Deployment and Installation Guide for Cisco Jabber, Release 10.5

First Published: 2014-08-14

Last Modified: 2017-12-06

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

PART I

Deployment

CHAPTER 1

Cisco Jabber Overview

About Cisco Jabber

Cisco Jabber is a suite of Unified Communications applications that allow seamless interaction with your contacts from anywhere. Cisco Jabber offers IM, presence, audio and video calling, voicemail, and conferencing.

The applications in the Cisco Jabber family of products are:

- Cisco Jabber for Android
- Cisco Jabber for iPhone and iPad
- Cisco Jabber for Mac
- Cisco Jabber for Windows

For more information about the Cisco Jabber suite of products, see https://www.cisco.com/go/jabber.

Cisco Jabber Features

Cisco Jabber has a broad range of features across all clients. These common features include:

- Instant Messaging
- Presence
- Voice and Video Calling
- Voicemail
- Cisco WebEx Meetings integration
- Predictive Contact Search
- Single Sign-On
- Automatic Upgrades

- Instant Messaging Encryption
- Voice and Video Encryption
- Multiple Resource Login
- Expressway Mobile and Remote Access
- Service Discovery
- URI Dialing
- Telemetry

Individual clients also have specific features that are not available in all clients. These include:

- Cisco Jabber for Windows
    - Persistent Chat
    - Hunt Group
    - Call Pickup
    - Custom Contact
    - Video Desktop Share (BFCP)
- Cisco Jabber for Android and Cisco Jabber for iPhone and iPad
    - Dial via Office - Reverse
    - Send to Mobile
- Cisco Jabber for Mac
    - Video Desktop Share (BFCP)

Related Topics

Telemetry, on page 2

Telemetry

Cisco Jabber Analytics

Applies to: All clients

To improve your experience and product performance, Cisco Jabber may collect and send non-personally identifiable usage and performance data to Cisco. The aggregated data is used by Cisco to understand trends in how Jabber clients are being used and how they are performing.

You must install the following root certificate to use the telemetry feature: `GoDaddy Class 2 Certification Authority Root Certificate`. The telemetry server certificate name is "metrics-a.wbx2.com". To resolve any warnings about this certificate name, install the required GoDaddy certificate. For more information about certificates, see the Planning Guide.

By default, the telemetry data is on. You can configure the following telemetry parameters:

- Telemetry_Enabled—Specifies whether analytics data is gathered. The default value is true.
- TelemetryEnabledOverCellularData—Specifies whether analytics data is sent over cellular data and Wi-Fi (true), or Wi-Fi only (false). The default value is true.
- TelemetryCustomerID—This optional parameter specifies the source of analytic information. This ID can be a string that explicitly identifies an individual customer, or a string that identifies a common source without identifying the customer. We recommend using a tool that generates a *Global Unique Identifier* (GUID) to create a 36 character unique identifier, or to use a reverse domain name.

For more information about these parameters, see the *Parameters Reference Guide*.

Full details on what analytics data Cisco Jabber does and does not collect can be found in the Cisco Jabber Supplement to Cisco's On-Line Privacy Policy at https://www.cisco.com/web/siteassets/legal/privacy_02Jun10.html.

Related Topics

Cisco Jabber Features, on page 1
About Certificate Validation, on page 307
Policies Parameters, on page 345

CHAPTER 2

Requirements

Planning Considerations

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.

3. If you deploy a hybrid cloud-based architecture where the domain of the IM and presence server differs from the domain of the voice server, ensure that you configure the Voice Services Domain.

   The Voice Services Domain allows the client to locate the DNS server that contains the `_collab-edge` record.

   You can configure the voice services domain using one of the following methods:

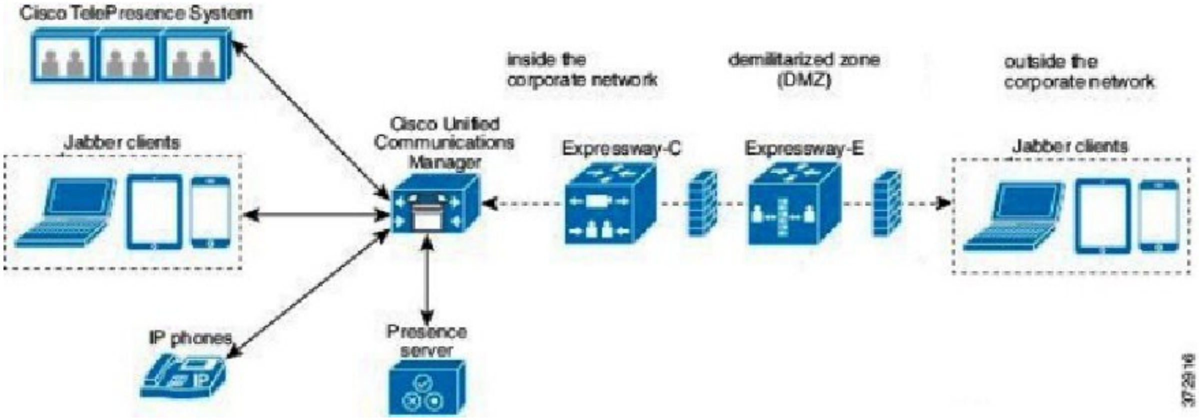
   - Client configuration file (all Cisco Jabber clients)
   - Configuration URL (all Cisco Jabber clients except Cisco Jabber for Windows)
   - Installer options (Cisco Jabber for Windows only)

Important In most cases, users can sign in to the client for the first time using Expressway for Mobile and Remote Access to connect to services from outside the corporate firewall. In the following cases, however, users must perform initial sign in while on the corporate network:

- If the voice services domain is different from the services domain. In this case, users must be inside the corporate network to get the correct voice services domain from the jabber-config.xml file.
- If the client needs to complete the CAPF enrollment process, which is required when using a secure or mixed mode cluster.

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 TelePresence System
inside the corporate network
demilitarized zone (DMZ)
outside the corporate network
Jabber clients
Cisco Unified Communications Manager
Expressway-C
Expressway-E
Jabber clients
IP phones
Presence server
372916

Related Topics

- Cisco Expressway Configuration Guides
- Cisco VCS Configuration Guides

Supported Services

The following table summarizes the services and functionality that are supported when the client uses Expressway for Mobile and Remote Access to remotely connect to Cisco Unified Communications Manager.

Table 1: Summary of supported services for Expressway for Mobile and Remote Access

Service		Supported	Unsupported
Directory			
	UDS directory search	X	
	LDAP directory search		X
	Directory photo resolution	X * Using HTTP white list on Cisco Expressway-C	
	Intradomain federation	X * Contact search support depends of the format of your contact IDs. For more information, see the note below.	
	Interdomain federation	X	
Instant Messaging and Presence			

Service		Supported	Unsupported
	On-premises	X	
	Cloud	X	
	Chat	X	
	Group chat	X	
	High Availability: On-premises deployments	X	
	File transfer: On-premises deployments		X
	File transfer: Cloud deployments	X Desktop clients, some file transfer features are supported for mobile clients.	
	Video desktop share - BFCP	X (Cisco Jabber for mobile clients only support BFCP receive.)	
Audio and Video			
	Audio and video calls	X * Cisco Unified Communications Manager 9.1(2) and later	
	Deskphone control mode (CTI)		X
	Remote Desktop Control		X
	Extend and connect		X
	Dial via Office - Reverse		X
	Session persistency		X
	Early media		X
	Self Care Portal access		X
Voicemail			
	Visual voicemail	X * Using HTTP white list on Cisco Expressway-C	

Service		Supported	Unsupported
Cisco WebEx Meetings			
	On-premises		X
	Cloud	X	
	Cisco WebEx desktop share	X	
Installation			
	Installer update	X * Using HTTP white list on Cisco Expressway-C	
Customization			
	Custom HTML tabs	X * Using HTTP white list on Cisco Expressway-C (Desktop clients only)	
Security			
	End-to-end encryption		X
	CAPF enrollment		X
Troubleshooting			
	Problem report generation	X	
	Problem report upload		X
High Availability (failover)			
	Audio and Video services		X
	Voicemail services		X
	IM and Presence services	X	

Directory

When the client connects to services using Expressway for Mobile and Remote Access, it supports directory integration with the following limitations.

- LDAP contact resolution —The client cannot use LDAP for contact resolution when outside of the corporate firewall. Instead, the client must use UDS for contact resolution.

  When users are inside the corporate firewall, the client can use either UDS or LDAP for contact resolution. If you deploy LDAP within the corporate firewall, Cisco recommends that you synchronize your LDAP directory server with Cisco Unified Communications Manager to allow the client to connect with UDS when users are outside the corporate firewall.

- Directory photo resolution — To ensure that the client can download contact photos, you must add the server on which you host contact photos to the white list of your Cisco Expressway-C server. To add a server to Cisco Expressway-C white list, use the **HTTP server allow** setting. For more information, see the relevant Cisco Expressway documentation.
- Intradomain federation — When you deploy intradomain federation and the client connects with Expressway for Mobile and Remote Access from outside the firewall, contact search is supported only when the contact ID uses one of the following formats:
    - sAMAccountName@domain
    - UserPrincipleName (UPN)@domain
    - EmailAddress@domain
    - employeeNumber@domain
    - telephoneNumber@domain
- Interdomain federation using XMPP — The client does not support interdomain federation with XMPP standard-based environments such as Google Talk when it connects with Expressway for Mobile and Remote Access from outside the firewall.

Instant Messaging and Presence

When the client connects to services using Expressway for Mobile and Remote Access, it supports instant messaging and presence with the following limitations.

File transfer — The client does not support file transfer including screen capture with Cisco Unified Communications Manager IM and Presence Service deployments. File Transfer is supported only with Cisco WebEx cloud deployments with desktop clients. Managed File Transfer is supported with Cisco Unified Communication IM and Presence when Cisco Jabber is connected to Cisco Unified services using Expressway. Peer-to-Peer files transfer is not supported.

Audio and Video Calling

When the client connects to services using Expressway for Mobile and Remote Access, it supports voice and video calling with the following limitations.

- Cisco Unified Communications Manager — Expressway for Mobile and Remote Access supports video and voice calling with Cisco Unified Communications Manager Version 9.1.2 and later. Expressway for Mobile and Remote Access is not supported with Cisco Unified Communications Manager Version 8.x.
- Deskphone control mode (CTI) — The client does not support deskphone control mode (CTI), including extension mobility.
- Extend and connect — The client cannot be used to:
    - Make and receive calls on a Cisco IP Phone in the office.
    - Perform mid-call control such as hold and resume on a home phone, hotel phone, or Cisco IP Phone in the office.

- Dial via Office - Reverse — The client cannot make Dial via Office - Reverse calls from outside the firewall.
- Session Persistency — The client cannot recover from audio and video calls drop when a network transition occurs. For example, if a users start a Cisco Jabber call inside their office and then they walk outside their building and lose Wi-Fi connectivity, the call drops as the client switches to use Expressway for Mobile and Remote Access.
- Early Media — Early Media allows the client to exchange data between endpoints before a connection is established. For example, if a user makes a call to a party that is not part of the same organization, and the other party declines or does not answer the call, Early Media ensures that the user hears the busy tone or is sent to voicemail.

  When using Expressway for Mobile and Remote Access, the user does not hear a busy tone if the other party declines or does not answer the call. Instead, the user hears approximately one minute of silence before the call is terminated.
- Self care portal access — Users cannot access the Cisco Unified Communications Manager Self Care Portal when outside the firewall. The Cisco Unified Communications Manager user page cannot be accessed externally.

  Cisco Expressway-E proxies all communications between the client and unified communications services inside the firewall. However, the Cisco Expressway-E does not proxy services that are accessed from a browser that is not part of the Cisco Jabber application.

Voicemail

Voicemail service is supported when the client connects to services using Expressway for Mobile and Remote Access.

Note To ensure that the client can access voicemail services, you must add the voicemail server to the white list of your Cisco Expressway-C server. To add a server to Cisco Expressway-C white list, use the **HTTP server allow** setting. For more information, see the relevant Cisco Expressway documentation.

Cisco WebEx Meetings

When the client connects to services using Expressway for Mobile and Remote Access, it supports only cloud-based conferencing using Cisco WebEx Meetings Center.

The client cannot access the Cisco WebEx Meetings Server or join or start on-premises Cisco WebEx meetings.

Installation

When the client connects to services using Expressway for Mobile and Remote Access, it supports installer updates.

Note To ensure that the client can download installer updates, you must add the server that hosts the installer updates to the white list of your Cisco Expressway-C server. To add a server to the Cisco Expressway-C white list, use the **HTTP server allow** setting. For more information, see the relevant Cisco Expressway documentation.

Customization

When the client connects to services using Expressway for Mobile and Remote Access, it supports custom HTML tab configuration for desktop clients.

Note To ensure that the client can download the custom HTML tab configuration, you must add the server that hosts the custom HTML tab configuration to the white list of your Cisco Expressway-C server. To add a server to the Cisco Expressway-C whitelist, use the **HTTP server allow** setting. For more information, see the relevant Cisco Expressway documentation.

