UseSecureConnection	0 1	Specifies if Cisco UC Integration for Microsoft Lync uses simple authentication for the connection to the directory service. **0** Use simple authentication. This is the default value. **1** Do not use simple authentication.

Directory Query Parameters

The following table describes parameters for configuring how Cisco UC Integration for Microsoft Lync queries your directory:

Parameter	Value	Description
BaseFilter	Base filter	Specifies a base filter for Active Directory queries. Specify a directory subkey name only to retrieve objects other than user objects when you query Active Directory. The default value is (&(objectCategory=person). Configuration files can contain only valid XML character entity references. Use `&amp;` instead of `&` if you specify a custom base filter. In some cases, base filters do not return query results if you specify a closing bracket in your Cisco UC Integration for Microsoft Lync configuration file. For example, this issue might occur if you specify the following base filter: (&(memberOf=CN=UCFilterGroup,OU=DN)) To resolve this issue, remove the closing bracket; for example, (&(memberOf=CN=UCFilterGroup,OU=DN)

Parameter	Value	Description
PredictiveSearchFilter	Search filter	Defines a filter to apply to predictive search queries. The default value is anr= When Cisco UC Integration for Microsoft Lync performs a predictive search, it issues a query using Ambiguous Name Resolution (ANR). This query disambiguates the search string and returns results that match the attributes that are set for ANR on your directory server. **Important** If you want Cisco UC Integration for Microsoft Lync to search for attributes that are not set for ANR, you must configure your directory server to set those attributes for ANR. See the following Microsoft documentation for more information on ANR: • *Ambiguous Name Resolution for LDAP in Windows 2000* • *LDAP Referrals*, see the *Ambiguous Name Resolution* section • *Common Default Attributes Set for Active Directory and Global Catalog*
DisableSecondaryNumberLookups	0 1	Specifies whether users can search for alternative contact numbers if the work number is not available, such as the mobile, home, or other number. **0** Users can search for alternative contact numbers. This is the default value. **1** Users cannot search for alternative contact numbers.

Parameter	Value	Description
PhoneNumberMasks	Mask string	Specifies masks to use when users search for phone numbers. For example, a user receives a call from +14085550100. However, this number in Active Directory is +(1) 408 555 0100. The following mask ensures that the contact is found: +14081+(#) ### ### #### The length of mask strings cannot exceed the size restriction for registry subkey names.
SearchTimeout	Number of seconds	Specifies the timeout period for queries in seconds. The default value is 5.
UseWildcards	0 1	Specifies whether to enable wildcard searches. **0** Do not use wildcards. This is the default value. **1** Use wildcards. If you set 1 as the value, the speed of searches on the LDAP might be affected, especially if users search for directory attributes that are not indexed. You can use phone number masks instead of wildcard searches.

Parameter	Value	Description
SearchBase1 SearchBase2 SearchBase3 SearchBase4 SearchBase5	Searchable organizational unit (OU) in the directory tree	Specifies a location in the directory server from which searches begin. In other words, a search base is the root from which Cisco UC Integration for Microsoft Lync executes a search. By default, Cisco UC Integration for Microsoft Lync searches from the root of the directory tree. You can specify the value of up to five search bases in your OU to override the default behavior. **Important** • Active Directory does not typically require you to specify a search base. If you use Active Directory, you should specify search bases only if you have specific performance requirements. • You must specify a search base for directory servers other than Active Directory. Directory servers other than Active Directory require search bases to create a binding to a specific location in the directory. **Tip** You can specify an OU to restrict searches to certain user groups. For example, if you want to search only for users who have instant messaging enabled, you can include those users in an OU and then specify that as the value of a search base.

Phone Masks

You can set masks to use when Cisco UC Integration for Microsoft Lync searches your directory for a phone number with the PhoneNumberMasks parameter.

Phone masks apply to phone numbers before Cisco UC Integration for Microsoft Lync searches your directory. If you configure phone masks correctly, directory searches succeed as exact query matches and prevent any impact to performance of your directory server.

