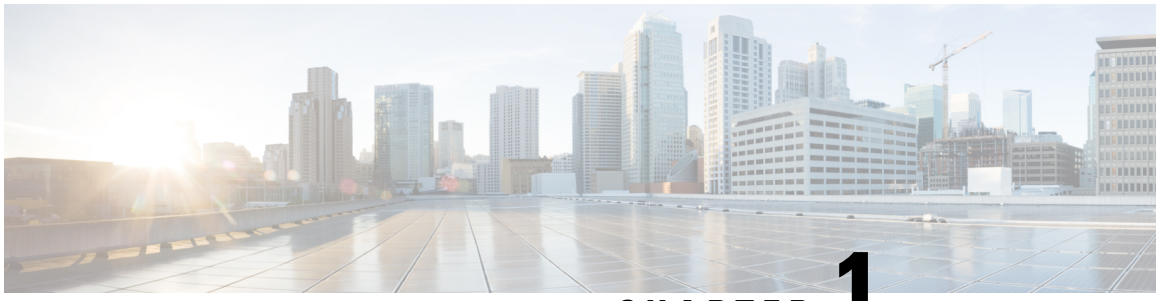
Cisco UC Integration for Microsoft Lync 10.6 Administration Guide

First Published: 2015-02-26

Last Modified: 2015-05-18

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

Overview

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 Internet Explorer, Microsoft Outlook and other Microsoft Office applications.
- Start a Cisco WebEx meeting from the contact list, a conversation, or a Microsoft Lync instant messaging session.
- Expressway Mobile and Remote Access
- Service Discovery

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/c/en/us/support/unified-communications/uc-integration-tm-microsoft-lync/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.

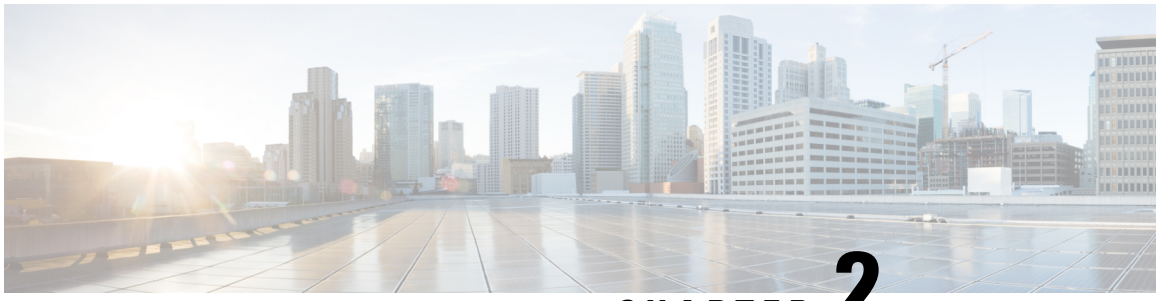
https://supportforums.cisco.com/community/netpro/collaboration-voice-video

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



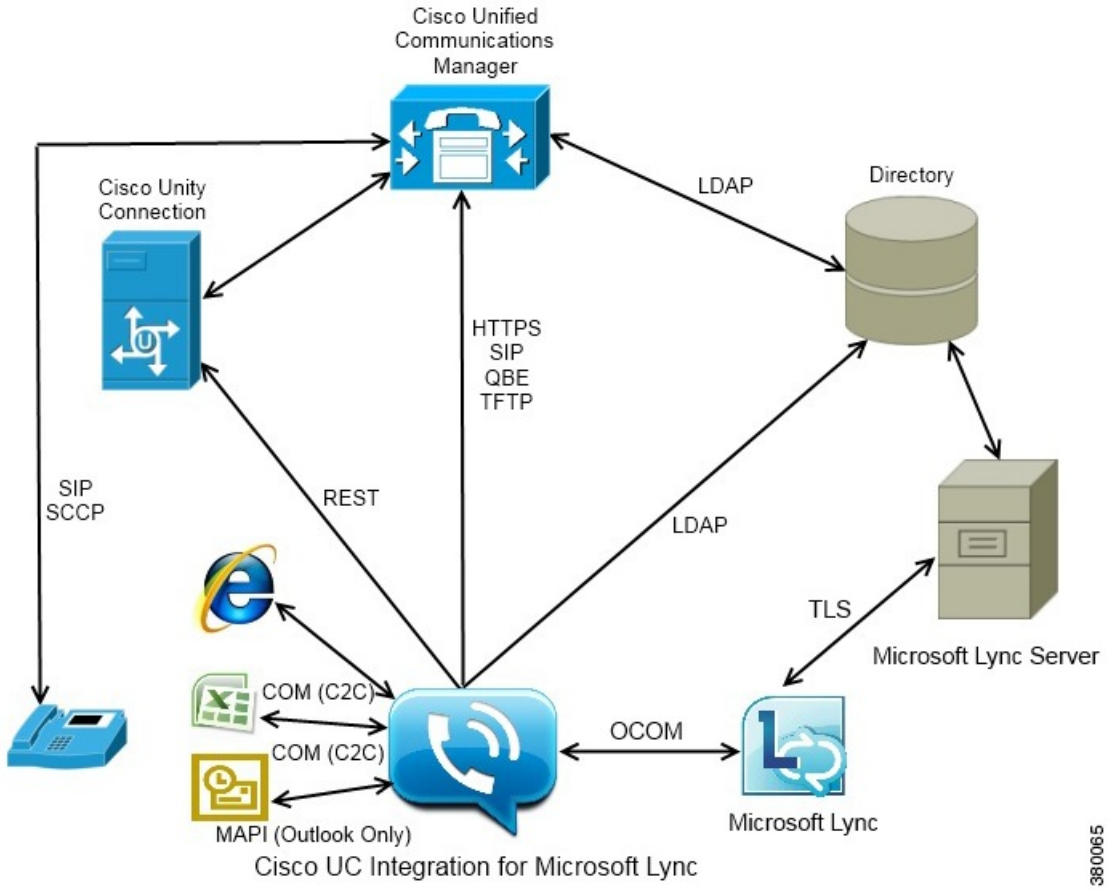
CHAPTER 2

Deployment Architecture Overview

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.

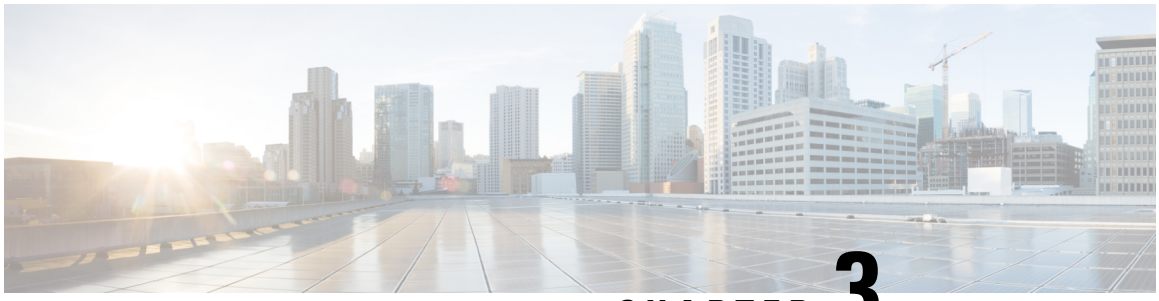
Cisco Unified Communications Manager

- 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



CHAPTER 3

Planning Your Deployment

Hardware Requirements

Installed RAM

2GB RAM on Microsoft Windows 7 and Microsoft Windows 8

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 11 on Microsoft Windows 7

I/O ports

USB 2.0 for USB camera and audio devices.

Software Requirements

Supported Versions of Microsoft Lync and Microsoft Skype for Business

- Microsoft Lync 2010
- Microsoft Lync 2013

  Microsoft Lync 2013 is supported with the following caveats:

  - Escalation from a Microsoft Lync group chat session to a voice or video call is not supported.
  - Microsoft Lync 2013 update KB2812461 must be installed to enable right-click to call support.

  Note Microsoft Lync 2013 64 bit is not supported.

- Microsoft Skype for Business 2015

  Note Microsoft Skype for Business 2015 64 bit is not supported.

Supported Operating Systems

- Microsoft Windows 7 SP1 or later, 32 and 64 bit
- Microsoft Windows 8.x, 32 and 64 bit

Supported Servers

- Cisco Unified Communications Manager version 8.6 or later
- Cisco Unity Connection version 8.5 or later

Supported Directories

- Active Directory Domain Services for Windows Server 2012 R2
- Active Directory Domain Services for Windows Server 2008 R2
- 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 8.0 or later. The application uses the Microsoft Internet Explorer rendering engine to display HTML content.

Support for Microsoft Office (Click to Call)

- Microsoft Office 2010 32 bit
- Microsoft Office 2013 32 bit

Support for Microsoft Office 365

Cisco UC Integration for Microsoft Lync integrates with Microsoft Lync for IM and Presence and with Microsoft Outlook and Microsoft Office applications for Click to Call on the client side only. Cisco UC Integration with Microsoft Lync is therefore compatible with all of the same versions of Microsoft Lync, Outlook, and Office applications whether they are Office 365-based or traditional on-premise deployments.

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		
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

Port	Protocol	Description
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
- 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 C310	Plantronics Voyager Pro UC B230
Plantronics Blackwire C320	Plantronics Voyager Pro UC BT300
Plantronics Blackwire C420	Plantronics Voyager Pro UC WG200/B
Plantronics Blackwire C435	Plantronics W740
Plantronics Blackwire C610	Plantronics WO200/A
Plantronics Blackwire C620	Plantronics WO300
Plantronics Blackwire C710	Polycom CX100 Speakerphone
Plantronics Blackwire C720	Jabra BIZ 2400
Plantronics C220UC	Jabra BIZ 620
Plantronics Calisto P240 series	Jabra GN2000 CIPC Duo
Plantronics Calisto P420	Jabra GN2000 CIPC Mono
Plantronics Calisto P610 series	Jabra Go 6470
Plantronics Calisto P800 series	Jabra PRO 930
Plantronics DSP 400	Jabra PRO 9470
Plantronics Savi 440	Jabra Speak 410
Plantronics Savi 740	Jabra-8120
Plantronics Voyager 510SL	

Cameras

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

Expressway for Mobile and Remote Access Deployments

Expressway for Mobile and Remote Access for Cisco Unified Communications Manager allows users to access their collaboration tools from outside the corporate firewall without a VPN client. Using Cisco collaboration gateways, the client can connect securely to your corporate network from remote locations such as public Wi-Fi networks or mobile data networks.

You set up Expressway for Mobile and Remote Access as follows:

1. Set up servers to support Expressway for Mobile and Remote Access using Cisco Expressway-E and Cisco Expressway-C.*
    1. See the following documents to set up the Cisco Expressway servers:
        - *Cisco Expressway Basic Configuration Deployment Guide*
        - *Mobile and Remote Access via Cisco Expressway Deployment Guide*

    * If you currently deploy a Cisco TelePresence Video Communications Server (VCS) environment, you can set up Expressway for Mobile and Remote Access. For more information, see *Cisco VCS Basic Configuration (Control with Expressway) Deployment Guide* and *Mobile and Remote Access via Cisco VCS Deployment Guide*.
    2. Add any relevant servers to the whitelist for your Cisco Expressway-C server to ensure that the client can access services that are located inside the corporate network.

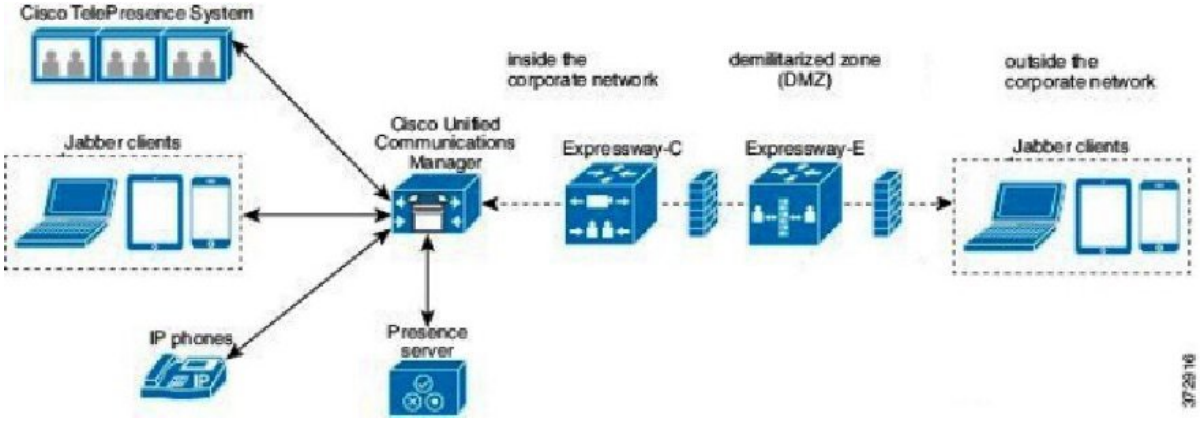
        To add a server to the Cisco Expressway-C whitelist, use the **HTTP server allow** setting.