Security

When the client connects to services using Expressway for Mobile and Remote Access, it supports most security features with the following limitations.

- Initial CAPF enrollment — Certificate Authority Proxy Function (CAPF) enrollment is a security service that runs on the Cisco Unified Communications Manager Publisher that issues certificates to Cisco Jabber (or other clients). To successfully enrol for CAPF, the client must connect from inside the firewall or using VPN.
- End-to-end encryption — When users connect 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, if either Cisco Jabber or an internal device is not configured with Encrypted security mode.
  - Media is encrypted on the call path between the Expressway-C and devices that are registered locally to Cisco Unified Communnication Manager, if both Cisco Jabber and internal device are configured with Encypted security mode.

Troubleshooting

Problem report upload — When the desktop client connects to services using Expressway for Mobile and Remote Access, it cannot send problem reports because the client uploads problem reports over HTTPS to a specified internal server.

To work around this issue, users can save the report locally and send the report in another manner.

High Availability (failover)

High Availability means that if the client fails to connect to the primary server, it fails over to a secondary server with little or no interruption to the service. In relation to high availability being supported on the Expressway for Mobile and Remote Access, high availability refers to the server for the specific service failing over to a secondary server (such as Instant Messaging and Presence), and not the Cisco Expressway-E server itself failing over.

Some services are available on the Expressway for Mobile and Remote Access that are not supported for high availability. This means that if users are connected to the client from outside the corporate network and the instant messaging and presence server fails over, the services will continue to work as normal. However, if the audio and video server or voicemail server fails over, those services will not work as the relevant servers do not support high availability.

Deployment in a Virtual Environment

You can deploy Cisco Jabber for Windows in virtual environments using the following software:

- Citrix XenDesktop 7.5
- Citrix XenDesktop 7.1
- Citrix XenDesktop 7.0
- Citrix XenDesktop 5.6
- Citrix XenApp 7.5 Enterprise Edition for Windows Server 2008 R2 Standard Service Pack 1 64 bit, published desktop
- Citrix XenApp 6.5 Feature Pack 2 Enterprise Edition for Windows Server 2008 Service Pack 2 64 bit, published desktop
- Citrix XenApp 6.5 Feature Pack 1 Enterprise Edition for Windows Server 2008 R2 Standard Service Pack 1 64 bit, published desktop
- Citrix XenApp 6.5 Enterprise Edition for Windows Server 2008 R2 Standard Service Pack 1 64 bit, published desktop
- VMware Horizon View 6.0
- VMware Horizon View 5.3
- VMware Horizon View 5.2

Supported Features

- Instant messaging and presence with other Cisco Jabber clients
- Desk phone control
- Voicemail
- Presence integration with Microsoft Outlook 2007, 2010 and 2013

Note Cisco Jabber credentials caching is not supported when using Cisco Jabber in non-persistent virtual deployment infrastructure (VDI) mode.

Softphones in Virtual Environments

Use Cisco Virtualization Experience Media Engine (VXME) for softphone calls in a virtual environment.

Roaming Profiles

The client stores user data such as user call history and configuration store cache on the local machine for use when the user next signs in. In virtual environments, users do not always access the same virtual desktop. To guarantee a consistent user experience, these files need to be accessible every time the client is launched.

To preserve the user's personal settings in a virtual environment when roaming between hosted virtual desktops, use dedicated profile management solutions from Citrix and VMware.

Citrix Profile Management is a profile solution for Citrix environments. In deployments with random hosted virtual desktop assignments, Citrix Profile Management synchronizes each user's entire profile between the system it is installed on and the user store.

VMware View Persona Management preserves user profiles and dynamically synchronizes them with a remote profile repository. VMware View Persona Management does not require the configuration of Windows roaming profiles and can bypass Windows Active Directory in the management of View user profiles. Persona Management enhances the functionality of existing roaming profiles.

You can specify which files and folders to omit from synchronization by adding them to an exclusion list. To include a subfolder within an excluded folder, add the subfolder to an inclusion list.

To preserve the user's personal settings, do not exclude the following directories:

```
AppData\Local\Cisco
AppData\Local\JabberWerxCPP
AppData\Roaming\Cisco
AppData\Roaming\JabberWerxCPP
```

Client Information Storage

The client stores user information in the following locations:

`C:\Users\`*`username`*`\AppData\Local\Cisco\Unified Communications\Jabber\CSF`

Folder Name	Description
`Contacts`	Contact cache files
`History`	Call history and chat history
`Photo cache`	Caches the directory photos locally

`C:\Users\`*`username`*`\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF`

Folder Name	Description
`Config`	Maintains users' Jabber configuration files and stores configuration store cache
`Credentials`	Stores encrypted user name and password file

Related Topics

Calendar Integration, on page 53

How the Client Connects to Services

To connect to services, Cisco Jabber requires the following information:

- Source of authentication that enables users to sign in to the client.
- Location of services.

You can provide that information to the client with the following methods:

URL Configuration

Users are sent an email from their administrators. The email contains a URL that will configure the domain needed for service discovery.

Service Discovery

The client automatically locates and connects to services.

Manual Connection Settings

Users manually enter connection settings in the client user interface.

Recommended Connection Methods

The method that you should use to provide the client with the information it needs to connect to services depends on your deployment type, server versions, and product modes. The following tables highlight various deployment methods and how to provide the client with the necessary information.

Table 2: On-Premises Deployments for Cisco Jabber for Windows

Product Mode	Server Versions	Discovery Method	Non DNS SRV Record Method
Full UC (default mode)	Release 9.1.2 and later: • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	A DNS SRV request against `_cisco-uds .<domain>`	Use the following installer switches and values: • `AUTHENTICATOR=CUP` • `CUP_ADDRESS=` <presence_server_address>
Full UC (default mode)	Release 8.x: • Cisco Unified Communications Manager • Cisco Unified Presence	A DNS SRV request against `_cuplogin.<domain>`	Use the following installer switches and values: • `AUTHENTICATOR=CUP` • `CUP_ADDRESS=` <presence_server_address>
IM Only (default mode)	Release 9 and later: Cisco Unified Communications Manager IM and Presence Service	A DNS SRV request against `_cisco-uds .<domain>`	Use the following installer switches and values: • `AUTHENTICATOR=CUP` • `CUP_ADDRESS=` <presence_server_address>

Product Mode	Server Versions	Discovery Method	Non DNS SRV Record Method
IM Only (default mode)	Release 8.x: Cisco Unified Presence	A DNS SRV request against `_cuplogin .<domain>`	Use the following installer switches and values: • `AUTHENTICATOR=CUP` • `CUP_ADDRESS=` `<presence_server_address>`
Phone Mode	Release 9 and later: Cisco Unified Communications Manager	A DNS SRV request against `_cisco-uds.<domain>`	Use the following installer switches and values: • `AUTHENTICATOR=CUCM` • `TFTP=<CUCM_address>` • `CCMCIP=<CUCM_address>` • `PRODUCT_MODE=phone_mode` High availability is not supported using this method of deployment.
Phone Mode	Release 8.x: Cisco Unified Communications Manager	Manual connection settings	Use the following installer switches and values: • `AUTHENTICATOR=CUCM` • `TFTP=<CUCM_address>` • `CCMCIP=<CUCM_address>` • `PRODUCT_MODE=phone_mode` High availability is not supported using this method of deployment.

Cisco Unified Communications Manager release 9.x and earlier—If you enable Cisco Extension Mobility, the `Cisco Extension Mobility` service must be activated on the Cisco Unified Communications Manager nodes that are used for CCMCIP. For information about Cisco Extension Mobility, see the *Feature and Services* guide for your Cisco Unified Communications Manager release.

Note Cisco Jabber release 9.6 and later can still discover full Unified Communications and IM-only services using the `_cuplogin` DNS SRV request but a `_cisco-uds` request will take precedence if it is present.

Use the SERVICES_DOMAIN installer switch to specify the value of the domain where DNS records reside if you want users to bypass the email screen during the first login of a fresh installation.

Note The services domain is read from a cached configuration if you are upgrading from Cisco Jabber for Windows 9.2.

Table 3: On-Premises Deployments for Cisco Jabber for Mac

Product Mode	Server Versions	Discovery Method
Full UC (default mode)	Release 9 and later: • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	A DNS SRV request against `_cisco-uds.<domain>`
Full UC (default mode)	Release 8.x: • Cisco Unified Communications Manager • Cisco Unified Presence	A DNS SRV request against `_cuplogin.<domain>`

Table 4: On-Premises Deployments for Cisco Jabber for Android and Cisco Jabber for iPhone and iPad

Product Mode	Server Versions	Discovery Method
Full UC (default mode)	Release 9 and later: • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	A DNS SRV request against `_cisco-uds .<domain>` and `_cuplogin.<domain>`
Full UC (default mode)	Release 8.x: • Cisco Unified Communications Manager • Cisco Unified Presence	A DNS SRV request against `_cuplogin.<domain>`
IM Only (default mode)	Release 9 and later: Cisco Unified Communications Manager IM and Presence Service	A DNS SRV request against `_cisco-uds .<domain>` and `_cuplogin.<domain>`
IM Only (default mode)	Release 8.x: Cisco Unified Presence	A DNS SRV request against `_cuplogin .<domain>`
Phone mode	Release 9 and later: Cisco Unified Communications Manager	A DNS SRV request against `_cisco-uds.<domain>`
Phone mode	Release 8.x: Cisco Unified Communications Manager	Manual connection settings or bootstrap file Manual connection settings

Note Cisco Unified Communications Manager version 9 and later can still discover full Unified Communications and IM-only services using the `_cuplogin` DNS SRV request but a `_cisco-uds` request will take precedence if it is present.

Table 5: Hybrid Cloud-Based Deployments

Server Versions	Connection Method
Cisco Webex Messenger	HTTPS request against `https://loginp.webexconnect.com/cas/FederatedSSO?org=<domain>`

Table 6: Cloud-Based Deployments

Deployment Type	Connection Method
Enabled for single sign-on (SSO)	Cisco Webex Administration Tool Bootstrap file to set the SSO_ORG_DOMAIN argument.
Not enabled for SSO	Cisco Webex Administration Tool

Sources of Authentication

A source of authentication, or an authenticator, enables users to sign in to the client.

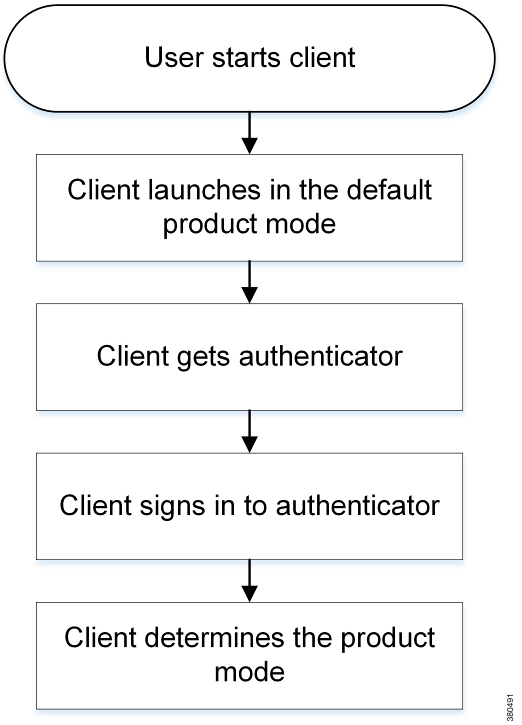
Three possible sources of authentication are as follows:

- Cisco Unified Communications Manager IM and Presence—On-premises deployments in either full UC or IM only.
- Cisco Unified Communications Manager—On-premises deployments in phone mode.
- Cisco Webex Messenger Service—Cloud-based or hybrid cloud-based deployments.

Initial Launch Sequence

On the initial launch after installation, Cisco Jabber starts in the default product mode. The client then gets an authenticator and signs the user in. After sign in, the client determines the product mode.

The following diagram illustrates the initial launch sequence:


User starts client
Client launches in the default product mode
Client gets authenticator
Client signs in to authenticator
Client determines the product mode
380491

How the Client Gets an Authenticator

Cisco Jabber looks for an authenticator as follows:

1. Client checks cache for manual settings.

   Users can manually enter authenticator through the client user interface.

2. Client checks cache to discover if the user's domain is a Webex organisation..

   The client chooses Webex as the authenticator.

3. Client makes a Webex cloud service HTTP request to discover if the user's organisation domain is a Webex organisation.

   The client chooses Webex as the authenticator.

4. Client checks cache for service discovery.

   The client loads settings from previous queries for service (SRV) records.

5. Client queries for SRV records.

   The client queries the DNS name server for SRV records to locate services.

   If the client finds the `_cisco-uds` SRV record, it can get the authenticator from the service profile.

If the client cannot get an authenticator, it prompts the user to manually select the source of authentication in the client user interface.

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. The client can retrieve service profiles from Cisco Unified Communications Manager to determine the authenticator.	• 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 mixed product modes. You can easily deploy users with full UC, IM only, or phone mode capabilities. • Supports Expressway for Mobile and Remote Access.