The following table describes the elements you can include in a phone mask:

Element	Description
Phone number pattern	Provides a number pattern to retrieve phone numbers from your directory. To add a phone mask, you specify a number pattern that applies to the mask. For example, to specify a mask for searches that begin with +1408, you can use the following mask: +1408|+(#) ### ### #### To enable a mask to process phone numbers that have the same number of digits, but different patterns, use multiple masks with the same number of digits. For example, your company has site A and site B. Each site maintains a separate directory in which the phone numbers have different formats, such as the following: +(1) 408 555 0100 +1-510-5550101 The following mask ensures you can use both numbers correctly: +1408|+(#) ### ### ####|+1510|+#-###-########.
Pipe symbol (|)	Separates number patterns and masks. For example, +1408|+(#) ### ### ####|+34|+(##) ### ####.
Wildcard character	Substitutes one or more characters for a subset of possible matching characters. Any wildcard character can exist in a phone mask. For example, an asterisk (*****) represents one or more characters and can apply to a mask as follows: +3498|+##*##*###*####. Using this mask with the wildcard, a phone number search can match any of the following formats: +34(98)555 0199 +34 98 555-0199 +34-(98)-555.0199
Reverse mask	Applies a number pattern from right to left. For example, a mask of +3498|R+34 (98) 559 #### applied to +34985590199 results in +34 (98) 559 0199. You can use both forward and reverse masks.

Contact Resolution

Contact Resolution Parameters

The following table describes parameters for configuring intradomain federation:

Parameter	Value	Description
UseSIPURIToResolveContacts	true false	Specifies whether Cisco UC Integration for Microsoft Lync retrieves contact information using the value of the attribute you specify in the SipUri parameter. **true** Retrieve contact information using the value of the attribute you specify in the SipUri parameter. You should specify true if the contact user names in your directory do not conform to the following format *username@domain*. **false** Cisco UC Integration for Microsoft Lync does not use the SipUri parameter. This is the default value.
UriPrefix	Text string	Defines the prefix that applies to the value of the attribute you specify in the SipUri parameter. The prefix is any text that exists before the username of the contact ID. For example, you specify msRTCSIP-PrimaryUserAddress as the value of SipUri. In your directory the value of the msRTCSIP-PrimaryUserAddress attribute has the following format: `sip:username@domain`. The default value is blank.
PresenceDomain	Text string	Specifies the domain name used for creating instant messaging addresses for directory contacts. `username@domain`

Note The Active Directory attribute msRTCSIP-PrimaryUserAddress must contain the SIP URI in the format sip:username@domain and the configuration file must have the following entry in the Directory section for contact resolution to perform properly.

```
<Directory>
  <UseSIPURIToResolveContacts>true</UseSIPURIToResolveContacts>
  <SipUri>msRTCSIP-PrimaryUserAddress</SipUri>
  <UriPrefix>sip:</UriPrefix>
  <PresenceDomain>example.com</PresenceDomain>
</Directory>
```

Phone Parameters

The following table describes the parameters you can specify within the Phone element:

Parameter	Value	Description
TFTPServer1	IP address Hostname FQDN	Specifies the address of your TFTP server. Set one of the following as the value: **Hostname** For example, hostname **IP address** For example, 123.45.254.1 **Fully qualified domain name** For example, hostname.domain.com
CtiServer1	IP address Hostname FQDN	Specifies the address of your CTI server. This parameter is required only if the address of your CTI server is not the same as the address of your TFTP server. If both server addresses are the same, you do not need to specify this parameter in your configuration file.
CcmcipServer1	IP address Hostname FQDN	Specifies the address of your CCMCIP server. This parameter is required only if the address of your CCMCIP server is not the same as the address of your TFTP server. If both server addresses are the same, you do not need to specify this parameter in your configuration file.