        This list can include the servers on which you host voicemail or contact photos.
2. Configure an external DNS server that contains the `_collab-edge` DNS SRV record to allow the client to locate the Expressway for Mobile and Remote Access server.

Important The services domain required for Service Discovery can bootstrapped in the installer or provided by the user in the very first login screen in the form of `user@example.com`. When the services domain is bootstrapped the initial logon screen is not presented to the user because the domain is already known.

Figure 1: How the Client Connects to the Expressway for Mobile and Remote Access

The following diagram illustrates the architecture of an Expressway for Mobile and Remote Access environment.



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.

Deployment with Single Sign-On

You can enable your services with Security Assertion Markup Language (SAML) single sign-on (SSO).

The following steps describe the sign-in flow for SAML SSO after users start their client:

1. The user starts the client. If you configure your Identity Provider (known as an *IdP*) to prompt users to sign in using a Web form, the form is displayed within the client.
2. The client sends an authorization request to the service it is connecting to, such as Cisco Unified Communications Manager, or Cisco Unity Connection.

3. The service redirects the client to request authentication from the IdP.
4. The IdP requests credentials. Credentials can be supplied in one of the following methods:
    - Form-based authentication that presents a page to the user containing username and password fields.
    - Kerberos for Integrated Windows authentication (IWA).
    - Smart card authentication.
    - Basic http authentication method in which client offers the username and password when making a HTTP request.
5. The IdP provides a cookie to the browser or other authentication method. The IdP authenticates the identity using SAML, which allows the service to provide the client with a token.
6. The client uses the token for authentication to login to the service.

Authentication Methods

The authentication mechanism impacts user experience of SSO. For example, if you use Kerberos, the client does not prompt users for credentials, because they already provided authentication to gain access to the desktop.

User Sessions

Users sign in for a *session*, which gives them a pre-defined period to use Cisco UC Integration for Microsoft Lync services. To control how long sessions last, you configure cookie and token timeout parameters. When a session has expired and the client is not able to silently renew it, because user input is required, the user will be prompted to re-authenticate. This can occur when the authorization cookie is no longer valid. If Kerberos or a Smart card is used, no action is needed to re-authenticate, unless a PIN is required for the Smart card; there is no risk of interruption to services, such as voicemail or incoming calls.

Single Sign-On Requirements

SAML 2.0

Use SAML 2.0 to enable single sign-on (SSO) for the client to use Cisco Unified Communications Manager services. SAML 2.0 is not compatible with SAML 1.1. Select an IdP that uses the SAML 2.0 standard. The supported identity providers have been tested to be compliant with SAML 2.0 and can be used to implement SSO.

Supported Identity Providers

The IdP must be Security Assertion Markup Language (SAML) compliant. The clients support the following identity providers:

- Ping Federate 6.10.0.4
- Microsoft Active Directory Federation Services (ADFS) 2.0
- Open Access Manager (OpenAM) 10.1

Note Ensure that you configure Globally Persistent cookies for use with OpenAM.

When you configure the IdP, the configured settings impact how you sign into the client. Some parameters, such as the type of cookie (persistent or session), or the authentication mechanism (Kerberos or Web form), determine how often you have to be authenticated.

Cookies

To enable cookie sharing with the browser, you must use persistent cookies and not session cookies. Persistent cookies prompt the user to enter credentials one time in the client or in any other desktop application that uses Internet Explorer. Session cookies require that users enter their credentials every time the client is launched. You configure persistent cookies as a setting on the IdP. If you are using Open Access Manager as your IdP, you must configure Globally Persistent cookies (and not Realm Specific Persistent Cookies).

Required Browsers

To share the authentication cookie (issued by IdP) between the browser and the client, you must specify **Internet Explorer** as your default browser.

Single Sign-On and Remote Access

For users that provide their credentials from outside the corporate firewall using Expressway Mobile and Remote Access, single sign-on has the following restrictions:

- Single sign-on (SSO) is available with Cisco Expressway 8.5 and Cisco Unified Communications Manager release 10.5.2 or later. You must either enable or disable SSO on both.
- The Identity Provider used must have the same internal and external URL. If the URL is different, the user may be prompted to sign in again when changing between inside and outside the corporate firewall.

Enable SAML SSO in the Client

Before you begin

- Enable SSO on Cisco Unified Communications Applications 10.5.1 Service Update 1—For information about enabling SAML SSO on this service, read the *SAML SSO Deployment Guide for Cisco Unified Communications Applications, Release 10.5*.
- Enable SSO on Cisco Unity Connection version 10.5—For more information about enabling SAML SSO on this service, read *Managing SAML SSO in Cisco Unity Connection*.

Procedure

Step 1 Deploy certificates on all servers so that the certificate can be validated by a web browser, otherwise users receive warning messages about invalid certificates. For more information about certificate validation, see *Certificate Validation*.

Step 2 Ensure Service Discovery of SAML SSO in the client. The client uses standard service discovery to enable SAML SSO in the client. Enable service discovery by using the following configuration parameters: ServicesDomain,VoiceServicesDomain, and ServiceDiscoveryExcludedServices. For more information about how to enable service discovery, see *How the Client Locates Services*.

Step 3 Define how long a session lasts.

A session is comprised of cookie and token values. A cookie usually lasts longer than a token. The life of the cookie is defined in the Identity Provider, and the duration of the token is defined in the service.

Step 4 When SSO is enabled, by default all Cisco UC Integration for Microsoft Lync users sign in using SSO. Administrators can change this on a per user basis so that certain users do not use SSO and instead sign in with their Cisco UC Integration for Microsoft Lync username and password. To disable SSO for a Cisco UC Integration for Microsoft Lync user, set the value of the SSO_Enabled parameter to FALSE.

If you have configured Cisco UC Integration for Microsoft Lync not to ask users for their email address, their first sign in to Cisco UC Integration for Microsoft Lync may be non-SSO. In some deployments, the parameter ServicesDomainSsoEmailPrompt needs to be set to ON. This ensures that Cisco UC Integration for Microsoft Lync has the information required to perform a first-time SSO sign in. If users signed in to Cisco UC Integration for Microsoft Lync previously, this prompt is not needed because the required information is available.

About Service Discovery

Service discovery enables clients to automatically detect and locate services on your enterprise network. Clients query domain name servers to retrieve service (SRV) records that provide the location of servers.

The primary benefits to using service discovery are as follows:

- Speeds time to deployment.
- Allows you to centrally manage server locations.

Important If you are migrating from Cisco Unified Presence 8.x to Cisco Unified Communications Manager IM and Presence Service 9.0 or later, you must specify the Cisco Unified Presence server FQDN in the migrated UC service on Cisco Unified Communications Manager. Open **Cisco Unified Communications Manager Administration** interface. Select **User Management > User Settings > UC Service**.

For UC services with type **IM and Presence**, when you migrate from Cisco Unified Presence 8.x to Cisco Unified Communications Manager IM and Presence Service the **Host Name/IP Address** field is populated with a domain name and you must change this to the Cisco Unified Presence server FQDN.

However, the client can retrieve different SRV records that indicate to the client different servers are present and different services are available. In this way, the client derives specific information about your environment when it retrieves each SRV record.

The following table lists the SRV records that you can deploy and explains the purpose and benefits of each record:

SRV Record	Purpose	Why You Deploy
`_cisco-uds`	Provides the location of Cisco Unified Communications Manager version 9.0 and later.	• Eliminates the need to specify installation arguments. • Lets you centrally manage configuration in UC service profiles. • Enables the client to discover the user's home cluster. As a result, the client can automatically get the user's device configuration and register the devices. You do not need to provision users with Cisco Unified Communications Manager IP Phone (CCMCIP) profiles or Trivial File Transfer Protocol (TFTP) server addresses. • Supports Expressway for Mobile and Remote Access.
`_cuplogin`	Provides the location of Cisco Unified Presence. Sets Cisco Unified Presence as the authenticator.	• Supports deployments with Cisco Unified Communications Manager and Cisco Unified Presence version 8.x. • Supports deployments where all clusters have not yet been upgraded to Cisco Unified Communications Manager 9.
`_collab-edge`	Provides the location of Cisco VCS Expressway or Cisco Expressway-E. The client can retrieve service profiles from Cisco Unified Communications Manager to determine the authenticator.	• Supports deployments with Expressway for Mobile and Remote Access.

How the Client Locates Services

The following steps describe how the client locates services with SRV records:

1. The client's host computer or device gets a network connection.

   When the client's host computer gets a network connection, it also gets the address of a Domain Name System (DNS) name server from the DHCP settings.

2. User starts the client.

3. The client queries the name server for the following SRV records in order of priority:

   - `_cisco-uds`
   - `_cuplogin`

- `_collab-edge`

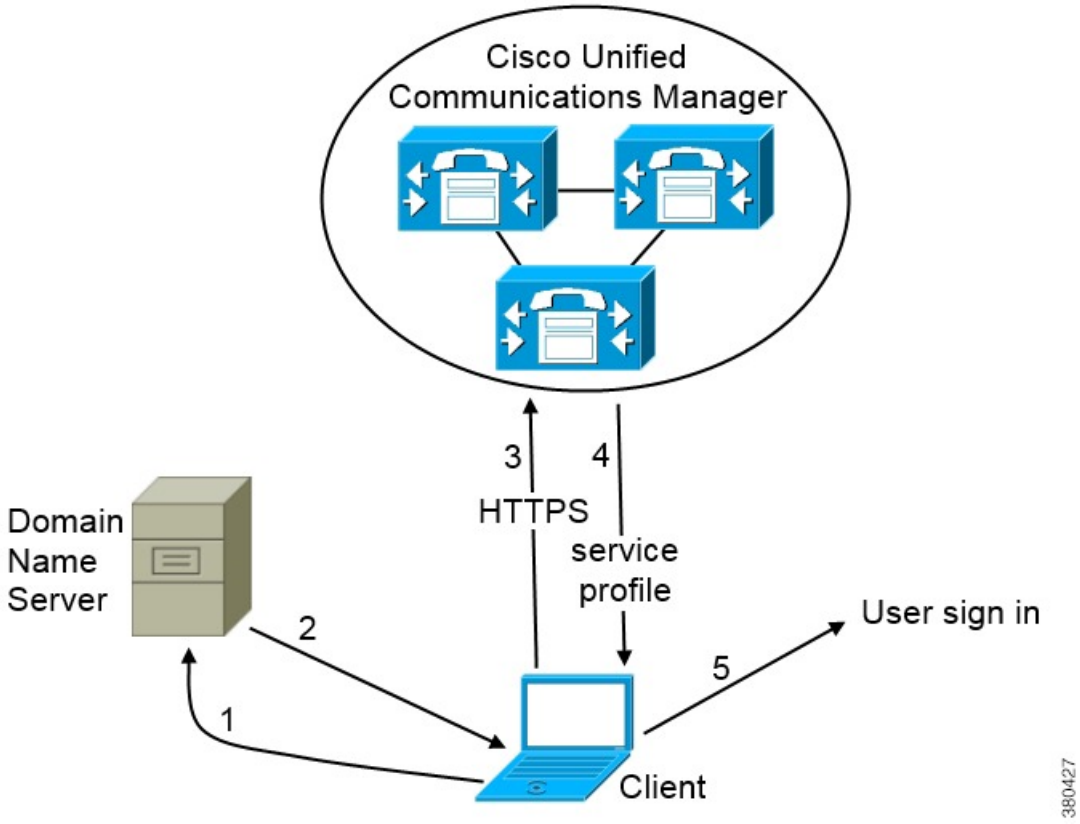
The client caches the results of the DNS query to load on subsequent launches.