SRV Record	Purpose	Why You Deploy
`_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. The user employs one of the following methods to discover the service during the first sign in:

   - Manual—The user starts Cisco Jabber and then inputs an email-like address on the welcome screen.
   - URL configuration—URL configuration allows users to click on a link to cross-launch Cisco Jabber without manually inputting an email.
   - Mobile Configuration Using Enterprise Mobility Management—As an alternative to URL configuration, you can configure Cisco Jabber using Enterprise Mobility Management (EMM) with Android for Work on Cisco Jabber for Android and with Apple Managed App Configuration on Cisco Jabber for iPhone and iPad. You need to configure the same parameters in the EMM console that are used for creating URL configuration link.

   To create a URL configuration link, you include the following:

   - ServicesDomain—The domain that Cisco Jabber uses for service discovery.
   - VoiceServicesDomain—For a hybrid deployment, the domain that Cisco Jabber uses to retrieve the DNS SRV records can be different from the ServicesDomain that is used to discover the Cisco Jabber domain.
   - ServiceDiscoveryExcludedServices—In certain deployment scenarios, services can be excluded from the service discovery process. These values can be a combination of the following:
     - WEBEX
     - CUCM
     - CUP

Note

When all three parameters are included, service discovery does not happen and the user is prompted to manually enter connection settings.

Create the link in the following format:

```
ciscojabber://provision?ServicesDomain=<domain_for_service_discover>
&VoiceServicesDomain=<domain_for_voice_services>
&ServiceDiscoveryExcludedServices=<services_to_exclude_from_service_discover>
```

Examples:

- `ciscojabber://provision?servicesdomain=example.com`
- `ciscojabber://provision?servicesdomain=example.com &VoiceServicesDomain=VoiceServices.example.com`
- `ciscojabber://provision?servicesdomain=example.com &ServiceDiscoveryExcludedServices=WEBEX,CUCM`

Provide the link to users using email or a website.

Note

If your organization uses a mail application that supports cross-launching proprietary protocols or custom links, you can provide the link to users using email, otherwise provide the link to users using a website.

3. The client gets the address of the DNS name server from the DHCP settings.
4. The client issues an HTTP query to a Central Authentication Service (CAS) URL for the Cisco Webex Messenger service.

   This query enables the client to determine if the domain is a valid Cisco Webex domain.
5. 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.

The following is an example of an SRV record entry:

```
_cisco_uds._tcp.DOMAIN SRV service location:
 priority = 0
 weight = 0
 port = 8443
 svr hostname=192.168.0.26
```

Client Issues HTTP Query

In addition to querying the name server for SRV records to locate available services, the client sends an HTTP query to the CAS URL for the Cisco WebEx Messenger service. This request enables the client to determine cloud-based deployments and authenticate users to the Cisco WebEx Messenger service.

When the client gets a domain from the user, it appends that domain to the following HTTP query:

```
http://loginp.webexconnect.com/cas/FederatedSSO?org=
```

For example, if the client gets `example.com` as the domain from the user, it issues the following query:

```
http://loginp.webexconnect.com/cas/FederatedSSO?org=example.com
```

That query returns an XML response that the client uses to determine if the domain is a valid Cisco WebEx domain.

If the client determines the domain is a valid Cisco WebEx domain, it prompts users to enter their Cisco WebEx credentials. The client then authenticates to theCisco WebEx Messenger service and retrieves configuration and UC services configured in Cisco WebEx Org Admin.

If the client determines the domain is not a valid Cisco WebEx domain, it uses the results of the query to the name server to locate available services.

Note The client will use any configured system proxies when sending the HTTP request to the CAS URL. Proxy support for this request has the following limitations :

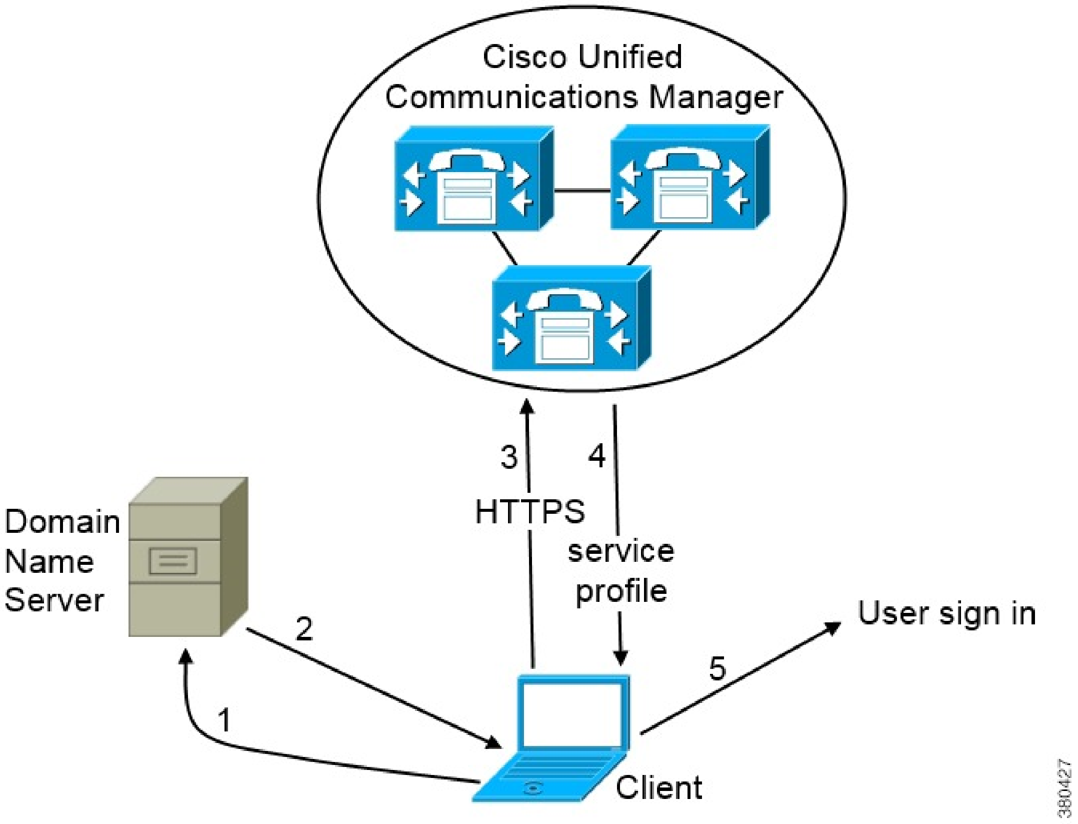
- Proxy Authentication is not supported.
- Wildcards in the bypass list are not supported. Use `example.com` instead of `*.example.com` for example.

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
```

Related Topics

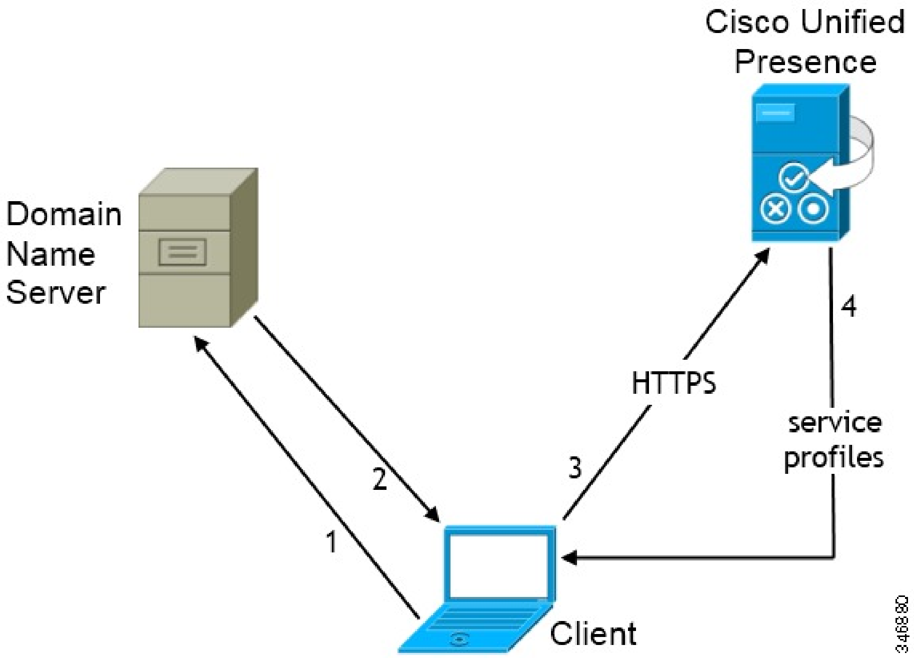
Remote Cluster Configuration on Cisco Unified Communications Manager 10.0

CUP Login SRV Record

Cisco Jabber can automatically discover and connect to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service with the `_cuplogin` SRV record.

The following figure shows how the client uses the `_cuplogin` SRV record.

Figure 3: CUP SRV Record Login Flow



1. The client queries the domain name server for SRV records.
2. The name server returns the `_cuplogin` SRV record.

   As a result, Cisco Jabber can locate the presence server and determine that Cisco Unified Presence is the authenticator.

3. The client prompts the user for credentials and authenticates to the presence server.
4. The client retrieves service profiles from the presence server.

Tip The `_cuplogin` SRV record also sets the default server address on the **Advanced Settings** window.

The following is an example of the `_cuplogin` SRV record:

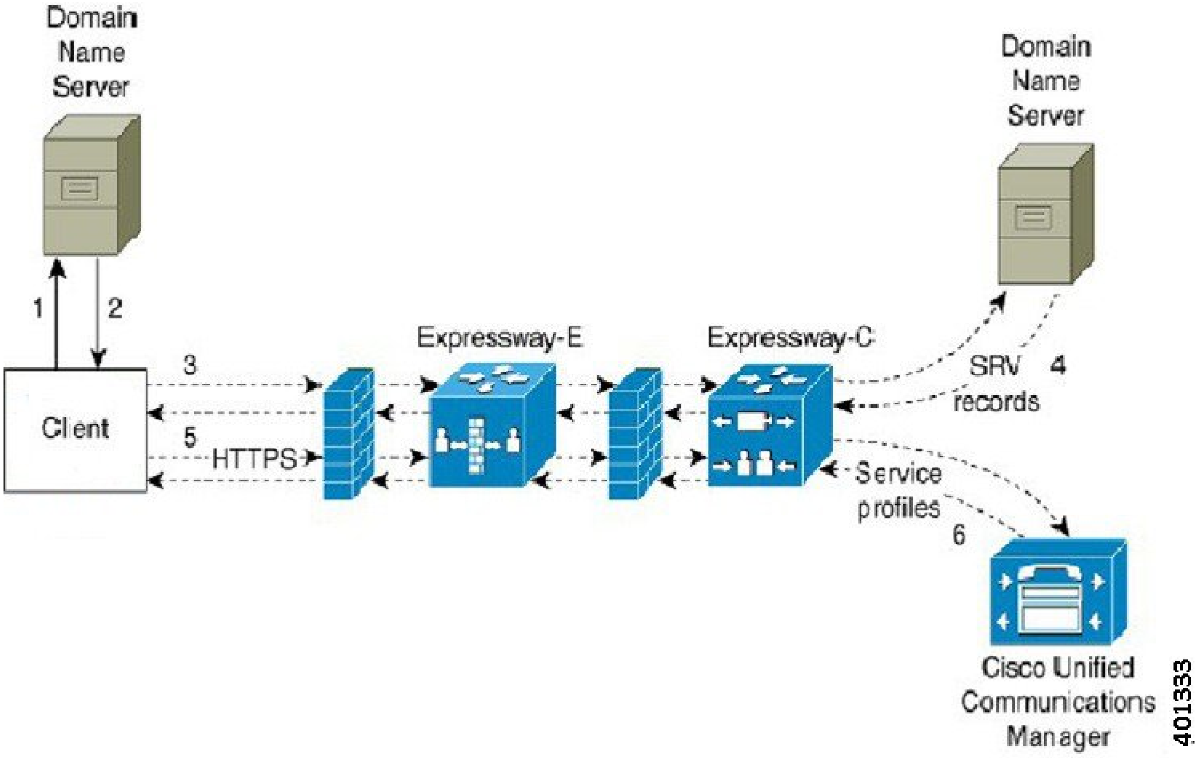
```
_cuplogin._tcp.example.com      SRV service location:
          priority       = 8
          weight         = 50
          port           = 8443
          svr hostname   = cup3.example.com
_cuplogin._tcp.example.com      SRV service location:
          priority       = 5
          weight         = 100
          port           = 8443
          svr hostname   = cup1.example.com
_cuplogin._tcp.example.com      SRV service location:
          priority       = 7
          weight         = 4
          port           = 8443
          svr hostname   = cup2.example.com
```

Collaboration Edge SRV Record

Cisco Jabber can attempt to connect to internal servers through Expressway for Mobile and Remote Access to discover services with the following `_collab-edge` SRV record.

The following figure shows how the client uses the `_collab-edge` SRV record.

Figure 4: Collaboration Edge Record Login Flow



1. The client queries the external domain name server for SRV records.
2. The name server returns the `_collab-edge` SRV record and does not return the `_cuplogin` or `_cisco-uds` SRV records.

   As a result, Cisco Jabber can locate the Cisco Expressway-E server.
3. The client requests the internal SRV records (through Expressway) from the internal domain name server.

   These SRV records must include the `_cisco-uds` SRV record.
4. The client obtains the internal SRV records (through Expressway).

   As a result, the client can locate the Cisco Unified Communications Manager server.
5. The client requests the service profiles (through Expressway) from Cisco Unified Communications Manager.
6. The client retrieves the service profiles (through Expressway) from Cisco Unified Communications Manager.

   The service profile contains the user's home cluster, the primary source of authentication, and the client configuration.

Configuration URL

You can create a configuration URL to make it easier for users to set up the client for the first time. Users can click this link to cross-launch Cisco Jabber without having to manually enter service discovery information.

To use this feature, you must create a URL and then distribute that URL to users.

Configuration URL

To enable users to launch Cisco Jabber without having to manually enter service discovery information, create and distribute a configuration URL to users.

You can provide a configuration URL link to users by emailing the link to the user directly, or by posting the link to a website.

Include the following parameters in the URL:

- ServicesDomain—Required. Every configuration URL must include the domain of the IM and presence server that Cisco Jabber needs for service discovery.
- VoiceServiceDomain—Required only if you deploy a hybrid cloud-based architecture where the domain of the IM and presence server differs from the domain of the voice server. Set this parameter to ensure that Cisco Jabber can discover voice services.
- ServiceDiscoveryExcludedServices—Optional. You can exclude any of the following services from the service discovery process:
  - Webex—When you set this value, the client:
    - Does not perform CAS lookup
    - Looks for:
      - `_cisco-uds`
      - `_cuplogin`
      - `_collab-edge`
  - CUCM—When you set this value, the client:
    - Does not look for `_cisco-uds`
    - Looks for:
      - `_cuplogin`
      - `_collab-edge`
  - CUP—When you set this value, the client:
    - Does not look for `_cuplogin`
    - Looks for:
      - `_cisco-uds`
      - `_collab-edge`

  You can specify multiple, comma-separated values to exclude multiple services.

  If you exclude all three services, the client does not perform service discovery and prompts the user to manually enter connection settings.

- ServicesDomainSsoEmailPrompt—Optional. Specifies whether the user is shown the email prompt for the purposes of determining their home cluster.
    - ON
    - OFF
- Telephony_Enabled—Specifies whether the user has phone capability or not. The default is true.
    - True
    - False
- ForceLaunchBrowser—Used to force user to use the external browser. Applies to Cisco Jabber mobile clients.
    - True
    - False

    Note ForceLaunchBrowser is used for client certificate deployments and for devices with Android OS below 5.0.

Create the configuration URL in the following format:

```
ciscojabber://provision?ServicesDomain=<domain_for_service_discover>
&VoiceServicesDomain=<domain_for_voice_services>
&ServiceDiscoveryExcludedServices=<services_to_exclude_from_service_discover>
&ServicesDomainSsoEmailPrompt=<ON/OFF>
```

Note The parameters are case sensitive. When you create the configuration URL, you must use the following capitalization:

- `ServicesDomain`
- `VoiceServicesDomain`
- `ServiceDiscoveryExcludedServices`
- `ServicesDomainSsoEmailPrompt`
- `Telephony_Enabled`
- `ForceLaunchBrowser`

Examples

- `ciscojabber://provision?ServicesDomain=cisco.com`

-
  ```
  ciscojabber://provision?ServicesDomain=cisco.com
  &VoiceServicesDomain=alphauk.cisco.com
  ```

-
  ```
  ciscojabber://provision?ServicesDomain=service_domain
  &VoiceServicesDomain=voiceservice_domain&ServiceDiscoveryExcludedServices=WEBEX
  ```

-
  ```
  ciscojabber://provision?ServicesDomain=cisco.com
  &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP
  ```

-
  ```
  ciscojabber://provision?ServicesDomain=cisco.com
  &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP
  &ServicesDomainSsoEmailPrompt=OFF
  ```

Provide Users with Configuration URL from a Website

You can provide a configuration URL link to users by emailing the link to the user directly, or by posting the link to a website.

Note Due to a limitation of the Android operating system, Cisco Jabber for Android users can encounter an issue if they open the configuration URL directly from an Android application. To work around this issue, we recommend that you distribute your configuration URL link using a website.

If you want to use the website explore option for URL provisioning, we recommended you to use Mozilla Firefox.

Use the following procedure to distribute the link from a website.

Procedure

Step 1 Create an internal web page that includes the configuration URL as an HTML hyperlink.

Step 2 Email the link to the internal web page to users.

In the email message, instruct users to perform the following steps:

1. Install the client.
2. Click the link in the email message to open the internal web page.
3. Click the link on the internal web page to configure the client.

Manual Connection Settings

Manual connection settings provide a fallback mechanism when Service Discovery is not used.

When you start Cisco Jabber, you can specify the authenticator and server address in the **Advanced settings** window. The client caches the server address to the local application configuration that loads on subsequent starts.

Cisco Jabber prompts users to enter these advanced settings on the initial start as follows:

- On-Premises with Cisco Unified Communications Manager release 9.x and Later — If the client cannot get the authenticator and server addresses from the service profile.
- Cloud-Based or On-Premises with Cisco Unified Communications Manager release 8.x — If you do not set the authenticator in the bootstrap file. The client also prompts users to enter server addresses in the **Advanced settings** window if you do not set server addresses in the bootstrap file or with SRV records.

Settings that you enter in the **Advanced settings** window take priority over any other sources including SRV records and bootstrap settings.

If you select either **Cisco IM & Presence** or **Cisco Communications Manager 8.x**options, the client retrieves UC services from Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service. The client does not use service profiles or SSO discovery.

Note For Cisco Jabber for Windows, service discovery stops after 20 seconds regardless of the number of servers the SRV record resolves to. During service discovery, once Cisco Jabber finds `_cisco-uds`, it attempts to connect to the first 2 servers within 20 seconds. Cisco Jabber doesn't attempt to connect to any servers after it's attempted service discovery for the highest 2 priority servers.

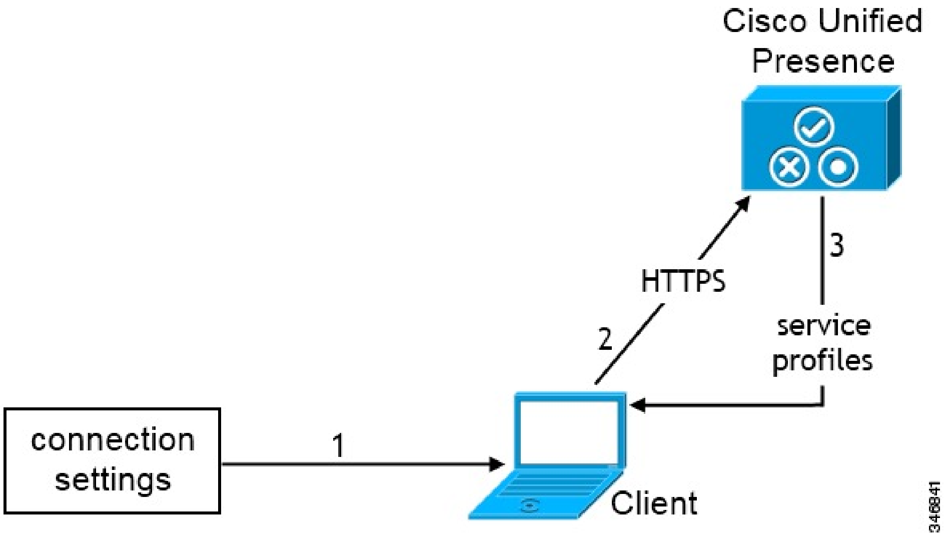
Users can manually point to the working server or re-order SRV priorities to at least one of the top two priority servers available for service discovery.

Manual Connection Settings for On-Premises Deployments

Users can set Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service as the authenticator and specify the server address in the **Advanced settings** window.

Remember You can automatically set the default server address with the `_cuplogin` SRV record.

The following diagram illustrates how the client uses manual connection settings in on-premises deployments:



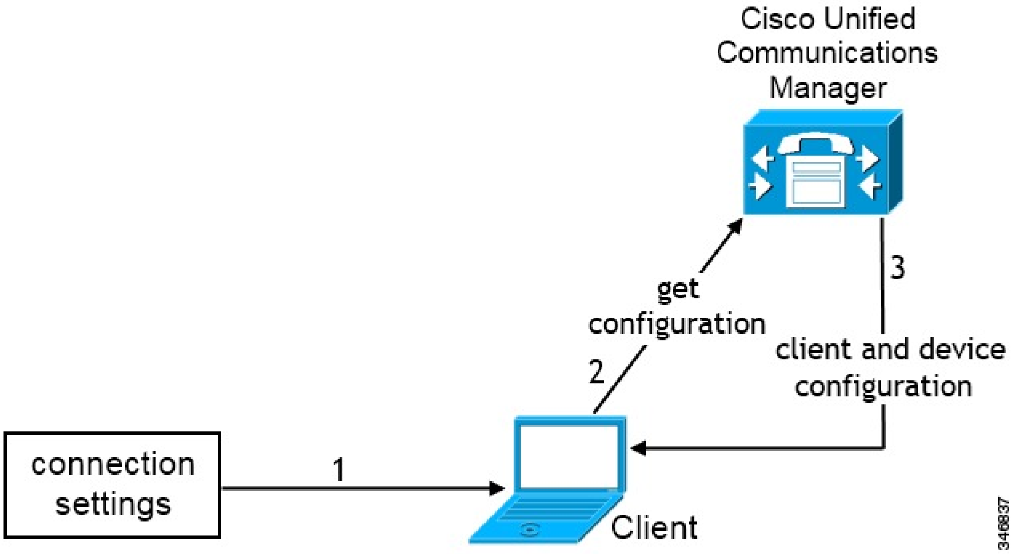
1. Users manually enter connection settings in the **Advanced settings** window.
2. The client authenticates to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.
3. The client retrieves service profiles from the presence server.

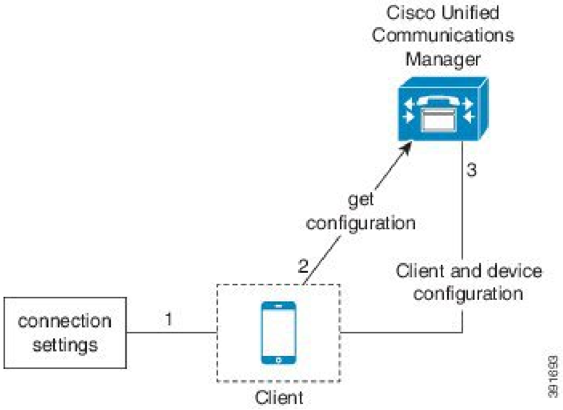
Manual Connection Settings for On-Premises Deployments in Phone Mode

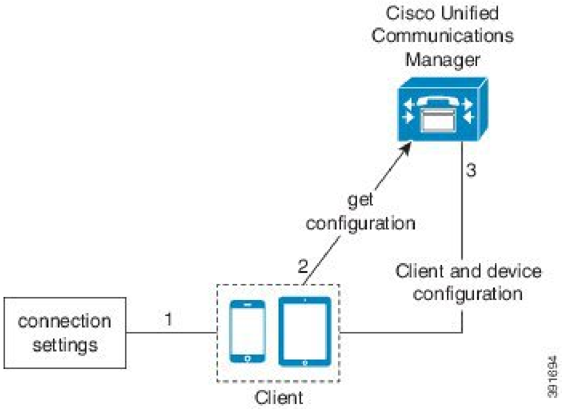
Users can set Cisco Unified Communications Manager as the authenticator and specify the following server addresses in the **Advanced settings** window:

- TFTP server
- CCMCIP server

The following diagram illustrates how the client uses manual connection settings in phone mode deployments:


Cisco Unified Communications Manager
get configuration
2
3
client and device configuration
connection settings
1
Client
346837


Cisco Unified Communications Manager
get configuration
2
3
Client and device configuration
connection settings
1
Client
391693

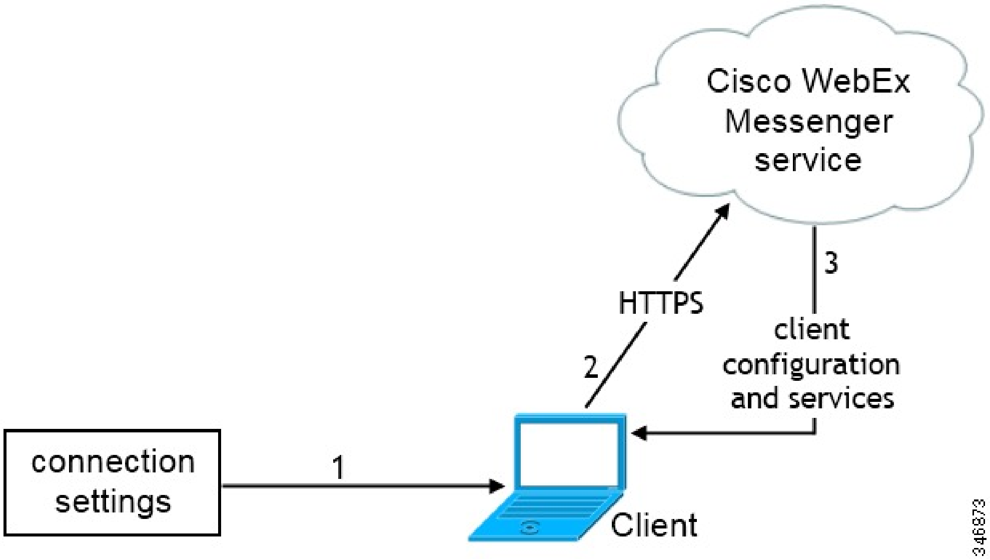

Cisco Unified Communications Manager
get configuration
2
3
Client and device configuration
connection settings
1
Client
391694

1. Users manually enter connection settings in the **Advanced settings** window.
2. The client authenticates to Cisco Unified Communications Manager and gets configuration.
3. The client retrieves device and client configuration.

Manual Connection Settings for Cloud-Based Deployments

Users can set the Cisco WebEx Messenger service as the authenticator and specify the CAS URL for login in the Advanced settings window.

The following diagram illustrates how the client uses manual connection settings in cloud-based deployments:


Cisco WebEx Messenger service
HTTPS
2
3
client configuration and services
connection settings
1
Client
346873

1. Users manually enter connection settings in the Advanced settings window.
2. The client authenticates to the Cisco WebEx Messenger service.
3. The client retrieves configuration and services.

Automatic Connection Setting for Service Discovery

Users can select the **Automatic** option in the **Advanced settings** window to discover servers automatically.

The Automatic option allows users change from manually setting the service connection details to using service discovery. For example, on the initial launch, you manually set the authenticator and specify a server address in the **Advanced settings** window.

The client always checks the cache for manual settings. The manual settings take higher priority over SRV records, and for Cisco Jabber for Windows, the bootstrap file. For this reason, if you decide to deploy SRV records and use service discovery, you override the manual settings from the initial launch.

Installer Switches: Cisco Jabber for Windows

When you install Cisco Jabber, you can specify the authenticator and server addresses. The installer saves these details to a bootstrap file. When users launch the client for the first time, it reads the bootstrap file. The bootstrap file takes priority if service discovery is deployed.

Bootstrap files provide a fallback mechanism for service discovery in situations where service discovery has not been deployed and where you do not want users to manually specify their connection settings.

The client only reads the bootstrap file on the initial launch. After the initial launch, the client caches the server addresses and configuration, and then loads from the cache on subsequent launches.

We recommend that you do not use a bootstrap file, and instead use service discovery, in on-premises deployments with Cisco Unified Communications Manager release 9.x and later.

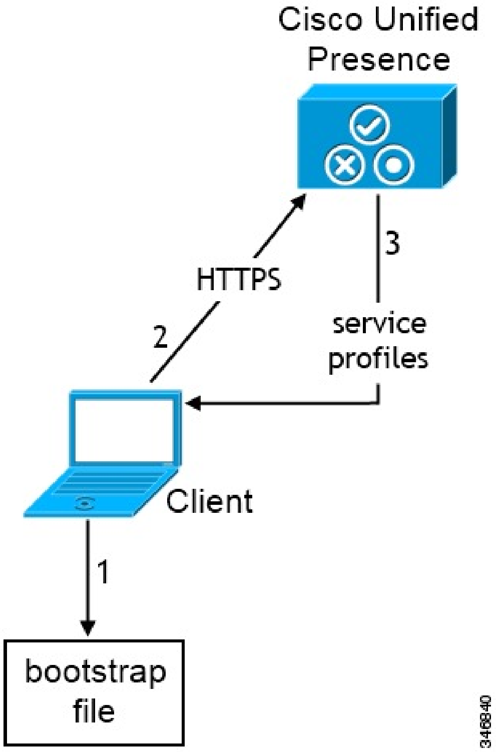
Bootstrap Settings for On-Premises Deployments

The following table lists the argument values for various deployment types.

Product Mode	Server Releases	Argument Values
Full UC (Default Mode)	Release 9 and later: • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	Use the following installer switches and values: • `AUTHENTICATOR=CUP` • `CUP_ADDRESS=` `<presence_server_address>`
Full UC (Default Mode)	Release 8.x: • Cisco Unified Communications Manager • Cisco Unified Presence	Use the following installer switches and values: • `AUTHENTICATOR=CUP` • `CUP_ADDRESS=` `<presence_server_address>`
IM Only (Default Mode)	Release 9 and later: Cisco Unified Communications Manager IM and Presence Service	Use the following installer switches and values: • `AUTHENTICATOR=CUP` • `CUP_ADDRESS=` `<presence_server_address>`

Product Mode	Server Releases	Argument Values
IM Only (Default Mode)	Release 8.x: Cisco Unified Presence	Use the following installer switches and values: • `AUTHENTICATOR=CUP` • `CUP_ADDRESS=` `<presence_server_address>`

The following diagram illustrates how the client uses bootstrap settings in on-premises deployments:



When users start the client for the first time, the following occurs:

1. The client retrieves settings from the bootstrap file.

   The client starts in default mode and determines that Cisco Unified Communications Manager IM and Presence Service is the authenticator. The client also gets the address of the presence server, unless Service Discovery results dictate otherwise.

2. The client authenticates to Cisco Unified Communications Manager IM and Presence Service .

3. The client retrieves service profiles from the presence server.

Bootstrap Settings for On-Premises Deployments in Phone Mode

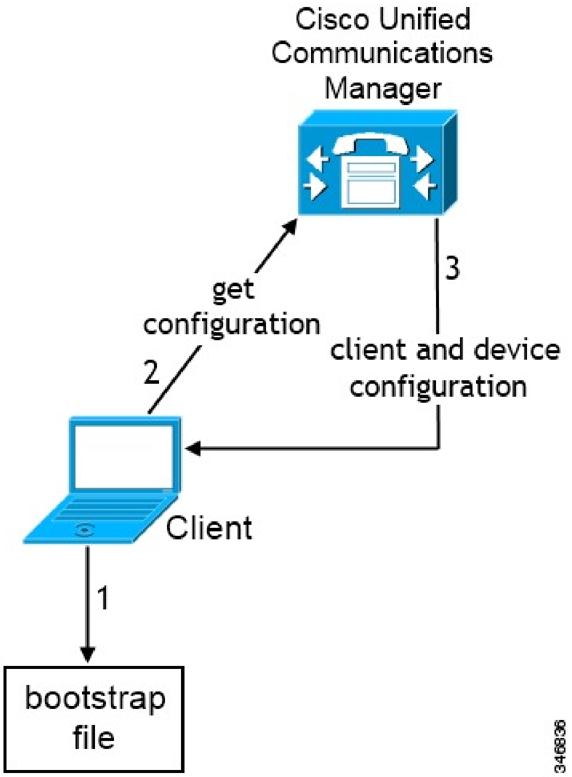
During installation, you set values for arguments as follows:

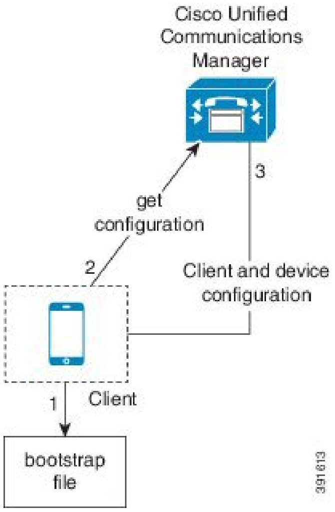
- Set `CUCM` as the value for AUTHENTICATOR.

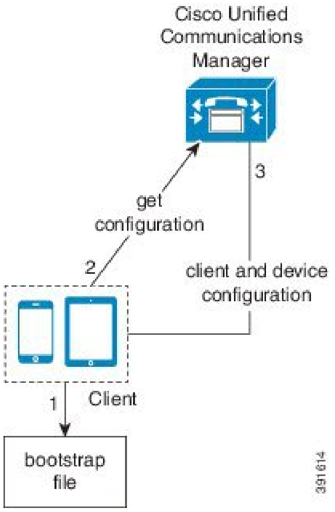
- Set `phone_mode` as the value for PRODUCT_MODE.
- Set the TFTP server address as the value for TFTP.
- Set the CTI server address as the value for CTI.
- Set the CCMCIP server address as the value for CCMCIP.