Phone Configuration Example

The following is an example phone configuration:

```
<Phone>
 <TftpServer1>tftpserver.domain.com</TftpServer1>
 <CtiServer1>ctiserver.domain.com</CtiServer1>
</Phone>
```

Registry Key Configuration

The application supports obtaining the location of TFTP and CCMCIP servers from the Microsoft Windows registry. The following registry values can be used to specify these servers:

- `CcmcipServer1`
- `CcmcipServer2`
- `TftpServer1`
- `TftpServer2`

The application will first search for these values in `HKEY_CURRENT_USER\Software\Cisco Systems, Inc.\Client Services Framework\AdminData` and then `HKEY_CURRENT_USER\Software\Policies\Cisco Systems, Inc.\Client Services Framework\AdminData`. Values located in these registry keys will override information specified in the configuration file. Values will be read from the configuration file if they cannot be found in either of these registry locations.

Note Configuration through the registry is only supported with these four values.

Internet Explorer Pop-up Parameters

A new Internet Explorer window or tab can be opened to display information about an incoming caller. This information is displayed after the incoming call is accepted. The behavior of the new window or tab and the information it displays are controlled using the configuration file. The following table lists the parameters used to display the new window or tab.

Parameter	Value	Description
BrowserContactURI		The base URI used to open Internet Explorer. Must have an `%ID%` key marker.
BrowserFallbackURI		A fall back URI used when the **BrowserIDType** information does not arrive within a period of time.
BrowserBehavior	The behavior of the browser when opening new URIs.	
	NewTab	Open the URI in a new tab if available. Open a new browser window if tabs are not supported.
	Navigate	Navigate to the new URI in the browser window already open.
	NewWindow	Always open a URI in a new browser window.

Parameter	Value	Description
BrowserIDType	The type of ID supplied to the URI defined in the registry.	
	CallNumber	The media address of the participant
	CallDisplayName	The display name of the participant
	ContactBusinessNumber	The business number of the contact
	ContactMobileNumber	The mobile number of the contact
	ContactHomeNumber	The home number of the contact
	ContactOtherNumber	The other number of the contact
	ContactDisplayName	The display name of the contact
	ContactURI	The URI of the contact (user@domain.com for example)
	ContactEmail	The email of the contact (email@work.com for example)
	ContactUsername	The user logon name of the contact.
BrowserIDFilter	Regular expression	A filter applied to the chosen **BrowserIDType** that will prevent a new browser window or tab if a match is made. The following are examples of regular expressions: • Phone number that has four digits and doesn't start with number 7: **(?!7)\d{4}** • Phone number that doesn't start with the digits 1, 2, 3 or 4: **[-90]\d+** • Phone number that doesn't end with 49: **\d+(?!49)\d{2}** Any valid regular expression supported by the Microsoft **std::tr1::regex** library can be used.

Note the following items when implementing this feature:

- A new browser window or tab is displayed when the user accepts a transferred call from an established incoming call.
- A new browser window or tab is displayed for each additional, unique call participant added to a conference call.

- A filter can be created that controls when a browser window or tab is opened. This enables the identification of internal and external contacts. This feature is typically implemented to display information about an external contact. This can be achieved by:

  1 Creating a regular expression that distinguishes internal and external contacts.

  2 Applying the regular expression to the incoming caller ID (typically the phone number).

  3 Opening the new browser window or tab when the regular expression is matched for an external contact.

Important This feature can only be implemented with Microsoft Internet Explorer 7.0, 8.0, or 9.0. No other browser is supported.

Example

The following examples demonstrate configuration file entries for this feature.

```
<BrowserPop>
            <BrowserContactURI>www.example.com/%ID%.html</BrowserContactURI>
            <BrowserIDType>ContactUsername</BrowserIDType>
            <BrowserFallbackURI>www.example.com</BrowserFallbackURI>
            <BrowserBehavior>NewTab</BrowserBehavior>
</BrowserPop>

 <BrowserPop>
            <BrowserContactURI>www.example.com/%ID%.html</BrowserContactURI>
            <BrowserIDType>ContactEmail</BrowserIDType>
            <BrowserFallbackURI>www.example.com</BrowserFallbackURI>
            <BrowserBehavior>NewWindow</BrowserBehavior>
 </BrowserPop>

 <BrowserPop>
            <BrowserContactURI>www.example.com/%ID%.html</BrowserContactURI>
            <BrowserIDType>CallNumber</BrowserIDType>
            <BrowserIDFilter>[^7]\d{3}</BrowserIDFilter>
            <BrowserFallbackURI>www.example.com</BrowserFallbackURI>
            <BrowserBehavior>Navigate</BrowserBehavior>
 </BrowserPop>
```