Cisco UDS SRV Record

In deployments with Cisco Unified Communications Manager version 9 and later, the client can automatically discover services and configuration with the `_cisco-uds` SRV record.

The following figure shows how the client uses the `_cisco-uds` SRV record.

Figure 2: UDS SRV Record Login Flow



1. The client queries the domain name server for SRV records.
2. The domain name server returns the `_cisco-uds` SRV record.
3. The client locates the user's home cluster.

   As a result, the client can retrieve the device configuration for the user and automatically register telephony services.

Important In an environment with multiple Cisco Unified Communications Manager clusters, you can configure the Intercluster Lookup Service (ILS). ILS enables the client to find the user's home cluster and discover services.

If you do not configure ILS, you must manually configure remote cluster information, similar to the Extension Mobility Cross Cluster (EMCC) remote cluster setup. For more information on remote cluster configurations, see the *Cisco Unified Communications Manager Features and Services Guide*.

4. The client retrieves the user's service profile.

   The user's service profile contains the addresses and settings for UC services and client configuration.

   The client also determines the authenticator from the service profile.

5. The client signs the user in to the authenticator.

The following is an example of the `_cisco-uds` SRV record:

```
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 6
          weight         = 30
          port           = 8443
          svr hostname   = cucm3.example.com
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 2
          weight         = 20
          port           = 8443
          svr hostname   = cucm2.example.com
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 1
          weight         = 5
          port           = 8443
          svr hostname   = cucm1.example.com
```

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. The following directory integration is supported:

- Enhanced Directory Integration (EDI)

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 automatically discovers the directory service and connects 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 receives 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, 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 that the following attributes are indexed:

- sAMAccountName
- telephoneNumber

  Also, 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

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, synchronize all users on the corporate directory to each Cisco Unified Communications Manager cluster. 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, synchronize all 40,000 users to both clusters. 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 2008
- Microsoft Active Directory 2003
- OpenLDAP
- Active Directory Lightweight Directory Service (AD LDS) or Active Directory Application Mode (ADAM)
- Any server that supports LDAPv3 protocol

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

- OpenLDAP integration using anonymous or authenticated binds.
- Active Directory Lightweight Directory Service (AD LDS) or Active Directory Application Mode (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

Cisco UC Integration for Microsoft Lync supports two methods for prioritizing and classifying Real-time Transport Protocol (RTP) traffic as it traverses the network:

- Deploy with Cisco Media Services Interface
- Set DSCP values in IP headers of RTP media packets

Tip We recommend deploying with Cisco Media Services Interface (MSI). This method effectively improves the quality of experience and reduces cost of deployment and operations. MSI also enables the client to become network aware so it can dynamically adapt to network conditions and integrate more tightly with the network.

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.

Before Cisco UC Integration for Microsoft Lync sends audio media or video media, it checks for Cisco Media Services Interface.

- 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.

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.

Set DSCP Values

Set Differentiated Services Code Point (DSCP) values in RTP media packet headers to prioritize Cisco UC Integration for Microsoft Lync traffic as it traverses the network.

Port Ranges on Cisco Unified Communications Manager

You define the port range that the client uses on the SIP profile in Cisco Unified Communications Manager. The client then uses this port range to send RTP traffic across the network.

Specify a Port Range on the SIP Profile

To specify a port range for the client to use for RTP traffic, do the following:

Procedure

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

Step 2 Select **Device** > **Device Settings** > **SIP Profile**.

Step 3 Find the appropriate SIP profile or create a new SIP profile.

The **SIP Profile Configuration** window opens.

Step 4 Specify the port range in the following fields:

Start Media Port

Defines the start port for media streams. This field sets the lowest port in the range.

Stop Media Port

Defines the stop port for media streams. This field sets the highest port in the range.

Step 5 Select **Apply Config** and then **OK**.

How the Client Uses Port Ranges

Cisco UC Integration for Microsoft Lync equally divides the port range that you set in the SIP profile. The client then uses the port range as follows:

- Lower half of the port range for audio streams
- Upper half of the port range for video streams

For example, if you use a start media port of 3000 and an end media port of 4000, the client sends media through ports as follows:

- Ports 3000 to 3501 for audio streams
- Ports 3502 to 4000 for video streams

As a result of splitting the port range for audio media and video media, the client creates identifiable media streams. You can then classify and prioritize those media streams by setting DSCP values in the IP packet headers.

Options for Setting DSCP Values

Methods for setting DSCP values:

- Set DSCP values with Microsoft Group Policy
- Set DSCP values on network switches and routers

Set DSCP Values with Group Policy

If you deploy Cisco UC Integration for Microsoft Lync on a later Windows operating system such as Microsoft Windows 7, you can use Microsoft Group Policy to apply DSCP values.

Complete the steps in the following Microsoft support article to create a group policy: http://technet.microsoft.com/en-us/library/cc771283%28v=ws.10%29.aspx

You should create separate policies for audio media and video media with the following attributes:

Attributes	Audio Policy	Video Policy	Signaling Policy
Application name	`CUCILync.exe`	`CUCILync.exe`	`CUCILync.exe`
Protocol	UDP	UDP	TCP
Port number or range	Corresponding port number or range from the SIP profile on Cisco Unified Communications Manager.	Corresponding port number or range from the SIP profile on Cisco Unified Communications Manager.	5060 for SIP 5061 for secure SIP

Attributes	Audio Policy	Video Policy	Signaling Policy
DSCP value	46	34	24

Set DSCP Values on the Network

You can configure switches and routers to mark DSCP values in the IP headers of RTP media.

To set DSCP values on the network, you must identify the different streams from the client application.

Media Streams

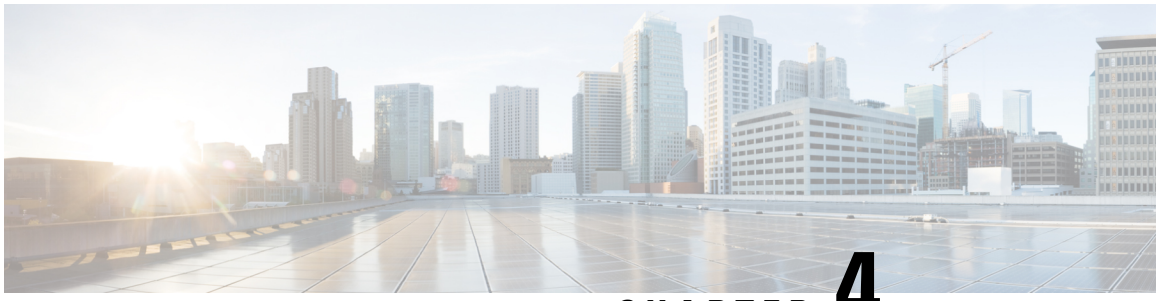
Because the client uses different port ranges for audio streams and video streams, you can differentiate audio media and video media based on those port range. Using the default port ranges in the SIP profile, you should mark media packets as follows:

- Audio media streams in ports from 16384 to 24574 as EF
- Video media streams in ports from 24575 to 32766 as AF41

Signaling Streams

You can identify signaling between the client and servers based on the various ports required for SIP, CTI QBE, and XMPP. For example, SIP signaling between Cisco UC Integration for Microsoft Lync and Cisco Unified Communications Manager occurs through port 5060.

You should mark signaling packets as AF31.



CHAPTER 4

Setup Certificate Validation

Cisco UC Integration for Microsoft Lync uses certificate validation to establish secure connections with servers.

Servers present Cisco UC Integration for Microsoft Lync with certificates when attempting to establish secure connections. Cisco UC Integration for Microsoft Lync validates those certificates against certificates in the Microsoft Windows certificate store. If the client cannot validate a certificate, it prompts the user to confirm if they want to accept the certificate.

Required Certificates

The following certificates are presented to establish a secure connection.

Server	Certificate
Cisco Unified Communications Manager	HTTP (Tomcat)
Cisco Unity Connection	HTTP (Tomcat)

Important Notes

- Every node in a cluster, including both subscribers and publishers, run a Tomcat service and can present the client with an HTTP certificate. You should plan to sign the certificates for each node in the cluster.
- To secure SIP signaling between the client and Cisco Unified Communications Manager, you should use Certification Authority Proxy Function (CAPF) enrollment.

Get Certificates Signed by Certificate Authority

Cisco recommends using server certificates that are signed by one of the following types of Certificate Authority (CA):

- **Public CA**

A third-party company verifies the server identity and issues a trusted certificate.

- **Private CA**

  You create and manage a local CA and issue trusted certificates.

The signing process varies for each server and can vary between server versions. It is beyond the scope of this document to provide detailed steps for every version of each server. You should consult the appropriate server documentation for detailed instructions on how to get certificates signed by a CA. However, the following steps provide a high-level overview of the procedure.

Procedure

Step 1 Generate a Certificate Signing Request (CSR) on each server that can present a certificate to the client.

Step 2 Submit each CSR to the CA.

Step 3 Upload the certificates that the CA issues to each server.

Certificate Signing Request Forms and Requirements

Public CAs typically require CSRs to conform to specific formats. For example, a public CA might only accept CSRs that:

- Are Base64-encoded.
- Do not contain certain characters, such as @&! , in the Organization, OU, or other fields.
- Use specific bit lengths in the server's public key.

Likewise, if you submit CSRs from multiple nodes, public CAs might require that the information is consistent in all CSRs.

To prevent issues with your CSRs, you should review the format requirements from the public CA to which you plan to submit the CSRs. You should then ensure that the information you enter when configuring your server conforms to the format that the public CA requires.

One Certificate Per FQDN: Some public CAs sign only one certificate per fully qualified domain name (FQDN).

Server Identity in Certificates

The CA specifies the server identity in the certificate as part of the signing process. When the client validates that certificate, it checks that:

- A trusted authority has issued the certificate.
- The identity of the server that presents the certificate matches the identity of the server specified in the certificate.

Note Public CAs generally require a fully qualified domain name (FQDN) as the server identity, not an IP address.

Identifier Fields

The client checks the following identifier fields in server certificates for an identity match:

- **HTTP certificates**
  - SubjectAltName\dnsNames
  - Subject CN

Tip The Subject CN field can contain a wildcard (*) as the leftmost character, for example, *.cisco.com.

Prevent Identity Mismatch

If users attempt to connect to a server with an IP address, and the server certificate identifies the server with an FQDN, the client cannot identify the server as trusted and prompts the user.

If your server certificates identify the servers with FQDNs, you should plan to specify each server name as FQDN throughout your environment.

Import Root Certificates on Client Computers

Every server certificate should have an associated root certificate present in the trust store on client computers. Cisco UC Integration for Microsoft Lync validates the certificates that servers present against the root certificates in the trust store.

If you get server certificates signed by a public CA, the public CA should already have a root certificate present in the trust store on the client computer. In this case, you do not need to import root certificates on the client computers.

You should import root certificates into the Microsoft Windows certificate store if:

- The certificates are signed by a CA that does not already exist in the trust store, such as a private CA.
  - Import the private CA certificate to the Trusted Root Certification Authorities store.
- The certificates are self-signed.
  - Import self-signed certificates to the Enterprise Trust store.

Important If root certificates are not present in the trust store, Cisco UC Integration for Microsoft Lync prompts users to accept certificates from each server in your environment.

When the client prompts users to accept a certificate, users can:

- **Accept the certificate**
  - The client saves the certificate to the Enterprise Trust store.
- **Decline the certificate**
  - The client
    - Does not save the certificate.

- Does not connect to the server.
- Displays an error notification.

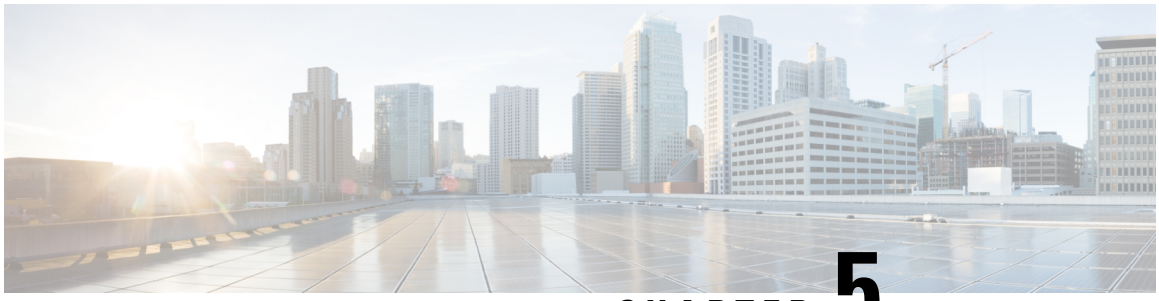
When users restart the client, it prompts them to accept the certificate again.

