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.

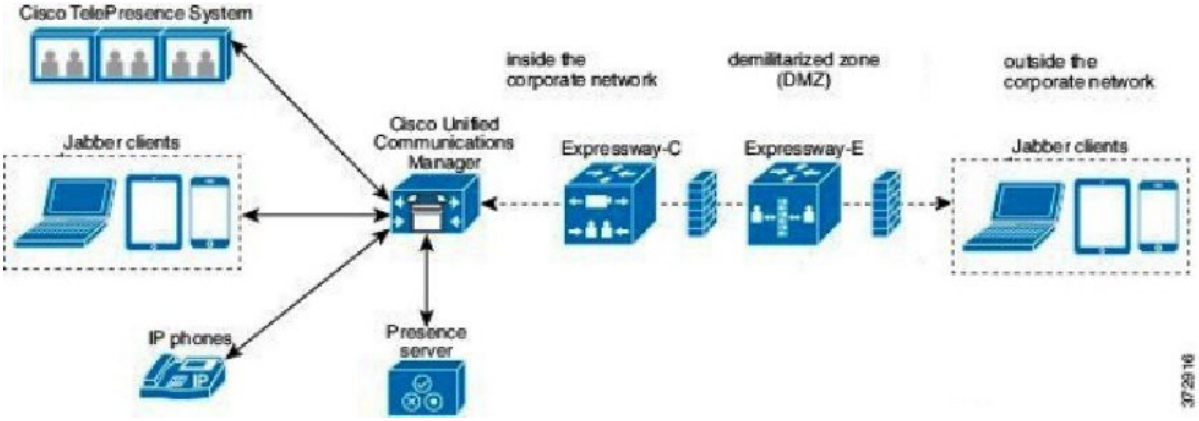
      To add a server to the Cisco Expressway-C whitelist, use the **HTTP server allow** setting.

      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`

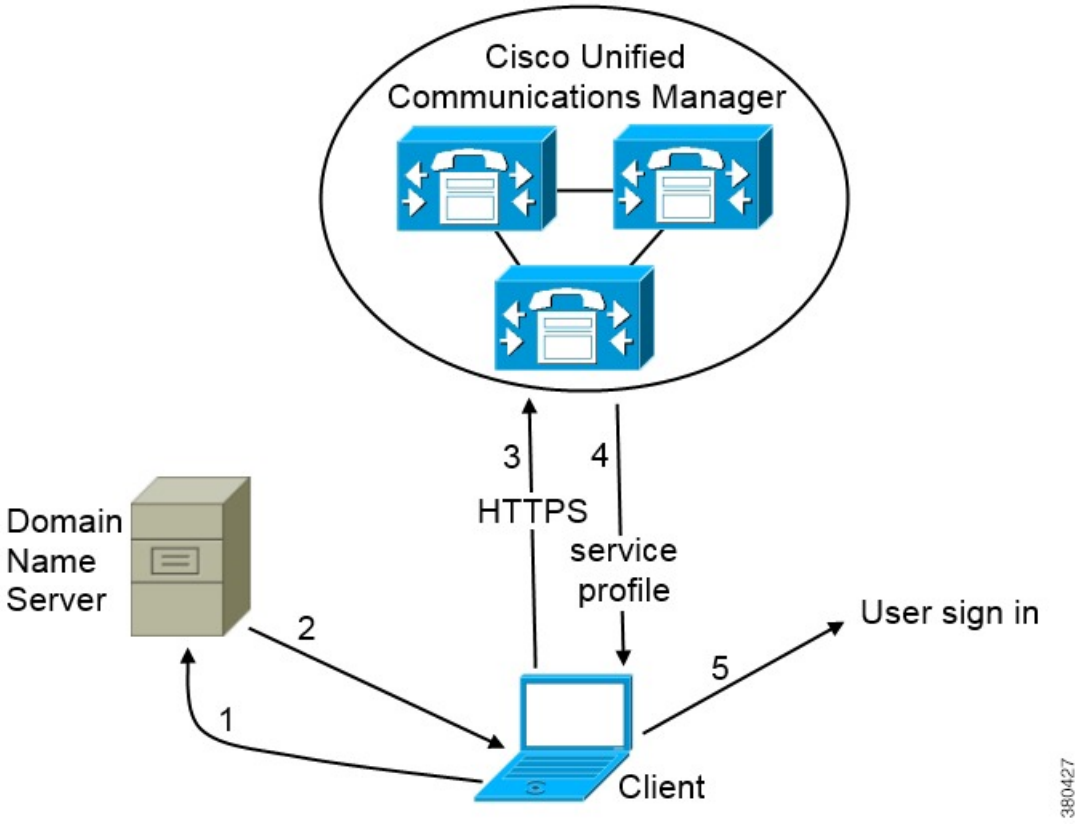
The client caches the results of the DNS query to load on subsequent launches.

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.