Configure Automatic Updates

To enable automatic updates, you create an XML file that contains the information for the most recent version, including the URL of the installation package on the HTTP server. Cisco UC Integration for Microsoft Lync retrieves the XML file when users sign in, resume their computer from sleep mode, or perform a manual update request from the **Help** menu.

The XML file for automatic updates uses the following format:

```
<JabberUpdate>
 <LatestBuildNum>value</LatestBuildNum>
 <LatestVersion>value</LatestVersion>
 <Message><![CDATA[your_html]]></Message>
 <DownloadURL>value</DownloadURL>
</JabberUpdate>
```

Before You Begin

To configure automatic updates for Cisco UC Integration for Microsoft Lync, you must have an HTTP server installed and configured to host the XML file and installation package.

Procedure

Step 1 Host the appropriate installation package on your HTTP server.
Step 2 Create an update XML file with any text editor.
Step 3 Specify the build number of the update as the value of the LatestBuildNum element.
Step 4 Specify the version number of the update as the value of the LatestVersion element.
Step 5 Specify HTML as the value of the Message element in the format: `<![CDATA[your_html]]>`
Step 6 Specify the URL of the installation package on your HTTP server as the value of the DownloadURL element.
Step 7 Save and close your update XML file.
Step 8 Host your update XML file on your HTTP server.
Step 9 Specify the URL of your update XML file as the value of the UpdateUrl parameter in your configuration file.

The following is an example of XML to configure automatic updates:

```
<JabberUpdate>
 <LatestBuildNum>12345</LatestBuildNum>
 <LatestVersion>9.2.1</LatestVersion>
 <Message><![CDATA[<b>This new version of Cisco UC Integration for Microsoft Lync lets you
 do the following:</b><ul><li>Feature 1</li><li>Feature 2</li></ul>For
more information click <a target="_blank"
href="http://cisco.com/go/cucilync">here</a>.]]></Message>
 <DownloadURL>http://server_name/CUCILyncSetup.msi</DownloadURL>
</JabberUpdate>
```

Configure Problem Reporting

Setting up problem reporting enables users to send a summary of issues that they encounter while using Cisco UC Integration for Microsoft Lync. There are two methods for submitting problem reports as follows:

- Users submit the problem report directly through Cisco UC Integration for Microsoft Lync.
- Users save the problem report locally and then upload it at a later time.

Cisco UC Integration for Microsoft Lync uses an HTTP POST method to submit problem reports. Create a custom script to accept the POST request and specify the URL of the script on your HTTP server as a configuration parameter. Because users can save problem reports locally, you should also create an HTML page with a form to enable users to upload problem reports.

Before You Begin

Complete the following steps to prepare your environment:

1. Install and configure an HTTP server.
2. Create a custom script to accept the HTTP POST request.

3 Create an HTML page to host on the HTTP server to enable users to upload problem reports that are saved locally. Your HTML page should contain a form that accepts the problem report saved as a `.ZIP` archive and contains an action to post the problem report using your custom script.