  Cisco Unified Communications Manager release 9.x and earlier—If you enable Cisco Extension Mobility, the `Cisco Extension Mobility` service must be activated on the Cisco Unified Communications Manager nodes that are used for CCMCIP. For information about Cisco Extension Mobility, see the *Feature and Services* guide for your Cisco Unified Communications Manager release.

The following diagram illustrates how the client uses bootstrap settings in phone mode deployments:


Cisco Unified Communications Manager
get configuration
2
3
client and device configuration
Client
1
bootstrap file
346836


Cisco Unified Communications Manager
3
get configuration
2
Client and device configuration
Client
1
bootstrap file
391613


Cisco Unified Communications Manager
3
get configuration
2
client and device configuration
Client
1
bootstrap file
391614

When users start the client for the first time, the following occurs:

1. The client retrieves settings from the bootstrap file.

   The client starts in phone mode and determines that Cisco Unified Communications Manager is the authenticator. The client also gets the addresses for the TFTP and CTI servers, unless Service Discovery results dictate otherwise.

   The client starts in phone mode and determines that Cisco Unified Communications Manager is the authenticator. The client also gets the addresses for the TFTP server, unless Service Discovery results dictate otherwise.

2. The client authenticates to Cisco Unified Communications Manager and gets configuration.

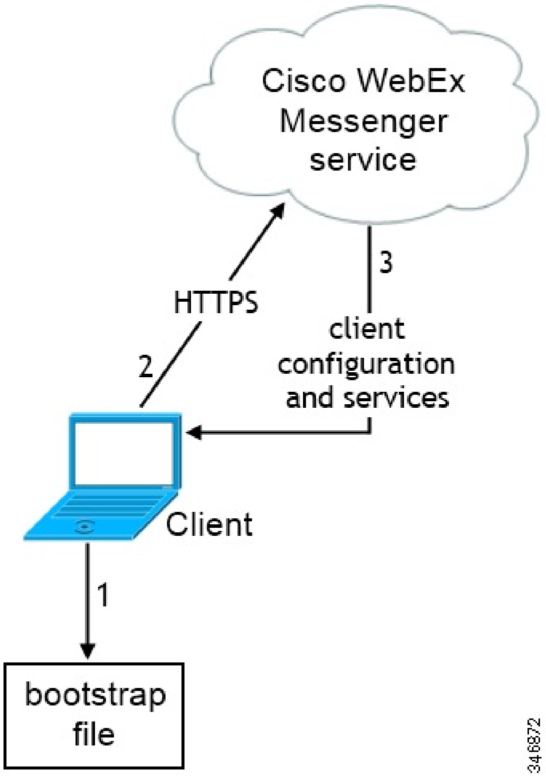
3. The client retrieves device and client configuration.

Bootstrap Settings for Cloud-Based Deployments

During installation, you set values for arguments as follows:

- Set WEBEX as the value for AUTHENTICATOR.

The following diagram illustrates how the client uses bootstrap settings in cloud-based deployments:


Cisco WebEx Messenger service
HTTPS
2
3
client configuration and services
Client
1
bootstrap file
346872

When users start the client for the first time, the following occurs:

1. The client retrieves settings from the bootstrap file.

   The client starts in default mode and determines that the Cisco WebEx Messenger service is the authenticator, unless Service Discovery results dictate otherwise.

2. The client authenticates to the Cisco WebEx Messenger service.

3. The client retrieves configuration and services.

Hardware Requirements

Hardware Requirements for Cisco Jabber for Windows

Installed RAM

2 GB RAM on Microsoft Windows 7 and 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

DirectX11 on Microsoft Windows 7

I/O Ports

USB 2.0 for USB camera and audio devices.

Hardware Requirements for Cisco Jabber for Mac

Installed RAM

2 GB RAM

Free Physical Memory

1 GB

Free Disk Space

300 MB

CPU Speed and Type

Intel Core 2 Duo or later processors in any of the following Apple hardware:

- Mac Pro
- MacBook Pro (including Retina Display model)
- MacBook
- MacBook Air
- iMac
- Mac Mini

I/O Ports

USB 2.0 for USB camera and audio devices.

Device Requirements for Cisco Jabber for Android

Device Support

Cisco Jabber for Android is available from the Google Play Store.

Cisco specifically supports Cisco Jabber for Android on audio and video for the following Android device and operating system combinations:

- Samsung Galaxy SII (Android OS 4.1.2 to Android OS 4.4 latest)
- Samsung Galaxy SIII (Android OS 4.1.2 to Android OS 4.4 latest)
- Samsung Galaxy S4 (Android OS 4.2.2 to Android OS 4.4 latest)
- Samsung Galaxy S4 mini (Android OS 4.2.2 to Android OS 4.4 latest)
- Samsung Galaxy S5 (Android OS 4.4.x)
- Samsung Galaxy Note II (Android OS 4.2 to Android OS 4.4 latest)
- Samsung Galaxy Note III (Android OS 4.3 to Android OS 4.4 latest)
- Samsung Galaxy Rugby Pro (Android OS 4.2.2 to Android OS 4.4 latest)
- Samsung Galaxy Note Pro 12.2 (Android OS 4.4.x)
- Google Nexus 5 (Android OS 4.4.x and Android OS 5.0)
- Google Nexus 10 (Android OS 4.4.x and Android OS 5.0)
- Sony Xperia Z1 (Android OS 4.2 to Android OS 4.4 latest)
- Sony Xperia ZR/A (Android OS 4.1.2 to Android OS 4.4 latest)
- Sony Xperia Z2 (Android OS 4.4.x)
- Sony Xperia M2 (Android OS 4.3)
- LG G2 (Android OS 4.2.2 to Android OS 4.4 latest)
- Motorola Moto G (Android OS 4.4.x)

Note Cisco supports Cisco Jabber for Android using IM only mode on all Android devices which meet the following minimum specifications:

- Android OS 4.1.2 or higher to Android OS 4.4.x
- 1.5 GHz dual-core or higher (quad-core recommended)
- Display 320 x 480 or higher
- Cisco Jabber for Android does not support the Tegra 2 chipset

Note

Cisco supports Cisco Jabber for Android with tested Android devices. Although other devices are not officially supported, you may be able to use Cisco Jabber for Android with other devices.

In general, you should be able to run Cisco Jabber for Android on any Android device that meets the following minimum specifications.

- **Minimum requirements for IM and Presence**
    - Android OS 4.1.2 or higher to Android OS 4.4.x
    - 1.5 GHz dual-core or higher (quad-core recommended)
    - Display 320 x 480 or higher
    - Cisco Jabber for Android does not support the Tegra 2 chipset
- **Minimum requirements for two-way video**
    - Android OS 4.1.2 or higher to Android OS 4.4.x
    - 1.5 GHz dual-core or higher (quad-core recommended)
    - Display 480 x 800 or higher
    - Cisco Jabber for Android does not support the Tegra 2 chipset

Note Due to an Android kernel issue, Cisco Jabber cannot register to the Cisco Unified Communications Manager on some Android devices. To resolve this problem, try the following:

- Upgrade the Android kernel to the latest version. This solution applies to the following supported devices:
  - Samsung Galaxy SII (Android OS 4.1.2 to Android OS 4.4 latest)
  - Samsung Galaxy SIII (Android OS 4.1.2 to Android OS 4.4 latest)
  - Samsung Galaxy S4 (Android OS 4.2.2 to Android OS 4.4 latest)
  - Samsung Galaxy S4 mini (Android OS 4.2.2 to Android OS 4.4 latest)
  - Samsung Galaxy S5 (Android OS 4.4.x)
  - Samsung Galaxy Note II (Android OS 4.2 to Android OS 4.4 latest)
  - Samsung Galaxy Note III (Android OS 4.3 to Android OS 4.4 latest)
  - Samsung Galaxy Rugby Pro (Android OS 4.2.2 to Android OS 4.4 latest)
  - Samsung Galaxy Note Pro 12.2 (Android OS 4.4.x)
  - Google Nexus 5 (Android OS 4.4.x and Android OS 5.0)
  - Google Nexus 10 (Android OS 4.4.x and Android OS 5.0)
  - LG G2 (Android OS 4.2.2 to Android OS 4.4 latest)
  - Motorola Moto G (Android OS 4.4.x)
- Set the Cisco Unified Communications Manager to use mixed mode security, enable secure SIP call signaling, and use port 5061. See the *Cisco Unified Communications Manager Security Guide* for your release for instructions on configuring mixed mode with the Cisco CTL Client. You can locate the security guides in the Cisco Unified Communications Manager Maintain and Operate Guides. This solution applies to the following supported devices:
  - Sony Xperia Z1 (Android OS 4.2 to Android OS 4.4 latest)
  - Sony Xperia ZR/A (Android OS 4.1.2 to Android OS 4.4 latest)
  - Sony Xperia Z2 (Android OS 4.4.x)
  - Sony Xperia M2 (Android OS 4.3)

Bluetooth Device Support

Cisco specifically tested and supports the following Bluetooth devices with Cisco Jabber for Android:

- Jabra Motion
- Jawbone ICON for Cisco Bluetooth Headset
- Plantronics BackBeat 903+
- Jabra Wave+

- Jabber Easygo

Note Cisco supports Cisco Jabber for Android with tested Bluetooth devices. Although other Bluetooth devices are not officially supported, you may be able to use Cisco Jabber for Android with other devices.

Important Using a Bluetooth device on a Samsung Galaxy SIII may cause distorted ringtone and distorted call audio.

If you use a Samsung Galaxy S4 with either Jawbone ICON for Cisco Bluetooth Headset or Plantronics BackBeat 903+, you may experience problems due to compatibility issues between these devices.

Remote Access

Note Administrators can configure remote access using either a VPN or Expressway for Mobile and Remote Access. If administrators configure Expressway for Mobile and Remote Access, there is no need to configure VPN access.

Cisco AnyConnect Secure Mobility Client

To connect with VPN, users can use the latest version of Cisco AnyConnect Secure Mobility Client, which is available from the Google Play Store.

Device Requirements for Cisco Jabber for iPhone and iPad

Device Support

Cisco Jabber for iPhone and iPad is available from the Apple App Store.

Cisco supports Cisco Jabber for iPhone and iPad on the following iOS devices:

- iTouch 5
- iPhone model 4, 4S, 5, 5C, and 5S

  Note Video call is not supported for iPhone model 4

- iPad second, third, fourth generation, iPad mini with Retina display, and iPad Air

The device must be able to access the corporate network using Wi-Fi or VPN.

Device Operating System Support

iOS support: iOS 7

Bluetooth Headset Support

iTouch: supported (optional)

iPhone: supported (optional)

iPad: Supported (optional)

Software Requirements

For successful deployment, ensure that client workstations meet the software requirements.

Operating System Requirements

Operating Systems for Cisco Jabber for Windows

You can install Cisco Jabber for Windows on the following operating systems:

- Microsoft Windows 8.1 32 bit
- Microsoft Windows 8.1 64 bit
- Microsoft Windows 8 32 bit
- Microsoft Windows 8 64 bit
- Microsoft Windows 7 32 bit
- Microsoft Windows 7 64 bit

Note Cisco Jabber for Windows does not require the Microsoft .NET Framework or any Java modules.

Note For Microsoft Windows 7 or 8.x, you can download Cisco Media Services Interface (MSI) 4.1.2 for use with deskphone video.

Important Cisco Jabber for Windows supports Microsoft Windows 8 in desktop mode only.

Operating Systems for Cisco Jabber for Mac

You can install Cisco Jabber for Mac on the following operating systems:

- Apple OS X Yosemite 10.10 (or later)
- Apple OS X Mavericks 10.9 (or later)
- Apple OS X Mountain Lion 10.8.1 (or later)

Software Requirements for On-Premise Servers

On-Premises Servers for Cisco Jabber for Windows and Cisco Jabber for Mac

Cisco Jabber uses domain name system (DNS) servers during startup. DNS servers are mandatory for Cisco Jabber.

Cisco Jabber supports the following on-premises servers:

- Cisco Unified Communications Manager, release 8.6(2) or later
- Cisco Unified Presence, release 8.6(2) or later
- Cisco Unity Connection, release 8.6(2) or later
- Cisco WebEx Meetings Server, version 1.5 or later (Windows only)
- Cisco WebEx Meetings Server, version 2.0 or later (Mac only)