You can use any appropriate method to import certificates into the Microsoft Windows certificate store, including the following. For detailed instructions on importing certificates, refer to the appropriate Microsoft documentation.

- Use the Certificate Import Wizard to import certificates individually.
- Deploy certificates to users with the CertMgr.exe command line tool on Microsoft Windows Server.

Note This option requires you to use the Certificate Manager tool, CertMgr.exe, not the Certificates Microsoft Management Console, CertMgr.msc.

- Deploy certificates to users with a Group Policy object (GPO) on Microsoft Windows Server.



CHAPTER 5

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.

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 Required: 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

Create CSF Devices

Complete the steps in this task to create CSF 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 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 create a CSF device for a user named Tanya Adams, whose username is tadams. In this case, you should specify CSFtadams as the device name.

Step 6 Specify configuration settings on the **Phone Configuration** window as appropriate.

See the *Phone Setup* topic in the Cisco Unified Communications Manager documentation for more information about the configuration settings on the **Phone Configuration** window.

Step 7 Select **Save**.

A 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.

Video Desktop Sharing

Binary Floor Control Protocol (BFCP) provides video desktop sharing capabilities for software phone devices, also known as CSF devices. Cisco Unified Communications Manager handles the BFCP packets that users transmit when using video desktop sharing capabilities. On Cisco Unified Communications Manager version 9.0(1) and later, BFCP presentation sharing is automatically enabled. For this reason, you do not need to perform any steps to enable video desktop sharing on CSF devices.

- You can enable video desktop sharing only on software phone devices. You cannot enable video desktop sharing on desk phone devices.
- Users must be on active calls to use video desktop sharing capabilities. You can only initiate video desktop sharing sessions from active calls.

Tip You must enable BFCP on the SIP trunk to allow video desktop sharing capabilities outside of a Cisco Unified Communications Manager cluster. To enable BFCP on the SIP trunk, do the following:

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.

Set Up Secure Phone Capabilities

Before you begin

Video Desktop Sharing, on page 37

What to do next

Add Directory Number to the Device for Desktop Applications, on page 44

Configure the Security Mode

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

Mixed mode security:

- Allows authenticated, encrypted, and non secure 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 the appropriate phone security profile from the Phone Security Profile type drop-down list and 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.

Restriction You must use fully qualified domain name (FQDN) format for the security profile name if users connect remotely to the corporate network through Expressway for Mobile and Remote Access.

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**.
- 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

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 To 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

If you are using CAPF enrollment to configure secure phones, then you must provide users with authentication strings. Users must specify the authentication string in the client interface to access their 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 user's computer or mobile device 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 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 device. The user 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 Standard CTI Secure Connection user group.

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.

Using Expressway for Mobile and Remote Access

Users cannot complete the enrollment process or use secure phone capabilities from outside the corporate network. This limitation also includes when users connects through Expressway for Mobile and Remote Access; for example,

1. You configure a user's CSF device for secure phone capabilities.
2. That user connects to the internal corporate network through Expressway for Mobile and Remote Access.
3. The client notifies the user that it cannot use secure phone capabilities instead of prompting the user to enter an authentication string.

When users connect to the internal network through Expressway for Mobile and Remote Access and participate in a call:

- Media is encrypted on the call path between the Cisco Expressway-C and devices that are registered to the Cisco Unified Communications Manager using Expressway for Mobile and Remote Access.
- Media is not encrypted on the call path between the Cisco Expressway-C and devices that are registered locally to Cisco Unified Communications Manager.

Note If you change the phone security profile while the client is connected through Expressway for Mobile and Remote Access, you must restart the client for that change to take effect.

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.

Add Directory Number to the Device for Desktop Applications

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**.

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**.
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**.

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

Create Desk Phone Devices

Users can control desk phones on their computers to place audio calls.

Before you begin

Create software phone 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 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 through the client.

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 that the client 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.
3. Install Cisco Media Services Interface on the computer.

   Cisco Media Services Interface provides the Cisco Discover Protocol (CDP) driver that enables the client 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 the download site on `cisco.com`.

Desk Phone Video Considerations

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

- 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. The client 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 the client.
- 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.

  See the following Symantec technical document for additional details about this issue: *Cisco IP Phone version 7970 and Cisco Unified Video Advantage is Blocked by Network Threat Protection*.

- You must not select the **Media Termination Point Required** checkbox on the SIP trunk configuration for Cisco Unified Communications Manager. Desk phone video capabilities are not available if you select this checkbox.

Desk Phone Video Troubleshooting

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 the client.
4. Run services.msc on the computer where you installed the client.
5. Restart Cisco Media Services Interface.
6. Restart the client.

Add Directory Number to the Device for Desktop Applications

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**.

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**.
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**.

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

Enable Video Rate Adaptation

The client 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.

Note RTCP is an integral component of Jabber Telephony services. Jabber will continue to send RTCP packets even when disabled.

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 CTI Service

The CTI service provides Jabber with the address of the UDS device service. The UDS device service provides a list of devices associated with the user.

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

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

Step 7 Select **Save**.

What to do next

Add the CTI service to your service profile.

Apply a CTI Service

After you add a CTI 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 exists or if you require a separate service profile for CTI.
- Add a CTI service.

Procedure

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

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

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

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

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

Step 5 Select **Save**.

URI Dialing

This feature is supported for on-premises deployments. URI dialing is enabled in Cisco Unified Communications Manager, release 9.1(2) or later.

This feature is enabled in the `jabber-config.xml` file using the EnableSIPURIDialling parameter.

Example: `<EnableSIPURIDialling>True</EnableSIPURIDialling>`

For more information on the values of the parameter, see the *Common Policies* section.

URI dialing allows users to make calls and resolve contacts with Uniform Resource Identifiers (URI). For example, a user named Adam McKenzie has the following SIP URI associated with his directory number:

amckenzi@example.com. URI dialing enables users to call Adam with his SIP URI rather than his directory number.

For detailed information on URI dialing requirements, such as valid URI formats, as well as advanced configuration including ILS setup, see the *URI Dialing* section of the *System Configuration Guide for Cisco Unified Communications Manager* .

Associate URIs to Directory Numbers

When users make URI calls, Cisco Unified Communications Manager routes the inbound calls to the directory numbers associated to the URIs. For this reason, you must associate URIs with directory numbers. You can either automatically populate directory numbers with URIs or configure directory numbers with URIs.

Automatically Populate Directory Numbers with URIs

When you add users to Cisco Unified Communications Manager, you populate the **Directory URI** field with a valid SIP URI. Cisco Unified Communications Manager saves that SIP URI in the end user configuration.

When you specify primary extensions for users, Cisco Unified Communications Manager populates the directory URI from the end user configuration to the directory number configuration. In this way, automatically populates the directory URI for the user's directory number. Cisco Unified Communications Manager also places the URI in the default partition, which is **Directory URI**.

The following task outlines, at a high level, the steps to configure Cisco Unified Communications Manager so that directory numbers inherit URIs:

Procedure

Step 1 Add devices.

Step 2 Add directory numbers to the devices.

Step 3 Associate users with the devices.

Step 4 Specify primary extensions for users.

What to do next

Verify that the directory URIs are associated with the directory numbers.

Verify Directory URIs

After you specify primary extensions for users, you should complete the following steps to verify that the directory URIs are associated with the directory numbers.

Procedure

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

Step 2 Select **Call Routing** > **Directory Number**.

The **Find and List Directory Numbers** window opens.

Step 3 Find and select the appropriate directory number.

The **Directory Number Configuration** window opens.

Step 4 Locate the **Directory URIs** section.

The primary directory URI for the directory number should correspond to the end user with whom you associated the device.

The partition should be **Directory URI**. This partition is the default into which Cisco Unified Communications Manager places URIs.

Configure Directory Numbers with URIs

You can specify URIs for directory numbers that are not associated with users. You should configure directory numbers with URIs for testing and evaluation purposes only.

To configure directory numbers with URIs, do the following:

Procedure

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

Step 2 Select **Call Routing** > **Directory Number**.

The **Find and List Directory Numbers** window opens.

Step 3 Find and select the appropriate directory number.

The **Directory Number Configuration** window opens.

Step 4 Locate the **Directory URIs** section.

Step 5 Specify a valid SIP URI in the **URI** column.

Step 6 Select the appropriate partition from the **Partition** column.

Note You cannot manually add URIs to the system **Directory URI** partition. You should add the URI to the same route partition as the directory number.

Step 7 Add the partition to the appropriate calling search space so that users can place calls to the directory numbers.

Step 8 Select **Save**.

Associate the Directory URI Partition

You must associate the default partition into which Cisco Unified Communications Manager places URIs with a partition that contains directory numbers.

Important To enable URI dialing, you must associate the default directory URI partition with a partition that contains directory numbers.

If you do not already have a partition for directory numbers within a calling search space, you should create a partition and configure it as appropriate.

Procedure

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

Step 2 Select **System** > **Enterprise Parameters**.

The **Enterprise Parameters Configuration** window opens.

Step 3 Locate the **End User Parameters** section.

Step 4 In the **Directory URI Alias Partition** row, select the appropriate partition from the drop-down list.

Step 5 Click **Save**.

The default directory URI partition is associated with the partition that contains directory numbers. As a result, Cisco Unified Communications Manager can route incoming URI calls to the correct directory numbers.

You should ensure the partition is in the appropriate calling search space so that users can place calls to the directory numbers.

Enable FQDN in SIP Requests for Contact Resolution

To enable contact resolution with URIs, you must ensure that Cisco Unified Communications Manager uses the fully qualified domain name (FQDN) in SIP requests.

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 Find and select the appropriate SIP profile.

Remember You cannot edit the default SIP profile. If required, you should create a copy of the default SIP profile that you can modify.

Step 4 Select **Use Fully Qualified Domain Name in SIP Requests** and then select **Save**.

What to do next

Associate the SIP profile with all devices that have primary extensions to which you associate URIs.

Call Pickup

The Call Pickup feature allows users to answer calls that come in on a directory number other than their own. Directory numbers are assigned to call pickup groups and Cisco Unified Communications Manager automatically dials the appropriate call pickup group number. Users select **Pickup** to answer the call.

Group call pickup allows users to pick up incoming calls in another group. Users enter the group pickup number, select **Pickup** and Cisco Unified Communications Manager automatically dials the appropriate call pickup group number.

Other group pickup allows users to pick up incoming calls in a group that is associated with their group. When the user selects **Other Pickup** Cisco Unified Communications Manager automatically searches for the incoming call in the associated groups.

Directed call pickup allows users to pick up an incoming call on a directory number. Users enter the directory number, select **Pickup** and Cisco Unified Communications Manager connects the incoming call.

For more information about configuring call pickup, see the *Feature Configuration Guide for Cisco Unified Communications Manager*.

Call pickup notifications

For multiple incoming calls, the notification displayed is *Call(s) available for pickup*. When the user answers a call, the user gets connected to the incoming call that has been ringing the longest.

Deskphone mode

In deskphone mode the following limitations apply:

- The Cisco Unified Communications Manager notification settings are not supported for the pickup group. The call pickup notification displayed is *CallerA->CallerB*.
- The Cisco Unified Communications Manager settings for audio and visual settings are not supported. The visual alerts are always displayed.

Shared line behavior

For users that have a deskphone and a CSF softphone with a shared line the following limitations apply:

- Attempt to pick up a call using the softphone when there is no call available, *No call available for PickUp* is displayed on the deskphone.
- Attempt to pick up a call using the deskphone when there is no call available, *No call available for PickUp* is displayed on the softphone.