The following is an example form that accepts problem reports:

```
<form name="uploadPrt" action="http://server_name.com/scripts/UploadPrt.php" method="post"
 enctype="multipart/form-data">
 <input type="file" name="zipFileName" id="zipFileName" /><br />
 <input type="submit" name="submitBtn" id="submitBtn" value="Upload File" />
</form>
```

Procedure

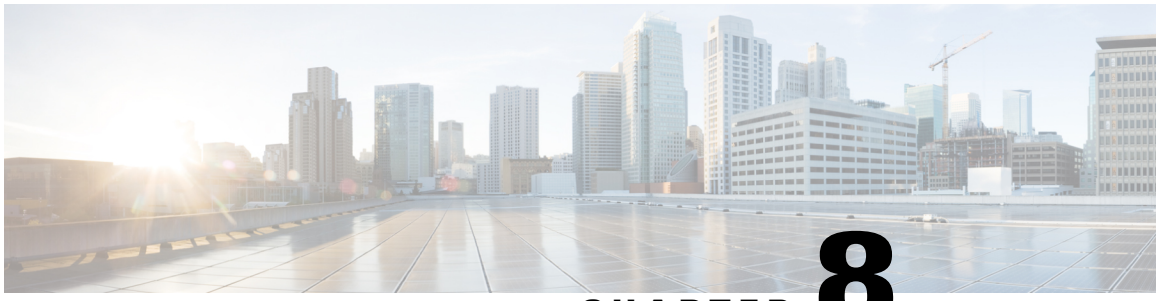
Step 1 Host your custom script on your HTTP server.

Step 2 Specify the URL of your script as the value of the PrtLogServerUrl parameter in your configuration file.

Configuration File Example

The following is an example of a configuration file.

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
  <Client>
    <PrtLogServerUrl>http://server_name.domain.com/prt_script.php</PrtLogServerUrl>
    <UpdateUrl>http://server_name.domain.com/update.xml</UpdateUrl>
    <Forgot_Password_URL>http://server_name.domain.com/password.html</Forgot_Password_URL>
  </Client>
  <Directory>
    <DirectoryServerType>EDI</DirectoryServerType>
    <BusinessPhone>aNonDefaultTelephoneNumberAttribute</BusinessPhone>
    <PhotoUriSubstitutionEnabled>true</PhotoUriSubstitutionEnabled>
    <PhotoUriSubstitutionToken>cn</PhotoUriSubstitutionToken>
    <PhotoUriWithToken>http://staffphoto.example.com/cn.jpg</PhotoUriWithToken>
  </Directory>
</config>
```



CHAPTER 8

Troubleshoot Cisco UC Integration for Microsoft Lync

The section contains information on resolving common issues with Cisco UC Integration for Microsoft Lync.

Configuration Issues

TFTP and CCMCIP Server Configuration Not Working

Problem description: The TFTP and CCMCIP server values specified in the configuration file are not used by the application.

Resolution: The TFTP and CCMCIP servers can be configured using the configuration file or through registry key settings. Ensure that the misconfigured values are not specified in a registry setting. Registry key values for the TFTP and CCMCIP servers take precedence over the configuration file on a key by key basis. See Phone Parameters, on page 87 for more information on this feature. Registry key values for TFTP and CCMCIP servers are only supported at this time.

Configuration File Does Not Download

Problem description: Cisco UC Integration for Microsoft Lync does not download the configuration file from the TFTP server. The configuration file is not available in the installation directory after you start Cisco UC Integration for Microsoft Lync.

Resolution:

1. Restart your TFTP server.
2. Check the name of your configuration file.

Remember

- The name of the configuration file is case sensitive.
- The global configuration filename must be `jabber-config.xml`.

3 Ensure your corporate firewall does not prevent Cisco UC Integration for Microsoft Lync from downloading the configuration file.

4 Host the configuration file on your TFTP server as follows:

a Open the **Cisco Unified OS Administration** interface.
b Select **Software Upgrades** > **TFTP File Management**.
c Select **Upload File**.
d Select **Browse** in the **Upload File** section.
e Select the configuration file on the file system.
f Leave the value of the **Directory** text box empty to host the configuration file in the default directory of your TFTP server.
g Select **Upload File**.

Cisco UC Integration for Microsoft Lync Does Not Read the Configuration File

Problem description: You host a global or group configuration file on your TFTP server. Cisco UC Integration for Microsoft Lync downloads the configuration file and saves it in the appropriate installation directory. However, Cisco UC Integration for Microsoft Lync does not apply any settings you specify in the configuration file.

Resolution: Ensure the XML in the configuration file is valid. Cisco UC Integration for Microsoft Lync configuration files must do the following:

- Use utf-8 encoding.
- Contain only valid XML character entities. For example, use `&` instead of `&`.
  Open your configuration file in Microsoft Internet Explorer to determine if any characters or entities are not valid. If Internet Explorer displays the entire XML structure, your configuration file does not contain invalid characters or entities. If Internet Explorer displays only part of the XML structure, your configuration file most likely contains invalid characters or entities.
- Contain a valid structure. Ensure parameters are nested under the correct elements. The following XML snippet shows the basic structure of a configuration file:

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
 <Client>
  <parameter_name>value</parameter_name>
 </Client>
 <Directory>
  <parameter_name>value</parameter_name>
 </Directory>
 <Policies>
  <parameter_name>value</parameter_name>
 </Policies>
</config>
```