- Cisco Expressway Series for Cisco Unified Communications Manager
    - Cisco Expressway-E, version 8.1.1 or later
    - Cisco Expressway-C, version 8.1.1 or later
- Cisco TelePresence Video Communications Server
    - Cisco VCS Expressway, version 8.1.1 or later
    - Cisco VCS Control, version 8.1.1 or later

Cisco Jabber supports the following features with Cisco Unified Survivable Remote Site Telephony, Version 8.5:

- Basic call functionality
- Ability to hold and resume calls

Refer to the *Cisco Unified SCCP and SIP SRST System Administrator Guide* for information about configuring Cisco Unified Survivable Remote Site Telephony at: http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/admin/sccp_sip_srst/configuration/guide/SCCP_and_SIP_SRST_Admin_Guide.html.

For Cisco Unified Communications Manager Express support details, refer to the Cisco Unified CME documentation: http://www.cisco.com/en/us/products/sw/voicesw/ps4625/products_device_support_tables_list.html

On-Premises and Cloud Servers for Cisco Jabber for Android and iOS

Cisco Jabber uses domain name system (DNS) servers during startup. DNS servers are mandatory for Cisco Jabber.

Cisco Jabber for mobile clients supports the following cloud servers:

WebEx Meeting Center

WebEx Meeting Center WBS28+

Cisco Jabber for mobile clients supports the following on-premises nodes and servers:

Cisco Unified Communications Manager

- Cisco Unified Communications Manager, Release 8.6(2) or later

Cisco Unified Presence

- Cisco Unified Presence, Release 8.6(2)

Cisco Unified Communications Manager IM and Presence Service

Note Cisco Unified Communications Manager IM and Presence Service is formerly known as Cisco Unified Presence.

- Cisco Unified Communications Manager IM and Presence Service, Release 9.1(1)
- Cisco Unified Communications Manager IM and Presence Service, Release 9.1(2)
- Cisco Unified Communications Manager IM and Presence Service, Release 10.0(1)
- Cisco Unified Communications Manager IM and Presence Service, Release 10.5(1)
- Cisco Unified Communications Manager IM and Presence Service, Release 10.5(2)
- Cisco Unified Communications Manager IM and Presence Service, Release 11.0

Video Conferencing Bridge

- Cisco TelePresence MCU 5310
- Cisco TelePresence Server 7010
- Cisco TelePresence Server MSE 8710
- Cisco Integrated Services Router (with Packet Voice/Data Module [PVDM3])

  Note Expressway for Mobile and Remote Access is not supported with Cisco Integrated Services Router (with PVDM3).

Cisco Unity Connection

- Cisco Unity Connection, Release 8.6(2) or later

Cisco WebEx Meetings Server

- Cisco WebEx Meetings Server, version 2.0 or later

Cisco WebEx Meetings Client

Cisco WebEx Meetings client, later than version 4.5

Note This Cisco WebEx Meetings Server client, version 8.0 supports Collaboration Meeting Room and Personal Meeting Room.

Cisco Unified Survivable Remote Site Telephony

Cisco Jabber for mobile clients support the following features with Cisco Unified Survivable Remote Site Telephony, version 8.5.

Cisco Expressway Series for Cisco Unified Communications Manager (Optional)

Use the following servers to set up mobile and remote access for the client. The Expressway servers do not provide call control for Cisco Jabber. The client uses Cisco Unified Communications Manager for call control.

- Cisco Expressway-E, version 8.5
- Cisco Expressway-C, version 8.5
- Cisco Expressway, version 8.2
- Cisco Expressway, version 8.2.1

If you currently deploy a Cisco TelePresence Video Communications Server (VCS) environment, you can set up Cisco Expressway for Mobile and Remote Access. A VCS environment requires Cisco VCS Expressway, version 8.1.1 and Cisco VCS Control, version 8.1.1.

Cisco Adaptive Security Appliance (Optional)

- Cisco Adaptive Security Appliance (ASA) 5500 Series, version 8.4(1) or later.
- Cisco Adaptive Security Device Manager (ASDM), version 6.4 or later.
- Cisco AnyConnect Secure Mobility Client Integration (Optional)—Android devices must run the latest version of Cisco AnyConnect Secure Mobility Client, which is available from the Google Play Store.

  Note When you are using AnyConnect with Samsung, the supported version is 4.0.01128.

- ASA license requirements—Use one of the following combinations:
  - AnyConnect Essentials and AnyConnect Mobile licenses
  - AnyConnect Premium and AnyConnect Mobile licenses
- Certificate authority (CA) if using certificate-based authentication—Cisco IOS Certificate Server, Microsoft Windows Server 2008 R2 Enterprise Certificate Authority, or Microsoft Windows Server 2003 Enterprise Certificate Authority.

On-Premises Servers for Cisco Jabber for iPhone and iPad

Cisco Jabber for iPhone and iPad supports the following on-premises servers:

Cisco Jabber uses domain name system (DNS) servers during startup. DNS servers are mandatory for Cisco Jabber.

Cisco Unified Communications Manager

- Cisco Unified Communications Manager, Release 8.6(2)
- Cisco Unified Communications Manager, Release 9.1(2)
- Cisco Unified Communications Manager, Release 10.0(1)
- Cisco Unified Communications Manager, Release 10.5(1)
- Cisco Unified Communications Manager, Release 10.5(2)

Cisco Unified Presence

- Cisco Unified Presence, Release 8.6(1)
- Cisco Unified Presence, Release 8.6(2)

Cisco Unified Communications Manager Release IM and Presence Service

Note Cisco Unified Communications Manager IM and Presence Service is formerly known as Cisco Unified Presence.

- Cisco Unified Communications Manager IM and Presence Service, Release 9.1(1)
- Cisco Unified Communications Manager IM and Presence Service, Release 9.1(2)
- Cisco Unified Communications Manager IM and Presence Service, Release 10.0(1)
- Cisco Unified Communications Manager IM and Presence Service, Release 10.5(1)
- Cisco Unified Communications Manager IM and Presence Service, Release 10.5(2)

Cisco Unity Connection

- Cisco Unity Connection, Release 8.5
- Cisco Unity Connection, Release 8.6(1)
- Cisco Unity Connection, Release 8.6(2)
- Cisco Unity Connection, Release 9.1(1)
- Cisco Unity Connection, Release 9.1(2)
- Cisco Unity Connection, Release 10.0(1)
- Cisco Unity Connection, Release 10.5(1)
- Cisco Unity Connection, Release 10.5(2)

Cisco WebEx Meetings Server

- Cisco WebEx Meetings Server, version 1.5
- Cisco WebEx Meetings Server, version 2.0
- Cisco WebEx Meetings Server, version 2.5
- Cisco WebEx Meetings Client, version 4.5 to 6.5

Cisco Adaptive Security Appliance (Optional)

- VPN On Demand (Optional)—The Apple iOS On-Demand VPN feature requires certificate-only authentication. If you set up an ASA without certificate-only authentication, the user must manually initiate the AnyConnect VPN connection as needed.

  The iOS device must be able to access the corporate network, servers, and telephony endpoints using a VPN client, such as Cisco AnyConnect Secure Mobility Client.

- Cisco AnyConnect Secure Mobility Client Integration (Optional)
  - iOS devices must run Cisco AnyConnect Secure Mobility Client version 3.0.09115, which is available from the Apple App Store
  - Cisco ASA 5500 Series Adaptive Security Appliance (ASA), version 8.4(1) or later
  - Cisco Adaptive Security Device Manager (ASDM), version 6.4 or later
  - ASA license requirements—Use one of the following combinations:
    - AnyConnect Essentials and AnyConnect Mobile licenses
    - AnyConnect Premium and AnyConnect Mobile licenses

    Note For more information about Cisco AnyConnect license requirements, see *VPN License and Feature Compatibility*.

  - Certificate authority (CA) if using certificate-based authentication: Cisco IOS Certificate Server, Cisco IOS Certificate Server or Microsoft Windows Server 2003 Enterprise Certificate Authority

Cisco Jabber supports the following features with Cisco Unified Survivable Remote Site Telephony, version 8.6:

- Basic call functionality
- Ability to hold and resume calls on different clients with the shared line.

High Availability for Instant Messaging and Presence

High availability refers to an environment in which multiple nodes exist in a subcluster to provide failover capabilities for instant messaging and presence services. If one node in a subcluster becomes unavailable, the instant messaging and presence services from that node failover to another node in the subcluster. In this way, high availability ensures reliable continuity of instant messaging and presence services for Cisco Jabber.

When using an LDAP or UDS contact source on Cisco Jabber for Mac and Cisco Jabber for mobile clients, high availability is not supported. High availability is only supported for LDAP (EDI) on Cisco Jabber for Windows.

Cisco Jabber supports high availability with the following servers:

Cisco Unified Presence releases 8.5 and 8.6

Use the following Cisco Unified Presence documentation for more information about high availability.

Configuration and Administration of Cisco Unified Presence Release 8.6

`Multi-node Deployment Administration`

`Troubleshooting High Availability`

Deployment Guide for Cisco Unified Presence Release 8.0 and 8.5

`Planning a Cisco Unified Presence Multi-Node Deployment`

Cisco Unified Communications Manager IM and Presence Service release 9.0 and higher

Use the following Cisco Unified Communications Manager IM and Presence Service documentation for more information about high availability.

Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager

`High Availability Client Login Profiles`

`Troubleshooting High Availability`

Active Calls on Hold During Failover

You cannot place an active call on hold if failover occurs from the primary instance of Cisco Unified Communications Manager to the secondary instance.

High Availability in the Client

Client Behavior During Failover

If high availability is configured on the server, then after the primary server fails over to the secondary server, the client temporarily loses presence states for up to one minute. Configure the re-login parameters to define how long the client waits before attempting to re-login to the server.

Configure Login Parameters

In Cisco Unified Communications Manager IM and Presence Service, you can configure the maximum and minimum number of seconds that Cisco Jabber waits before attempting to re-login to the server. On the server, you specify the re-login parameters in the following fields:

- **Client Re-Login Lower Limit**
- **Client Re-Login Upper Limit**

Related Topics