User not a member of an associated group

For an incoming call to another pickup group where the user is not a member of an associated group:

- Directed call pickup can be used to pick up the incoming call.
- Group pickup does not work

Expected behavior using group call pickup and directed call pickup

The following are expected behaviors when using group call pickup and directed call pickup:

- Enter an invalid number
  - Softphone mode—The conversation window appears and the annunciator is heard immediately.
  - Deskphone mode—The conversation window, fast busy tone, or the annunciator followed by the fast busy tone, *Pickup failed* error message.
- Enter a valid number and no current call available to pick up
  - Softphone mode—Tone in headset, no conversation window appears and *No call available for pickup* error message.
  - Deskphone mode—No conversation window and *No call available for pickup* error message.
- Enter directory number of a phone in an associated group and no current call available to pick up
  - Softphone mode—Tone in headset, no conversation window appears and *No call available for pickup* error message.
  - Deskphone mode—No conversation window and *No call available for pickup* error message.
- Enter a directory number of a phone on the same Cisco Unified Communications Manager node and not in an associated group
  - Softphone mode—Conversation window appears and fast busy tone.
  - Deskphone mode—Conversation window appears, fast busy tone, and *Pickup failed* error message.
- Enter first digits of a valid group
  - Softphone mode—Tone in headset, conversation window appears, and after 15 seconds annunciator followed by the fast busy tone.
  - Deskphone mode—Conversation window appears, after 15 seconds annunciator, fast busy tone, and *Pickup failed* error message.

Call pickup using a deskphone that is not in a call pickup group

If a user attempts a call pickup from a deskphone that is not in a call pickup group, the conversation window appears for a moment. The user should not be configured to use the call pickup feature if they are not members of a call pickup group.

Original recipient information not available

When the Cisco Unified Communications Manager *Auto Call Pickup Enabled* setting is true, the recipient information is not available in the client when the call is picked up in softphone mode. If the setting is false, the recipient information is available.

Configure Call Pickup Group

Call pickup groups allow users to pick up incoming calls in their own group.

Procedure

Step 1 Open the **Cisco Unified Communication Manager** interface.

Step 2 Select **Call Routing** > **Call Pickup Group**

The **Find and List Call Pickup Groups** window opens.

Step 3 Select **Add New**

The **Call Pickup Group Configuration** window opens.

Step 4 Enter call pickup group information:

a) Specify a unique name for the call pickup group.
b) Specify a unique directory number for the call pickup group number.
c) Enter a description.
d) Select a partition.

Step 5 (Optional) Configure the audio or visual notification in the **Call Pickup Group Notification Settings** section.

a) Select the notification policy.
b) Specify the notification timer.

For further information on call pickup group notification settings see the call pickup topics in the relevant Cisco Unified Communications Manager documentation.

Step 6 Select **Save**.

What to do next

Assign a call pickup group to directory numbers.

Assign Directory Number

Assign a call pickup group to a directory number. Only directory numbers that are assigned to a call pickup group can use call pickup, group call pickup, other group pickup, and directed call pickup.

Before you begin

Before you assign a call pickup group to a directory number, you must create the call pickup group.

Procedure

Step 1 Open the **Cisco Unified Communications Manager Administration** interface.

Step 2 Assign a call pickup group to a directory number using one of the following methods:

- Select **Call Routing** > **Directory Number**, find and select your directory number and in the Call Forward and Call Pickup Settings area select the call pickup group from the call pickup group drop down list.
- Select **Device** > **Phone**, find and select your phone and in the **Association Information** list choose the directory number to which the call pickup group will be assigned.

Step 3 To save the changes in the database, select **Save**.

Other Call Pickup

Other Group Pickup allows users to pick up incoming calls in a group that is associated with their own group. The Cisco Unified Communications Manager automatically searches for the incoming call in the associated groups to make the call connection when the user selects **Other Pickup**.

Configure Other Call Pickup

Other Group Pickup allows users to pick up incoming calls in an associated group. Cisco Unified Communications Manager automatically searches for the incoming call in the associated groups to make the call connection when the user selects **Other Pickup**.

Before you begin

Before you begin, configure call pickup groups.

Procedure

Step 1 Open the **Cisco Unified Communication Manager Administration** interface.

Step 2 Select **Call Routing** > **Call Pickup Group**

The **Find and List Call Pickup Groups** window opens.

Step 3 Select your call pickup group.

The **Call Pickup Group Configuration** window opens.

Step 4 In the **Associated Call Pickup Group Information** section, you can do the following:

- Find call pickup groups and add to current associated call pickup groups.
- Reorder associated call pickup groups or remove call pickup groups.

Step 5 Select **Save**.

Directed Call Pickup

Directed Call Pickup allows a user to pick up a incoming call directly. The user enters the directory number in the client and selects **Pickup**. Cisco Unified Communications Manager uses the associated group mechanism to control if the user can pick up an incoming call using Directed Call Pickup.

To enable directed call pickup, the associated groups of the user must contain the pickup group to which the directory number belongs.

When the user invokes the Directed Call Pickup feature and enters a directory number to pick up an incoming call, the user connects to the call that is incoming to the specified phone whether or not the call is the longest incoming call in the call pickup group to which the directory number belongs.

Configure Directed Call Pickup

Directed call pickup allows you to pick up a incoming call directly. The user enters the directory number in the client and selects **Pickup**. Cisco Unified Communications Manager uses the associated group mechanism to control if the user can pick up an incoming call using Directed Call Pickup.

To enable directed call pickup, the associated groups of the user must contain the pickup group to which the directory number belongs.

When the user invokes the feature and enters a directory number to pick up an incoming call, the user connects to the call that is incoming to the specified phone whether or not the call is the longest incoming call in the call pickup group to which the directory number belongs.

Procedure

Step 1 Configure call pickup groups and add associated groups. The associated groups list can include up to 10 groups.

For more information, see topics related to defining a pickup group for Other Group Pickup.

Step 2 Enable the Auto Call Pickup Enabled service parameter to automatically answer calls for directed call pickups.

For more information, see topics related to configuring Auto Call Pickup.

Auto Call Pickup

You can automate call pickup, group pickup, other group pickup, and directed call pickup by enabling the Auto Call Pickup Enabled service parameter. When this parameter is enabled, Cisco Unified Communications Manager automatically connects users to the incoming call in their own pickup group, in another pickup group, or a pickup group that is associated with their own group after users select the appropriate pickup on the phone. This action requires only one keystroke.

Auto call pickup connects the user to an incoming call in the group of the user. When the user selects **Pickup** on the client, Cisco Unified Communications Manager locates the incoming call in the group and completes the call connection. If automation is not enabled, the user must select **Pickup** and answer the call, to make the call connection.

Auto group call pickup connects the user to an incoming call in another pickup group. The user enters the group number of another pickup group and selects **Pickup** on the client. Upon receiving the pickup group number, Cisco Unified Communications Manager completes the call connection. If auto group call pickup is not enabled, dial the group number of another pickup group, select **Pickup** on the client, and answer the call to make the connection.

Auto other group pickup connects the user to an incoming call in a group that is associated with the group of the user. The user selects **Other Pickup** on the client. Cisco Unified Communications Manager automatically searches for the incoming call in the associated groups in the sequence that the administrator enters in the **Call Pickup Group Configuration** window and completes the call connection after the call is found. If automation is not enabled, the user must select **Other Pickup**, and answer the call to make the call connection.

Auto directed call pickup connects the user to an incoming call in a group that is associated with the group of the user. The user enters the directory number of the ringing phone and selects **Pickup** on the client. Upon receiving the directory number, Cisco Unified Communications Manager completes the call connection. If

auto directed call pickup is not enabled, the user must dial the directory number of the ringing phone, select **Pickup**, and answer the call that will now ring on the user phone to make the connection.

For more information about **Call Pickup**, see the *Feature Configuration Guide for Cisco Unified Communications Manager*.

Configure Auto Call Pickup

Procedure

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

Step 2 Select **System** > **Service Parameters**

Step 3 Select your server from the Server drop down list and then select the **Cisco Call Manager** service from the Service drop down list.

Step 4 In the **Clusterwide Parameters (Feature - Call Pickup)** section, select one of the following for **Auto Call Pickup Enabled**:

- true—The auto call pickup feature is enabled.
- false—The auto call pickup feature is not enabled. This is the default value.

Step 5 Select **Save**.

Hunt Group

Applies to: All clients

A Hunt Group is a group of lines that are organized hierarchically, so that if the first number in the hunt group list is busy, the system dials the second number. If the second number is busy, the system dials the next number, and so on. Every hunt group has a pilot number that is also called as hunt pilot. A hunt pilot contains a hunt pilot number and an associated hunt list. Hunt pilots provide flexibility in network design. They work with route filters and hunt lists to direct calls to specific devices and to include, exclude, or modify specific digit patterns.

A hunt pilot number is the number that a user dials. A hunt list contains a set of line groups in a specific order. A line group comprises a group of directory numbers in a specific order. The order controls the progress of the search for available directory numbers for incoming calls. A single-line group can appear in multiple hunt lists.

Cisco Unified Communications Manager identifies a call that is to be routed through a defined hunt list, Cisco Unified Communications Manager finds the first available device on the basis of the order of the line groups that a hunt list defines.

Cisco Unified Communications Manager 9.x and later allows configuring of automatic log out of a hunt member when there is no answer. Once the user is logged out, the system displays a log out notification regardless of whether the user is auto logged out, manually logged out, or logged out by the Cisco Unified Communications Manager administrator.

Limitation

Desktop clients must be in softphone mode before users can log in to or out of hunt groups.

Line Group

A line group allows you to designate the order in which directory numbers are chosen. Cisco Unified Communications Manager distributes a call to an idle or available member of a line group based on the call distribution algorithm and on the Ring No Answer (RNA) Reversion timeout setting.

Users cannot pick up calls to a DN that belongs to a line group by using the directed call pickup feature.

Configure Line Group

Before you begin

Configure directory numbers.

Procedure

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

Step 2 Select **Call Routing** > **Route/Hunt** > **Line Group**.

The **Find and List Line Groups** window opens.

Step 3 Select **Add New**.

The **Line Group Configuration** window opens.

Step 4 Enter settings in the **Line Group Information** section as follows:

1. Specify a unique name in the **Line Group Name** field.
2. Specify number of seconds for **RNA Reversion Timeout**.
3. Select a **Distribution Algorithm** to apply to the line group.

Step 5 Enter settings in the **Hunt Options** section as follows:

- Select a value for **No Answer** from the drop-down list.
- Select **Automatically Logout Hunt Member on No Answer** to configure auto logout of the hunt list.
- Select a value for **Busy** from the drop-down list.
- Select a value for **Not Available** from the drop-down list.

Step 6 In the **Line Group Member Information** section, you can do the following:

- Find directory numbers or route partitions to add to the line group.
- Reorder the directory numbers or route partitions in the line group.
- Remove directory numbers or route partitions from the line group.

Step 7 Select **Save**.

What to do next

Configure a hunt list and add the line group to the hunt list.

Hunt List

A hunt list contains a set of line groups in a specific order. A hunt list associates with one or more hunt pilots and determines the order in which those line groups are accessed. The order controls the progress of the search for available directory numbers for incoming calls.

A hunt list comprises a collection of directory numbers as defined by line groups. After Cisco Unified Communications Manager determines a call that is to be routed through a defined hunt list, Cisco Unified Communications Manager finds the first available device on the basis of the order of the line group(s) that a hunt list defines.

A hunt list can contain only line groups. Each hunt list should have at least one line group. Each line group includes at least one directory number. A single line group can appear in multiple hunt lists.

Note The group call pickup feature and directed call pickup feature do not work with hunt lists.

Configure Hunt List

Procedure

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

Step 2 Select **Call Routing** > **Route/Hunt** > **Hunt List**.

The **Find and Hunt List Groups** window opens.

Step 3 Select **Add New**.

The **Hunt List Configuration** window opens.

Step 4 Enter settings in the **Hunt List Information** section as follows:

1. Specify a unique name in the **Name** field.
2. Enter a description for the Hunt List.
3. Select a **Cisco Unified Communications Manager Group** from the drop-down list.
4. The system selects **Enable this Hunt List** by default for a new hunt list when the hunt list is saved.
5. If this hunt list is to be used for voice mail, select **For Voice Mail Usage**.

Step 5 Select **Save** to add the hunt list.

What to do next

Add line groups to the hunt list.

Add Line Group to Hunt List

Before you begin

You must configure line groups and configure a hunt list.

Procedure

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

Step 2 Select **Call Routing** > **Route/Hunt** > **Hunt List**.

The **Find and Hunt List Groups** window opens.

Step 3 Locate the hunt list to which you want to add a line group.

Step 4 To add a line group, select **Add Line Group**.