Cisco UC Integration for Microsoft Lync Uses Old Configuration Settings

Problem description: Cisco UC Integration for Microsoft Lync is not using the current configuration settings. You change settings in a configuration file and host it on your TFTP server. However, Cisco UC Integration for Microsoft Lync uses the settings from the previous version of the configuration file.

Resolution:

1. Restart your TFTP server.
2. Open the configuration file in your browser to verify the settings. Typically, you can access the configuration file at the following URL: `http://tftp_server_address:6970/jabber-config.xml`

If restarting your TFTP server does not resolve this issue, it is likely that Cisco UC Integration for Microsoft Lync uses the cached configuration file because it cannot download the current version.

Contacts in Microsoft Outlook Do Not Display in Search

Problem description: Contacts in Microsoft Outlook do not display in search results.

Resolution: Review the following requirements to ensure users can search for and communicate with Microsoft Outlook contacts:

- To search for local contacts in Microsoft Outlook using Cisco UC Integration for Microsoft Lync, users must have profiles set in Microsoft Outlook.
- To add local contacts in Microsoft Outlook to contact lists in Cisco UC Integration for Microsoft Lync, user profiles must have email or instant message addresses.
- To communicate with local contacts in Microsoft Outlook using Cisco UC Integration for Microsoft Lync, user profiles must contain the relevant details. For example, to send instant messages to contacts in Microsoft Outlook, the user profiles must have email or instant message addresses. Likewise, to call contacts in Microsoft Outlook, the user profiles must contain phone numbers.

Directory Integration Issues

Cannot Determine If a Directory Connection is Established

Problem description: You specify directory settings in a Cisco UC Integration for Microsoft Lyncconfiguration file. However, you are not sure whether Cisco UC Integration for Microsoft Lync is successfully connected to the directory.

Resolution: Perform the following steps to determine whether Cisco UC Integration for Microsoft Lync is connected to the directory:

1. Start the client.
2. Enter at least three characters in the search field.

If Cisco UC Integration for Microsoft Lync displays a list of matching contacts, search is working. Cisco UC Integration for Microsoft Lync is successfully connected to the directory.

If Cisco UC Integration for Microsoft Lync is not successfully connected to the directory, review the configuration settings. By default, the client uses Enhanced Directory Integration and connects to a Global Catalog server.

ADSI Error Codes

Cisco UC Integration for Microsoft Lync uses Microsoft Active Directory Service Interfaces (ADSI) for directory integration. You should refer to the ADSI error codes to help troubleshoot directory integration issues.

See the following Microsoft documentation for information about ADSI error codes:

- *ADSI Error Codes* at http://msdn.microsoft.com/en-us/library/windows/desktop/aa772195(v=vs.85).aspx
- *Generic ADSI Error Codes* at http://msdn.microsoft.com/en-us/library/windows/desktop/aa705940(v=vs.85).aspx
- *Error Codes for ADSI 2.5* at http://support.microsoft.com/kb/242076

Audio, Video, and Device Issues

Note The section contains information on troubleshooting audio, video, and device issues related to Cisco UC Integration for Microsoft Lync. Refer to the Microsoft Lync documentation for troubleshooting issues related to Microsoft Lync.