Cisco Unified Communications Manager Configuration Guides

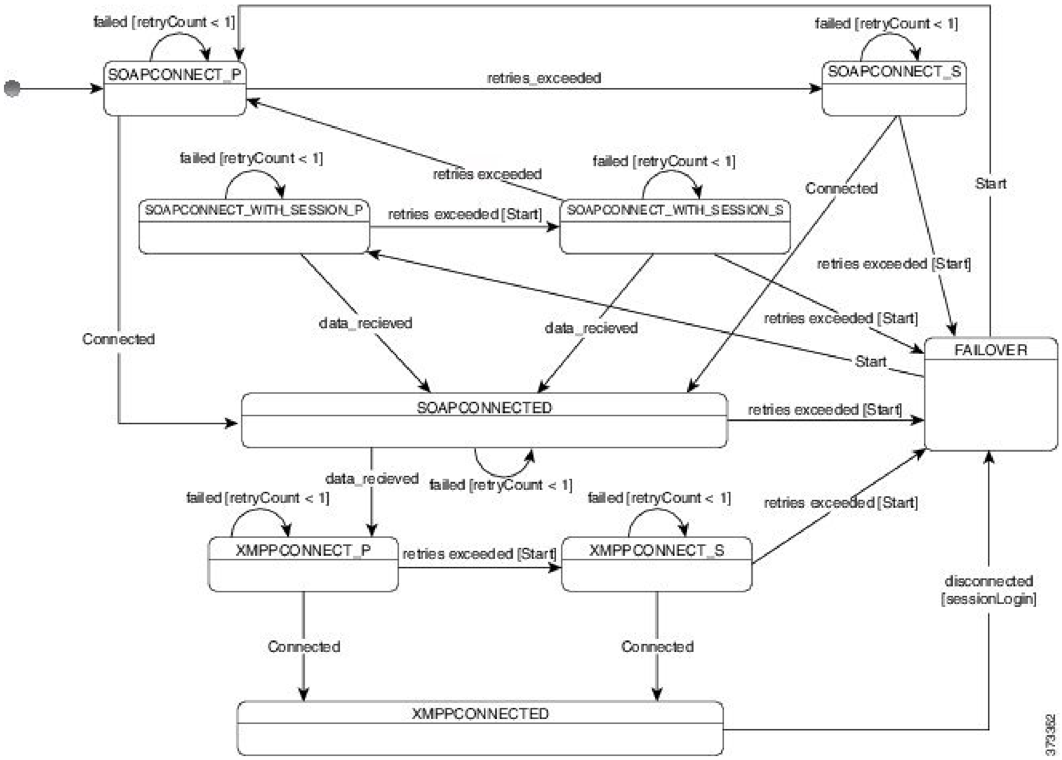
Cisco Unified Presence Configuration Guides

Supported Services, on page 7

Client Behavior During a Failover

The following figure shows the client's behavior when the Cisco Unified Communications Manager IM and Presence service during a failover.

Figure 5: Client Behavior During a Failover



1. When the client is disconnected from its active server, the client goes from XMPPCONNECTED state to a FAILOVER state.
2. From a FAILOVER state, the client tries to attain a SOAPCONNECTED state by attempting SOAPCONNECT_SESSION_P (as the primary server), and if that fails, attempts SOAPCONNECT_SESSION_S (as the secondary server).
   - If it is unable to attain SOAPCONNECT_SESSION_P or SOAPCONNECT_SESSION_S, the client re-enters into the FAILOVER state.
   - From a FAILOVER state, the clients attempts to attain a SOAPCONNECT_P state, and if that fails, attempts to reach a SOAPCONNECT_S state.
   - If the client cannot reach the SOAPCONNECT_P or SOAPCONNECT_S state, then the client does not attempt any more automatic connections to the IM&P server until a user initiates a login attempt.
3. From a SOAPCONNECT_SESSION_P, SOAPCONNECT_SESSION_S, SOAPCONNECT_P, or SOAPCONNECT_S state, the client retrieves its current primary secondary XMPP server address. This address changes during a failover.
4. From a SOAPCONNECTED state, the client tries to attain an XMPPCONNECTED state by attempting to connect to the XMPPCONNECT_P state, and if that fails, attempts XMPPCONNECT_S state.

- If client cannot reach XMPPCONNECT_P or XMPPCONNECT_S state, then the client does not attempt any more automatic connections to the IM&P server until a user initiates a login attempt.

5. After the client is in an XMPPCONNECTED state, then the client has IM&P capability.

Cloud-Based Servers

Cisco Jabber supports integration with the following hosted servers:

- Cisco WebEx Messenger service
- Cisco WebEx Meeting Center, minimum supported versions WBS27 or later

Directory Servers

You can use the following directory servers with Cisco Jabber:

Note Cisco Jabber for Windows, Cisco Jabber for Mac, Cisco Jabber for iPhone and iPad, and Cisco Jabber for Android support the LDAPv3 standard for directory integration. Any directory server that supports this standard should be compatible with these clients.

- Active Directory Domain Services for Windows Server 2012 R2
- Active Directory Domain Services for Windows Server 2008 R2
- Cisco Unified Communications Manager User Data Server (UDS)

  Cisco Jabber supports UDS using the following Cisco Unified Communications Manager versions:

  Cisco Unified Communications Manager, version 9.1(2), with the following Cisco Options Package (COP) file: `cmterm-cucm-uds-912-5.cop.sgn`.
  Cisco Unified Communications Manager, version 10.0(1). No COP file is required.

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

Restriction Directory integration with OpenLDAP, AD LDS, or ADAM requires that you define specific parameters in a Cisco Jabber configuration file.

Integration with Microsoft Products

Applies to: Cisco Jabber for Windows

Cisco Jabber for Windows supports a range of Microsoft products that integrate with the application. This section describes the support and integrations for these products.

Internet Explorer

Microsoft Internet Explorer 8 or later is required. Cisco Jabber for Windows uses the Internet Explorer rendering engine to display HTML content.

Cisco Jabber for Windows requires Internet Explorer active scripting to render IMs. See https://windows.microsoft.com/en-US/windows/help/genuine/ie-active-script for instructions on enabling active scripting.

Note Internet Explorer 9 users in Cloud-based deployments that use Single Sign On (SSO) get security alerts when they sign in to Cisco Jabber for Windows. Add **webexconnect.com** to the list of websites in the **Compatibility View Settings** window of Internet Explorer 9 to stop these alerts.

Office

Integration with the following versions of Office is supported:

- Microsoft Office 2013, 32 and 64 bit
- Microsoft Office 2010, 32 and 64 bit

Office 365

Microsoft Office 365 supports different configuration types based on the plan or subscription type. Cisco Jabber for Windows has been tested with small business plan P1 of Microsoft Office 365. This plan requires an on-premises Active Directory server.

Client-side integration with Microsoft Office 365 is supported with the following applications:

- Microsoft Office 2013, 32 bit and 64 bit
- Microsoft Office 2010, 32 bit and 64 bit
- Microsoft SharePoint 2010

SharePoint

Integration with the following versions of SharePoint is supported:

- Microsoft SharePoint 2013
- Microsoft SharePoint 2010

Availability status in Microsoft SharePoint sites is supported only if users access those sites with Microsoft Internet Explorer. You should add the Microsoft SharePoint site to the list of trusted sites in Microsoft Internet Explorer.

Calendar Integration

You can use the following client applications for calendar integration:

- Microsoft Outlook 2013, 32 bit and 64 bit

- Microsoft Outlook 2010, 32 bit and 64 bit
- IBM Lotus Notes 9, 32 bit
- IBM Lotus Notes 8.5.3, 32 bit
- IBM Lotus Notes 8.5.2, 32 bit
- IBM Lotus Notes 8.5.1, 32 bit
- Google Calendar

Local Contacts in Mac Address Book

Cisco Jabber allows users search for and add local contacts in the Mac Address book.

To search for local contacts in Mac Address book with the client, users must install the Address Book plug-in:

1. Select **Jabber** > **Install Mac Address Book Plug-In**.

To enable the Address Book plug-in:

1. Select **Jabber** > **Preferences** > **General** > **Enable "Mac Address Plug-in"**.
2. Restart the client for this to take effect.

To communicate with local contacts in Mac Address book using the client, local contacts must have the relevant details. To send instant messages to contacts, local contacts must have an instant message address. To call contacts in Mac Address book, local contacts must have phone numbers.

Computer Telephony Integration

Cisco Jabber for Windows and Cisco Jabber for Mac for Mac support CTI of Cisco Jabber from a third party application.

Computer Telephony Integration (CTI) enables you to use computer-processing functions while making, receiving, and managing telephone calls. A CTI application can allow you to retrieve customer information from a database on the basis of information that caller ID provides and can enable you to use information that an interactive voice response (IVR) system captures.

For more information on CTI, see the CTI sections in the appropriate release of the *Cisco Unified Communications Manager System Guide*. Or you can see the following sites on the Cisco Developer Network for information about creating applications for CTI control through Cisco Unified Communications Manager APIs:

- Cisco TAPI: https://developer.cisco.com/site/jtapi/overview/
- Cisco JTAPI: https://developer.cisco.com/site/jtapi/overview/

Accessibility

Accessibility for Cisco Jabber for Android

Screen Readers

Cisco Jabber for Android is compatible with the TalkBack screen reader. Users who require screen readers should always use the most recent version to ensure the best possible user experience.

Assistive Touch

You can navigate Cisco Jabber for Android using Explore by Touch.

Accessibility for Cisco Jabber for iPhone and iPad

Screen Readers

Cisco Jabber for iPhone and iPad is compatible with the VoiceOver screen reader. Users who require screen readers should always use the most recent version to ensure the best possible user experience.

Assistive Touch

You can navigate Cisco Jabber for iPhone and iPad using Assistive Touch.

Network Requirements

When using Cisco Jabber over your corporate Wi-Fi network, we recommend that you do the following:

- Design your Wi-Fi network to eliminate gaps in coverage as much as possible, including in areas such as elevators, stairways, and outside corridors.
- Ensure that all access points assign the same IP address to the mobile device. Calls are dropped if the IP address changes during the call.
- Ensure that all access points have the same service set identifier (SSID). Hand-off may be much slower if the SSIDs do not match.
- Ensure that all access points broadcast their SSID. If the access points do not broadcast their SSID, the mobile device may prompt the user to join another Wi-Fi network, which interrupts the call.

Conduct a thorough site survey to minimize network problems that could affect voice quality. We recommend that you do the following:

- Verify nonoverlapping channel configurations, access point coverage, and required data and traffic rates.
- Eliminate rogue access points.
- Identify and mitigate the impact of potential interference sources.

For more information, see the following documentation:

- The “VoWLAN Design Recommendations” section in the *Enterprise Mobility Design Guide*.
- The *Cisco Unified Wireless IP Phone 7925G Deployment Guide*.
- The *Capacity Coverage & Deployment Considerations for IEEE 802.11g* white paper.
- The *Solutions Reference Network Design (SRND)* for your Cisco Unified Communications Manager release.

Ports and Protocols

Ports and Protocols for Desktop Clients

The following table lists outbound ports and protocols that Cisco Jabber uses.

Port	Protocol	Description
443	TCP (Extensible Messaging and Presence Protocol [XMPP] and HTTPS)	XMPP traffic to the WebEx Messenger service. The client sends XMPP through this port in cloud-based deployments only. If port 443 is blocked, the client falls back to port 5222. **Note** Cisco Jabber can also use this port for: • HTTPS traffic to Cisco Unity Connection and Cisco WebEx Meetings Server. • Saving chats to the Microsoft Exchange server.
30000 to 39999	UDP	The client uses this port for far end camera control.
389	UDP/TCP	Lightweight Directory Access Protocol (LDAP) directory server.
636	LDAPS	LDAP directory server (secure).
2748	TCP	Computer Telephony Interface (CTI) used for desk phone control.
3268	TCP	Global Catalog server.
3269	LDAPS	Global Catalog server (secure).
5070 to 6070	UDP	Binary Floor Control Protocol (BFCP) for video desktop sharing capabilities.
5222	TCP (XMPP)	XMPP traffic to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.
8443	TCP (HTTPS)	Traffic to Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service.