The **Hunt List Detail Configuration** window displays.

Step 5 Select a line group from the **Line Group** drop-down list.

Step 6 To add the line group, select **Save**.

Step 7 To add additional line groups, repeat Step 4 to Step 6.

Step 8 Select Save.

Step 9 To reset the hunt list, select **Reset**. When the dialog box appears, select **Reset**.

Hunt Pilot

A hunt pilot comprises a string of digits (an address) and a set of associated digit manipulations that route calls to a hunt list. Hunt pilots provide flexibility in network design. They work in conjunction with route filters and hunt lists to direct calls to specific devices and to include, exclude, or modify specific digit patterns. For more information about hunt pilots, see the *System Configuration Guide for Cisco Unified Communications Manager*.

For more detailed information on the configuration options for hunt pilots, see the relevant *Cisco Unified Communications Manager documentation*.

Configure Hunt Pilot

Procedure

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

Step 2 Select **Call Routing** > **Route/Hunt** > **Hunt Pilot**.

The **Find and List Hunt Pilots** window opens.

Step 3 Select **Add New**.

The **Hunt Pilot Configuration** window opens.

Step 4 Enter the hunt pilot, including numbers and wildcards.

Step 5 Select a hunt list from the **Hunt List** drop-down list.

Step 6 Enter any additional configurations in the **Hunt Pilot Configuration** window. For more information on hunt pilot configuration settings, see the relevant Cisco Unified Communications Manager documentation.

Step 7 Select **Save**.

Configure User Associations

When you associate a user with a device, you provision that device to the user.

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. Jabber only supports a single softphone association per device type. For example, only one TCT, BOT, CSF, and TAB device can be associated with a 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 Access Control Group**.

The **Find and List Access Control Groups** dialog box opens.

Step 13 Select the access control groups to which you want to assign the user.

At a minimum you should assign the user to the following access control groups:

- **Standard CCM End Users**

- **Standard CTI Enabled**

Certain phone models require additional control groups, as follows:

- Cisco Unified IP Phone 9900, 8900, or 8800 series or DX 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 Access Control Groups** window closes.

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

TFTP Server Address Options

The client gets device configuration from the TFTP server. You must specify your TFTP server address when you provision users with devices.

Automatic TFTP Server Configuration

If the client gets the `_cisco-uds` SRV record from a DNS query, it can automatically locate the user's home cluster. As a result, the client can also locate the Cisco Unified Communications Manager TFTP service.

You do not need to specify your TFTP server address if you deploy the `_cisco-uds` SRV record.

Manual TFTP Server Configuration

You can manually provide the TFTP server address using the following methods:

- Users manually enter the TFTP server address when they start the client.
- You specify the TFTP server address during installation with the TFTP argument.
- You specify the TFTP server address in the Microsoft Windows registry. Refer to Phone Parameters, on page 108 for more information.

Reset Devices

After you create and associate users with devices, you should reset 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.

Create a CCMCIP Profile

Automatic CCMCIP Profile Configuration

If the client gets the `_cisco-uds` SRV record from a DNS query, it can automatically locate the user's home cluster and discover services. One of the services the client discovers is UDS, which replaces CCMCIP.

You do not need to create a CCMCIP profile if you deploy the `_cisco-uds` SRV record.

Manual CCMCIP Profile Configuration

You can manually provide the CCMCIP server address using the following methods:

- Users manually enter the CCMCIP server address when they start the client.
- You specify the CCMCIP server address during installation with the CCMCIP argument.
- You specify the CCMCIP server address in the Microsoft Windows registry. Refer to Phone Parameters, on page 108 for more information.

Dial Plan Mapping

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

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 client.

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 the client 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 phone numbers. An example of this type of rule is to transform `4089023139` into `23139`.

Publish Dial Rules

Cisco Unified Communications Manager release 8.6.1 or earlier does 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.

Remember You must deploy the COP file every time you update or modify dial rules on Cisco Unified Communications Manager release 8.6.1 or earlier.

Before you begin

1. Create your dial rules in Cisco Unified Communications Manager.
2. Download the Cisco Jabber administration package from cisco.com.
3. Copy `cmterm-cupc-dialrule-wizard-0.1.cop.sgn` from the Cisco Jabber 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-cupc-dialrule-wizard-0.1.cop.sgn` in the **Software Installation/Upgrade** window.

Step 4 Select **Next**.

Step 5 Select `cmterm-cupc-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`.

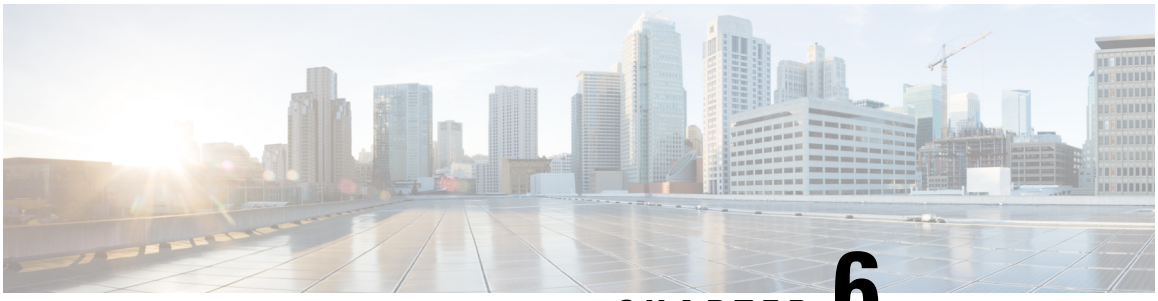
b) Navigate to `http://`*`tftp_server_address`*`:6970/CUPC/DirLookupDialRules.xml`.

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 the client.



CHAPTER 6

Cisco WebEx Meeting Integration

Configure Conferencing for a Cloud-Based Deployment Using Cisco WebEx Meeting Center

Configure the appropriate settings with the Cisco WebEx Administration Tool and assign the meeting and conferencing capabilities to the appropriate users.

Authentication with Cisco WebEx Meeting Center

You can use the following types of authentication with Cisco WebEx Meeting Center:

- Direct Authentication — The client can pass user credentials directly to Cisco WebEx Meeting Center.

  To enable direct authentication, complete the following steps:

  1. Create user accounts for Cisco WebEx Meeting Center using the Cisco WebEx Administration Tool.

     Cisco WebEx Meeting Center must validate user credentials in a direct authentication scenario. The user accounts hold the credentials so that Cisco WebEx Meeting Center can validate them when the client attempts to authenticate.

  2. Specify Cisco WebEx Meeting Center credentials in the client interface.

  See the *Overview of Loosely Coupled Integration* topic for more information.

Related Topics

Disable Instant WebEx Meeting Menu Option, on page 70

Specify Conferencing Credentials in the Client, on page 70

Disable Instant WebEx Meeting Menu Option

Procedure

Step 1 Remove one of the following registry keys to disable Instant WebEx Meeting menu option.

- 64 bit versions of Windows—
  `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Communicator\SessionManager\Apps\{7DE5E338-CF87-4824-810D-3822EDEFE97E}`
- 32 bit versions of Windows—
  `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Communicator\SessionManager\Apps\{7DE5E338-CF87-4824-810D-3822EDEFE97E}`

Step 2 Restart the client for this to take effect.

Related Topics

Authentication with Cisco WebEx Meeting Center, on page 69
Specify Conferencing Credentials in the Client, on page 70

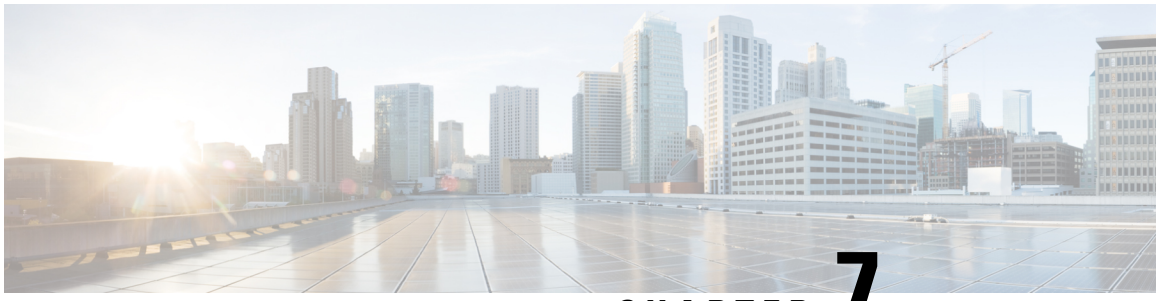
Specify Conferencing Credentials in the Client

Users can specify their credentials in the **Meetings** tab on the **Options** window.

To open the **Options** window, select **File** > **Options**.

Related Topics

Authentication with Cisco WebEx Meeting Center, on page 69
Disable Instant WebEx Meeting Menu Option, on page 70



CHAPTER 7

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 8, 32 bit and 64 bit
- Microsoft Windows 7, 32 bit and 64 bit

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

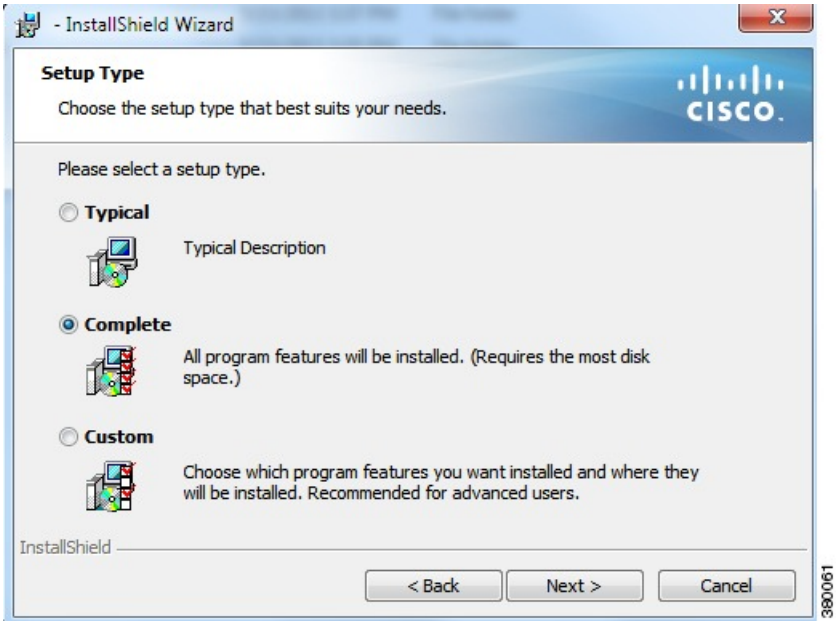
You can run the MSI manually on the file system of the client computer and then specify connection properties when you start Cisco UC Integration for Microsoft Lync for the first time.

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 include or exclude Click to Call.



By default, Click to Call functionality is installed when you use the command line to install Cisco UC Integration for Microsoft Lync. To install the client without the Click to Call functionality, use the `INSTALLLEVEL=100` argument.

For example: `msiexec.exe /i CUCILyncSetup.msi INSTALLLEVEL=100 /quiet`

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.
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. See the *LCID for Languages* topic for a full list of the languages that you can specify. 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. The regional language is set at **Control Panel** > **Region and Language** > **Change the date, time, or number format** > **Formats tab** > **Format dropdown**> >> > . See the *Supported Languages* topic for a full list of the languages you can specify.

Argument	Value	Description

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`
		Note There is a known limitation for this functionality in virtualized environments. Cisco UC Integration for Microsoft Lync must be started once and then the HVD needs to be restarted before this functionality will work.

FORGOT_PASSWORD_URL	URL	Specifies the URL to which users are directed if they forget, or need to reset, their passwords. This argument is optional but recommended.
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.
PRESENCE_DOMAIN	Domain name used	Specifies the domain name used to resolve the contacts on the active directory. For example *domain.com*.
VOICEMAIL_ENABLED	true false	Specifies if voicemail is enabled. • true (default)—Enables voicemail. • false—Disables voicemail.

Argument	Value	Description
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 Required: 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 Required: 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`.
   1. Select **File** > **Open**.
   2. Browse to the location of `CUCILyncSetup.msi` on your file system.
   3. 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.