Microsoft Lync Devices Are Not Available

Devices configured in Microsoft Lync must be independently configured in Cisco UC Integration for Microsoft Lync.

Audio and Video Communication is Not Available

Problem description: You provision audio and video devices, but cannot connect to the devices.

Resolution: Ensure you set up a CTI gateway and create a CCMCIP profile on Cisco Unified Communications Manager as appropriate.

Voicemail Prompt is Truncated

Problem description: The start of voicemail prompts is truncated.

The start of the audio that prompts users to leave voicemail messages can be truncated in some instances. The result of the truncation is that users do not hear the first second or two of the voicemail prompt.

Resolution

To resolve this issue, set a value for the **Delay After Answer** field in the Cisco Unity Connection advanced telephony integration settings. See the Cisco Unity Connection documentation at: http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/gui_reference/guide/8xcucgrg120.html#wp1056978

End Users Cannot Retrieve Phone Account Details

Problem description: Cisco UC Integration for Microsoft Lync users cannot retrieve phone account details when they log in to an extension mobility profile. As a result, error messages display in the **Phone services** section of the **Phone accounts** tab on the **Options** dialog box.

The affected users have multiple devices configured on Cisco Unified Communications Manager.

The following exceptions are written to the csf-unified.log file in the `%USER_PROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\Logs` directory:

```
<time_stamp> DEBUG [0x00001d80] [src\config\CCMCIPClient.cpp(230)] [csf.ecc]
[curlDebugCallback] -
<html>
<body>
org.apache.jasper.JasperException: java.lang.reflect.InvocationTargetException<br>
<!--
org.apache.jasper.JasperException: java.lang.reflect.InvocationTargetException
at
org.apache.jasper.runtime.JspRuntimeLibrary.handleSetPropertyExpression(JspRuntimeLibrary.java:622)
at
org.apache.jsp.ControlledDevices_jsp._jspx_meth_c_005fforEach_005f0(ControlledDevices_jsp.java:834)
at org.apache.jsp.ControlledDevices_jsp._jspService(ControlledDevices_jsp.java:180)
at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
at javax.servlet.http.HttpServlet.service(HttpServlet.java:722)
```

Resolution: To resolve this issue, do the following:

1. Disassociate the affected users from all extension mobility profiles.
2. Contact your Cisco support representative and request an Engineering Special (ES) to resolve this issue on Cisco Unified Communications Manager.

After you apply the ES on Cisco Unified Communications Manager, you can re-associate the affected users with the extension mobility profiles.

Off Hook Dialing Does Not Change Presence States

Problem description: A Cisco UC Integration for Microsoft Lync user dials a number directly from the desk phone, or other device. The availability status does not change to indicate the user is on a call.

Resolution: To resolve this issue, do the following:

1. Ensure the user is associated with the line number.
    1. Open Cisco Unified Communications Manager and browse to the **Phone Configuration** window for the device.
    2. Locate the **Association Information** section and select the line associated with the device. The **Directory Number Configuration** window opens.
    3. Locate the **Users Associated with Line** section.
    4. Verify that the user is associate with the line.
2. Ensure the SIP trunk exists from Cisco Unified Communications Manager to Cisco Unified Presence.
    1. Open Cisco Unified Communications Manager.
    2. Select **Device** > **Trunk**.
    3. Search for a SIP trunk to Cisco Unified Presence.
    4. Create a SIP trunk if one does not exist.

Calls Drop Intermittently on Network Profile Change

Problem description: Audio and video calls drop intermittently when the network profile changes.

A known bug exists with Microsoft Windows 7 and Microsoft Windows Server 2008 R2 that causes the network profile to change unexpectedly. This change in the network profile closes network ports that Cisco UC Integration for Microsoft Lync requires for calls. As a result, if you are on a call when the network profile changes, that call automatically terminates.

Resolution: Apply the fix available from the Microsoft support site at: http://support.microsoft.com/kb/2524478/en-us