Custom Presence Status

Cisco UC Integration for Microsoft Lync includes the custom presence status of **On the Phone**. This status is configured by the *custompresence.xml* file, which is installed with the application. The default location for this file is *C:\Program Files (x86)\Cisco Systems\CUCILync\custompresence.xml*. On 32-bit Windows installations, the file is located at *C:\Program Files\CiscoSystems\CUCILync\custompresence.xml*

Microsoft Lync 2010 cannot use this file by default because the registry key which defines the location of the custom presence file is ignored by Microsoft Lync 2010 unless it begins with ***https://***. Therefore, administrators have two options for deploying the custom presence file:

1. Deploy the *custompresence.xml* file to a secure web server such as the instance of Microsoft Internet Information Services that runs on the Microsoft Lync Server and update the registry value ***HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Communicator\CustomStateURL*** for Microsoft Lync 2010 or ***HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Office\15.0\Lync\CustomStateURL*** for Microsoft Lync 2013 with this location for all Lync users. See these Microsoft sites for more information:
   - http://www.microsoft.com/DOWNLOADS/details.aspx?familyid=5D6F4B90-6980-430B-9F97-FFADBC07B7A9&displaylang=en
   - http://www.microsoft.com/downloads/details.aspx?FamilyID=dd3cae08-3153-4c6a-a314-daa79d616248&displaylang=en
2. Administrators can use the *custompresence.xml* file installed on the local machine if they currently are not using the Lync SIP High Security Mode or use of the Lync SIP High Security Mode is not necessary. Lync SIP High Security Mode is disabled in the Windows Registry by setting the ***EnableSIPHighSecurityMode*** value to zero (0). This value is located in ***HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Communicator*** for Microsoft Lync 2010 or ***HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Office\15.0\Lync*** for Microsoft Lync 2013.

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. Cisco UC Integration for Microsoft Lync sends audio media and video media on your network with minimum latency or packet loss.

Traffic Marking

For each audio call or video call, 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.

Desk Phone Video Capabilities

To enable desk phone video capabilities, install Cisco Media Services Interface. 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

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

- 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.

  Not all devices on your network must support Cisco Medianet. The first hop prioritizes traffic based on the metadata attributes from Cisco Media Services Interface. As the traffic traverses the network, all other devices 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.

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:

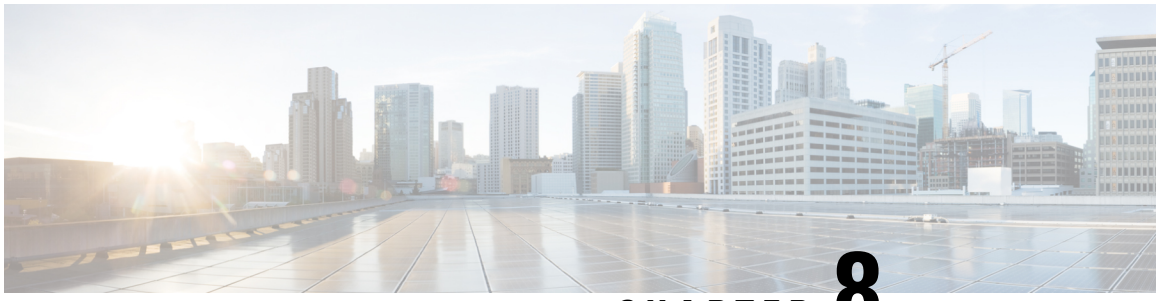
Option	Command

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.

Option	Command

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 8

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

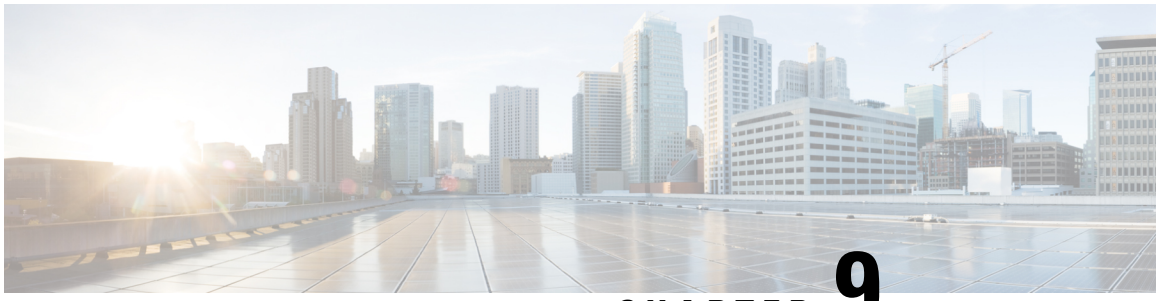
See the Installation chapter for more information about the command line arguments.

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 9

Deployment Configuration

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>
 <Directory>
  <parameter_name>value</parameter_name>
 </Directory>
 <Options>
  <parameter_name>value</parameter_name>
 </Options>
 <Phone>
  <parameter_name>value</parameter_name>
 </Phone>
 <Policies>
  <parameter_name>value</parameter_name>
 </Policies>
 <Voicemail>
```

```
  <parameter_name>value</parameter_name>
 </Voicemail>
</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.
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.
Phone	Parent element that contains configuration parameters for phone services.
Policies	Parent element that contains policy configuration parameters.
Voicemail	Parent element that contains voicemail 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*
jabber-plugin-config	Plug-in definition	Contains plug-in configuration elements. You can define custom embedded tabs to display HTML content in Cisco UC Integration for Microsoft Lync. For more information, see *Custom Embedded Tabs*.

Client Configuration Example

The following is an example client configuration:

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

```
 <jabber-plugin-config>
  <browser-plugin>
  <page refresh="true" preload="true">
   <tooltip>Cisco</tooltip>
   <icon>http://www.cisco.com/web/fw/i/logo.gif</icon>
   <url>www.cisco.com</url>
  </page>
  </browser-plugin>
 </jabber-plugin-config>
</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
Firstname	givenName
Lastname	sn
EmailAddress	mail
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

Parameter	Default Value
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 Lync connects 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.
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.

Parameter	Value	Description
UseWindowsCredentials	0 1	Specifies if Cisco UC Integration for Microsoft Lync uses Microsoft Windows credentials. • 0—Use credentials you specify as the values for the ConnectionUsername and ConnectionPassword parameters. • 1—Use Microsoft Windows credentials. This is the default value.
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.

Parameter	Value	Description
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.
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.
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.

Parameter	Value	Description
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 Number Masks parameter

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

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. In the directory, this number is +(1) 408 555 0100. The following mask resolves the number: `+14081+(#) ### ### ####` The length of mask strings cannot exceed the size restriction for registry subkey names.

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

Element	Description
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 Photo Retrieval

Cisco UC Integration for Microsoft Lync retrieves contact photos with the following methods.

Note When you change a photo in the Active Directory, the photo can take up to 24 hours to refresh in the client.

URI substitution

The client dynamically builds a URL to contact photos with a directory attribute and a URL template.

To use this method, set the following values in your configuration file:

1. Specify true as the value of the **PhotoUriSubstitutionEnabled** parameter.
2. Specify a directory attribute to use as a dynamic token as the value of the **PhotoUriSubstitutionToken** parameter. For example,

   ```
   <PhotoUriSubstitutionToken>sAMAccountName</PhotoUriSubstitutionToken>
   ```

3. Specify the URL and the dynamic token as the value of the **PhotoUriWithToken** parameter. For example,

   ```
   <PhotoUriWithToken>http://staffphoto.example.com/sAMAccountName.jpg</PhotoUriWithToken>
   ```

With the example values in the preceding steps, the sAMAccountName attribute might resolve to msmith in your directory. Cisco UC Integration for Microsoft Lync then takes this value and replaces the token to build the following URL: `http://staffphoto.example.com/msmith.jpg`.

Binary Objects

Cisco UC Integration for Microsoft Lync retrieves the binary data for the photo from your database.

If you are using binary objects from Active Directory do not set **PhotoURiWithToken**.

To use this method to retrieve contact photos, specify the attribute that contains the binary data as the value of the **PhotoSource** parameter in the configuration. For example,

```
<PhotoSource>jpegPhoto</PhotoSource>
```

PhotoURL Attribute

Cisco UC Integration for Microsoft Lync retrieves a URL from a directory attribute.

To use this method to retrieve contact photos, specify the attribute that contains the photo URL as the value of the **PhotoSource** parameter in the configuration. For example,

```
<PhotoSource>photoUri</PhotoSource>
```

Contact Photo Parameters

The following table describes parameters for configuring how Cisco UC Integration for Microsoft Lync retrieves contact photos:

Parameter	Value	Description
PhotoUriSubstitutionEnabled	true false	Specifies if photo URI substitution is enabled. **true** Photo URI substitution is enabled. **false** Specifies if photo URI substitution is disabled. This is the default value.

Parameter	Value	Description
PhotoUriSubstitutionToken	Directory attribute	Specifies a directory attribute to insert in the photo URI; for example, sAMAccountName. Only the following attributes are supported for use with the PhotoURISubstitutionToken parameter: • Common Name • Display Name • First Name • Last Name • Nickname • Email Address • Photo Source • Business Phone • Mobile Phone • Home Phone • Preferred Phone • Other Phone • Title • Company Name • User Account Name • Domain Name • Location • Post Code • State • City • Street
PhotoUriWithToken	URI	Specifies a photo URI with a directory attribute as a variable value; for example, `http://staffphoto.example.com/sAMAccountName.jpg`. To configure photo URI substitution, you set the directory attribute as the value of PhotoUriSubstitutionToken. The client must be able to retrieve the photos from the web server without credentials

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(default)—Cisco UC Integration for Microsoft Lync does not use the SipUri parameter.
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.
SipUri	mail msRTCSIP-PrimaryUserAddress	Specifies the directory attribute field that the IM Address scheme field is mapped to. To ensure that contacts are resolved, the value from SipUri must match [UserID]@[domain]
PresenceDomain	Text string	Specifies the domain name used for creating instant messaging addresses for directory contacts. `username@domain`

When you specify a value for SipUri, ensure that the login user id matches with the value of the Contact ID in the

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 the primary Cisco Unified Communications Manager TFTP service where device configuration files reside. Set one of the following as the value: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*hostname.domain.com*)
TFTPServer2	IP address Hostname FQDN	Specifies the address of the secondary Cisco Unified Communications Manager TFTP service where device configuration files reside. Set one of the following as the value: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*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.
CtiServer2	IP address Hostname FQDN	Specifies the address of the secondary CTI server.

Parameter	Value	Description
CcmcipServer1	IP address Hostname FQDN	Specifies the address of the primary 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.
CcmcipServer2	IP address Hostname FQDN	Specifies the address of the secondary CCMCIP server.
useCUCMGroupForCti	true false	Specifies if the Cisco Unified Communications Manager Group handles load balancing for CTI servers. Set one of the following values: • true — The Cisco Unified Communications Manager Group handles CTI load balancing. You should set this value in phone mode deployments only. In full UC mode, the presence server automatically handles CTI load balancing. • false (default) — The Cisco Unified Communications Manager Group does not handle CTI load balancing.

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 CCMCIP, CTI, TFTP servers, and useCUCMGroupForCti values from the Microsoft Windows registry. The following registry values can be used to specify these servers:

- `TftpServer1`
- `TftpServer2`
- `CtiServer1`
- `CtiServer2`
- `CcmcipServer1`
- `CcmcipServer2`
- `useCUCMGroupForCti`

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.

Policy Parameters

The following table describes the parameters you can specify within the Policies element in the configuration file:

Parameter	Value	Description
EnableCallPickup	true false	Specifies if a user can pickup a call in their call pickup group. • true—Enables call pickup. • false (default)—Disables call pickup. Example: `<EnableCallPickup>true </EnableCallPickup>`
EnableGroupCallPickup	true false	Specifies if a user can pickup incoming calls in another call pickup group, by entering the call pickup group number. • true—Enables group call pickup. • false (default)—Disables group call pickup. Example: `<EnableGroupCallPickup>true </EnableGroupCallPickup>`
EnableOtherGroupPickup	true false	Specifies if a user can pickup an incoming call in a group that is associated with their own call pickup group. • true—Enables other group call pickup. • false (default)—Disables other group call pickup. Example: `<EnableOtherGroupPickup>true </EnableOtherGroupPickup>`
EnableHuntGroup	true false	Specifies if a user can log into a hunt group. • true—Users can log into their hunt group. • false (default)—Users cannot log into their hunt group. Example: `<EnableHuntGroup>true</EnableHuntGroup>`

Parameter	Value	Description
PreventDeclineOnHuntCall	true false	Specifies if the Decline button is displayed for an incoming call in a hunt group. • true—Decline button is not displayed for an incoming call in a hunt group. • false (default)—Decline button is displayed for an incoming call in a hunt group. Example: <PreventDeclineOnHuntCall>true</PreventDeclineOnHuntCall>
TelemetryCustomerID	String	Specifies the source of analytic information. This can be a string that explicitly identifies an individual customer or a string that identifies a common source without identifying the customer. Cisco recommends using a Global Unique Identifier (GUID) generating utility to generate a 36 character unique identifier or to use a reverse domain name. The following utilities are available for generating a GUID: • Mac OS X - uuidgen • Linux - uuidgen • Microsoft Windows - [guid]::NewGuid().ToString() or (from cmd.exe) powershell -command "[guid]::NewGuid().ToString()" • Online - guid.us This identifier should be globally unique regardless of the method used to create the GUID. Example: <TelemetryCustomerID>customerIdentifier</TelemetryCustomerID>
SSO_Enabled	TRUE FALSE	Specifies whether users sign in by using single sign-on (SSO). • TRUE (default)—Users sign in by using SSO. • FALSE—Users do not use SSO to sign in. Example: <SSO_Enabled>FALSE</SSO_Enabled>
EnableSIPURIDialling	true false	Enables URI dialing with Cisco UC Integration for Microsoft Lync and allows users to make calls with URIs. • true—Users can make calls with URIs. • false (Default)—Users can't make calls with URIs. Example: <EnableSIPURIDialling>true</EnableSIPURIDialling>

Parameter	Value	Description
ServicesDomainSsoEmailPrompt	ON OFF	Specifies whether the user is shown the email prompt for the purposes of determining their home cluster. • ON—The prompt is shown. • OFF (default)—The prompt is not shown. Example: <ServicesDomainSsoEmailPrompt>ON</ServicesDomainSsoEmailPrompt>

Voicemail Parameters

The following table describes the voicemail service configuration parameters you can specify within the Voicemail element:

Parameter	Value	Description
VoicemailPrimaryServer	Hostname IP address FQDN	Specifies the address of your voicemail server. Set one of the following as the value: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*hostname.domain.com*)

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.

Parameter	Value	Description
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.
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: **[5-90]\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.

Custom Embedded Tabs

Custom embedded tabs display HTML content in the client interface. Learn how to create custom embedded tab definitions for Cisco UC Integration for Microsoft Lync.

Custom Embedded Tab Definitions

The custom embedded tab can only be configured using the `jabber-config.xml` file. The following XML snippet shows the structure for custom tab definitions:

```
<jabber-plugin-config>
 <browser-plugin>
  <page refresh="" preload="">
   <tooltip></tooltip>
   <icon></icon>
   <url></url>
  </page>
 </browser-plugin>
</jabber-plugin-config>
```

TESTBCisco Jabber for Windows supports Internet Explorer version 9 or earlier. The client uses Internet Explorer in version 9 mode if a later version is on the workstation.

The following table describes the parameters for custom embedded tab definitions:

Parameter	Description
browser-plugin	Contains all definitions for custom embedded tabs. The value includes all custom tab definitions.
page	Contains one custom embedded tab definition.
refresh	Controls when the content refreshes. • true — Content refreshes each time users select the tab. • false (default) — Content refreshes when users restart the client or sign in. This parameter is optional and is an attribute of the page element.
preload	Controls when the content loads. • true — Content loads when the client starts. • false (default) — Content loads when users select the tab. This parameter is optional and is an attribute of the page element.
tooltip	Defines hover text for the custom embedded tab. This parameter is optional. If you do not specify the hover text, the client will use *Custom tab*. The value is string of unicode characters.
icon	Specifies an icon for the tab. You can specify a local or hosted icon as follows: • Local icon—Specify the URL as follows: `file://file_path/icon_name` • Hosted icon—Specify the URL as follows: `http://path/icon_name` You can use any icon that the client browser can render, including .JPG, .PNG, and .GIF formats. This parameter is optional. If you do not specify an icon, the client loads the favicon from the HTML page. If no favicon is available, the client loads the default icon.
url	Specifies the URL where the content for the embedded tab resides. The client uses the browser rendering engine to display the content of the embedded tab. For this reason, you can specify any content that the browser supports. This parameter is required.

User Custom Tabs

Users can create their own custom embedded tabs through the client user interface.

You must enable users to create custom embedded tabs. Set true as the value for the AllowUserCustomTabs parameter in your configuration file as follows:

```
<Options>
  <AllowUserCustomTabs>true</AllowUserCustomTabs>
</Options>
```

Note User custom embedded tabs are set to true by default.

Custom Icons

To achieve optimal results, your custom icon should conform to the following guidelines:

- Dimensions: 20 x 20 pixels
- Transparent background
- PNG file format

UserID Tokens

You can specify the `${UserID}` token as part of the value for the url parameter. When users sign in, the client replaces the `${UserID}` token with the username of the logged in user.

Tip You can also specify the `${UserID}` token in query strings; for example, `www.cisco.com/mywebapp.op?url=${UserID}`.

The following is an example of how you can use the `${UserID}` token:

1. You specify the following in your custom embedded tab:

   ```
   <url>www.cisco.com/${UserID}/profile</url>
   ```

2. Mary Smith signs in. Her username is msmith.
3. The client replaces the `${UserID}` token with Mary's username as follows:

   ```
   <url>www.cisco.com/msmith/profile</url>
   ```

JavaScript Notifications

You can implement JavaScript notifications in custom embedded tabs. This topic describes the methods the client provides for JavaScript notifications. This topic also gives you an example JavaScript form that you can use to test notifications. It is beyond the scope of this documentation to describe how to implement JavaScript notifications for asynchronous server calls and other custom implementations. You should refer to the appropriate JavaScript documentation for more information.

Notification Methods

The client includes an interface that exposes the following methods for JavaScript notifications:

- SetNotificationBadge — You call this method from the client in your JavaScript. This method takes a string value that can have any of the following values:
  - Empty — An empty value removes any existing notification badge.
  - A number from 1 to 999
  - Two digit alphanumeric combinations, for example, A1
- onPageSelected() — The client invokes this method when users select the custom embedded tab.
- onPageDeselected() — The client invokes this method when users select another tab.

Note Not applicable for Jabber for iPhone and iPad

Show Call Events in Custom Tabs

You can use the following JavaScript function to show call events in a custom tab:

OnTelephonyConversationStateChanged — An API in the telephony service enables the client to show call events in a custom embedded tab. Custom tabs can implement the `OnTelephonyConversationStateChanged` JavaScript function. The client calls this function every time a telephony conversation state changes. The function accepts a JSON string that the client parses to get call events.

The following snippet shows the JSON that holds the call events:

```
{
      "conversationId": string,
      "acceptanceState": "Pending" | "Accepted| | "Rejected",
      "state": "Started" | "Ending" | "Ended",
      "callType": "Missed" | "Placed" | "Received" | "Passive" | "Unknown",
      "remoteParticipants": [{participant1}, {participant2}, …, {participantN}],
      "localParticipant": {
      }
}
```

Each participant object in the JSON can have the following properties:

```
{
      "voiceMediaDisplayName": "<displayName>",
      "voiceMediaNumber": "<phoneNumber>",
      "translatedNumber": "<phoneNumber>",
      "voiceMediaPhoneType": "Business" | "Home" | "Mobile" | "Other" | "Unknown",
      "voiceMediaState": "Active" | "Inactive" | "Pending" | "Passive" | "Unknown",
}
```

The following is an example implementation of this function in a custom embedded tab. This example gets the values for the `state` and `acceptanceState` properties and shows them in the custom tab.

```
function OnTelephonyConversationStateChanged(json) {
      console.log("OnTelephonyConversationStateChanged");
      try {
        var conversation = JSON.parse(json);
        console.log("conversation id=" + conversation.conversationId);
        console.log("conversation state=" + conversation.state);
        console.log("conversation acceptanceState=" + conversation.acceptanceState);
        console.log("conversation callType=" + conversation.callType);
```

```
      }
      catch(e) {
        console.log("cannot parse conversation:" + e.message);
      }
    }
```

The following is an example implementation of this function with all possible fields:

```
function OnTelephonyConversationStateChanged(json) {
      console.log("OnTelephonyConversationStateChanged");
      try {
        var conversation = JSON.parse(json);
        console.log("conversation state=" + conversation.state);
        console.log("conversation acceptanceState=" + conversation.acceptanceState);
        console.log("conversation callType=" + conversation.callType);
        for (var i=0; i<conversation.remoteParticipants.length; i++) {
          console.log("conversation remoteParticipants[" + i + "]=");
          console.log("voiceMediaDisplayName=" +
conversation.remoteParticipants[i].voiceMediaDisplayName);
          console.log("voiceMediaNumber=" +
conversation.remoteParticipants[i].voiceMediaNumber);
          console.log("translatedNumber=" +
conversation.remoteParticipants[i].translatedNumber);
          console.log("voiceMediaPhoneType=" +
conversation.remoteParticipants[i].voiceMediaPhoneType);
          console.log("voiceMediaState=" +
conversation.remoteParticipants[i].voiceMediaState);
        }
        console.log("conversation localParticipant=");
        console.log("  voiceMediaDisplayName=" +
conversation.localParticipant.voiceMediaDisplayName);
       console.log("  voiceMediaNumber=" + conversation.localParticipant.voiceMediaNumber);

       console.log("  translatedNumber=" + conversation.localParticipant.translatedNumber);

        console.log("  voiceMediaPhoneType=" +
conversation.localParticipant.voiceMediaPhoneType);
        console.log("  voiceMediaState=" + conversation.localParticipant.voiceMediaState);
      }
      catch(e) {
        console.log("cannot parse conversation:" + e.message);
      }
    }
```

Custom Embedded Tab Example

The following is an example of a configuration file with one embedded tab:

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
 <Client>
  <jabber-plugin-config>
   <browser-plugin>
     <page refresh ="true" preload="true">
     <tooltip>Cisco</tooltip>
     <icon>https://www.cisco.com/web/fw/i/logo.gif</icon>
     <url>https://www.cisco.com</url>
    </page>
   </browser-plugin>
  </jabber-plugin-config>
 </Client>
</config>
```

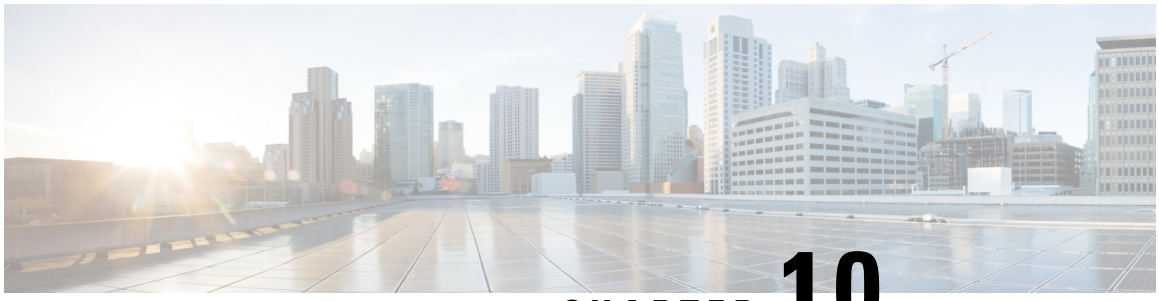
Configuration File Example

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>
```

Registry Key Configuration

Cisco UC Integration for Microsoft Lync supports obtaining the parameters listed in this document in the Windows registry. 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.



CHAPTER 10

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. Registry key values for TFTP and CCMCIP servers are only supported at this time.

Configuration File Is Not Downloaded from the TFTP Server

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:
    1. Open the **Cisco Unified OS Administration** interface.
    2. Select **Software Upgrades** > **TFTP File Management**.
    3. Select **Upload File**.
    4. Select **Browse** in the **Upload File** section.
    5. Select the configuration file on the file system.
    6. Leave the value of the **Directory** text box empty to host the configuration file in the default directory of your TFTP server.
    7. 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.

Microsoft Outlook Contacts Are Not Displayed in Search Results

Problem description: Microsoft Outlook contacts are not displayed 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 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.

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