7080	TCP (HTTPS)	Cisco Unity Connection for notifications of voice messages (new message, message update, and message deletion).
53	UDP/TCP	Domain Name System (DNS) traffic.

Port	Protocol	Description
80	HTTP	Saving chats to Microsoft Exchange server. Depending on your server configuration on Microsoft Exchange, use either port 80 or 443, but not both.
37200	SOCKS5 Bytestreams	Peer-to-peer file transfers. In on-premises deployments, the client also uses this port to send screen captures.
5060	UDP/TCP	Session Initiation Protocol (SIP) call signaling.
5061	TCP	Secure SIP call signaling.
49152 to 65535	TCP	IM-only screen share. The client randomly selects a port from the range. The actual range may vary. To find the real range, enter the **netsh interface ipv4 show dynamicportrange tcp** command. You can use the SharePortRangeStart and SharePortRangeSize parameters to narrow the range used for IM screen share. For more information on these parameters, see the section on Common Policies parameters in the *Deployment and Installation Guide*.

Ports for Additional Services and Protocols

In addition to the ports listed in this section, you should review the required ports for all protocols and services in your deployment. See to the appropriate documentation for your server version. You can find the port and protocol requirements for different servers in the following documents:

- For Cisco Unified Communications Manager, Cisco Unified Communications Manager IM and Presence Service, and Cisco Unified Presence, see the *TCP and UDP Port Usage Guide*.
- For Cisco Unity Connection, see the *System Administration Guide*.
- For Cisco WebEx Meetings Server, see the *Administration Guide*.
- For Cisco WebEx services, see the *Administrator's Guide*.
- Expressway for Mobile and Remote Access, refer to *Cisco Expressway IP Port Usage for Firewall Traversal*.

Ports and Protocols for Cisco Jabber for Android, iPhone, and iPad

The client uses the ports and protocols listed in the following table. If you plan to deploy a firewall between the client and a server, you must configure the firewall to allow these ports and protocols.

Note No TCP/IP services are enabled in the client.

Port	Application Layer Protocol	Transport Layer Protocol	Description
Inbound			
16384 to 32766	RTP	UDP	Receives Real-Time Transport Protocol (RTP) media streams for audio and video. You set these ports in Cisco Unified Communications Manager.
Outbound			
7080	HTTPS	TCP	Used for Cisco Unity Connection to receive notifications of voice messages (new message, message update, and message deleted).
6970	HTTP	TCP	Connects to the TFTP server to download client configuration files.
80	HTTP	TCP	Connects to services such as Cisco WebEx Meeting Center for meetings or Cisco Unity Connection for voicemail.
389	LDAP	TCP (UDP)	Connects to an LDAP directory service.
3268	LDAP	TCP	Connects to a Global Catalog server for contact searches.
443	HTTPS	TCP	Connects to services such as such as Cisco WebEx Meeting Center for meetings or Cisco Unity Connection for voicemail.
636	LDAPS	TCP	Connects securely to an LDAP directory service.
3269	LDAPS	TCP	Connects securely to the Global Catalog server.
5060	SIP	TCP	Provides Session Initiation Protocol (SIP) call signaling.
5061	SIP over Transport Layer Security (TLS)	TCP	Provides secure SIP call signaling.
5222	XMPP	TCP	Connects to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service for instant messaging and presence.
5269	XMPP	TCP	Enables XMPP federation.
8191	SOAP	TCP	Connects to the local port to provide Simple Object Access Protocol (SOAP) web services.

Port	Application Layer Protocol	Transport Layer Protocol	Description
8443	HTTPS	TCP	Is the port for 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) for contact resolution.
16384 to 32766	RTP	UDP	Sends RTP media streams for audio and video.
53	DNS	UDP	Provides hostname resolution.
3804	CAPF	TCP	Issues Locally Significant Certificates (LSC) to IP phones. This port is the listening port for Cisco Unified Communications Manager Certificate Authority Proxy Function (CAPF) enrollment.

For information about port usage for Expressway for Mobile and Remote Access, see *Cisco Expressway IP Port Usage for Firewall Traversal*.

For information about file transfer port usage see the Managed File Transfer chapter of the *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager, Release 10.5(2)*.

Call Control with Accessories API

Cisco Jabber for Windows includes an API that exposes call control functions to third party accessories. This API lets our vendor partners create software plugins that enable their accessories to use the API call control functions in Cisco Jabber.

Compatible Third Party Accessories

You can use certain Cisco compatible accessories such as headsets, speakers, keyboards, and audio devices to perform call control actions with Cisco Jabber from the device. For example, with some headsets you can use controls to answer incoming calls, end active calls, mute audio, and place calls on hold.

For a list of devices that are compatible with Cisco Jabber, refer to the *Unified Communications Endpoint and Client Accessories* site at: http://www.cisco.com/en/US/prod/voicesw/uc_endpoints_accessories.html

Note You can use certain third party accessories that are not Cisco compatible. However, Cisco cannot guarantee an optimal user experience with such third party accessories. For the best user experience, you should use only Cisco compatible devices with Cisco Jabber.

Install Vendor Plugins

To use compatible accessories with Cisco Jabber, you must do the following:

Procedure

Step 1 Download a compatible plugin from the third party vendor site.

Step 2 Install the plugin separately to Cisco Jabber.

Plugin Versions

The following are the minimum plugin versions required for integration with Cisco Jabber:

- Jabra PC Suite Version 2.12.3655
- Logitech UC Plugin 1.1.27

CTI Supported Devices

To view the list of Computer Telephony Integration (CTI) supported devices: From Cisco Unified Reporting, select **Unified CM Phone Feature List**. From the **Feature** drop-down list, select **CTI controlled**.

Supported Codecs

Supported Codecs for Cisco Jabber for Windows and Cisco Jabber for Mac

Supported Audio Codecs

- G.722
- G.722.1—32k and 24k. G.722.1 is supported on Cisco Unified Communications Manager 8.6.1 or later.
- G.711—a-law and u-law
- G.729a

Supported Video Codec

- H.264/AVC

Supported Codecs for Cisco Jabber for Android, iPhone, and iPad

Supported Audio Codecs

Codec	Codec type	Notes
G.711	mu-law a-law	Supports normal mode.
G.722.1		Supports normal mode.
G.729a		Minimum requirement for low-bandwidth availability. Only codec that supports low bandwidth mode. Supports normal mode.
G.722		
Opus		

Users can turn low bandwidth mode on and off in the client settings if they experience voice quality issues.

Supported Video Codecs

H.264/AVC

Users can turn low bandwidth mode on to improve the video quality issue.

Supported Voicemail Codecs

- PCM linear
- G.711—mu-law (default)
- G.711—a-law
- GSM 6.10

Note Cisco Jabber for mobile does not support visual voicemail with G.729. However, you can access voice messages using G.729 and the **Call Voicemail** feature.

COP Files

COP Files for Cisco Jabber for Windows and Cisco Jabber for Mac

In certain cases, you might need to apply COP files to Cisco Unified Communications Manager.

You can download the following COP files from the Cisco Jabber administration package on Cisco.com:

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*.	8.6.1 and earlier
cmterm-cupc-dialrule-wizard-0.1.cop.sgn	Publishes application dial rules and directory lookup rules to Cisco Jabber. For more information, see *Publish Dial Rules*.	8.6.1 and earlier

Related Topics

Download software

Device COP file for Cisco Jabber for Android

You must install the device COP file on Cisco Unified Communications Manager to add the Cisco Dual Mode for Android device type for the first time, or to update your existing Cisco Dual Mode for Android devices with the configuration settings for the latest release of the client. To obtain the device COP file, do the following:

1. Go to the software downloads site.
2. In the search box, search for Cisco Jabber for Android.
3. On the Cisco Jabber for Android software downloads page, locate the device COP file for your release.
4. Download the file.

Device COP File for Cisco Jabber for iPhone and iPad

The device COP file adds the TCT/TAB device type to Cisco Unified Communications Manager . To obtain the device COP file, do the following:

1. Go to the software download site: http://www.cisco.com/go/jabber_iphone_cop..
2. Locate `cmterm-iphone-install-141105.cop.sgn` for TCT device and `cmterm-jabberipad-140904.cop.sgn` for TAB device..

3. Download the file.

Contact Sources

In on-premises deployments, the client requires a contact source to resolve directory look ups for user information. You can use the following as a contact source:

Enhanced Directory Integration

Enhanced Directory Integration (EDI) is an LDAP-based contact source.

Basic Directory Integration

Basic Directory Integration (BDI) is an LDAP-based contact source.

Cisco Unified Communications Manager User Data Service

Cisco Unified Communications Manager User Data Service (UDS) is a contact source on Cisco Unified Communications Manager.

UDS is used for contact resolution in the following cases:

- If you configure the DirectoryServerType parameter in the client configuration file to use “UDS”.

  With this configuration, the client uses UDS for contact resolution when it is inside or outside of the corporate firewall.

- If you deploy Expressway for Mobile and Remote Access.

  With this configuration, the client automatically uses UDS for contact resolution when it is outside of the corporate firewall.

Note Cisco Jabber supports UDS using the following Cisco Unified Communications Manager versions:

- Cisco Unified Communications Manager Version 9.1(2) or later with the following COP file: cmterm-cucm-uds-912-5.cop.sgn.
- Cisco Unified Communications Manager Version 10.0(1). No COP file is required.

You can deploy approximately 50 percent of the maximum number of Cisco Jabber clients that your Cisco Unified Communications Manager node supports.

For example, if a Cisco Unified Communications Manager node can support 10,000 Cisco Jabber clients using an LDAP-based contact source, that same node can support 5,000 Cisco Jabber clients using UDS as a contact source.

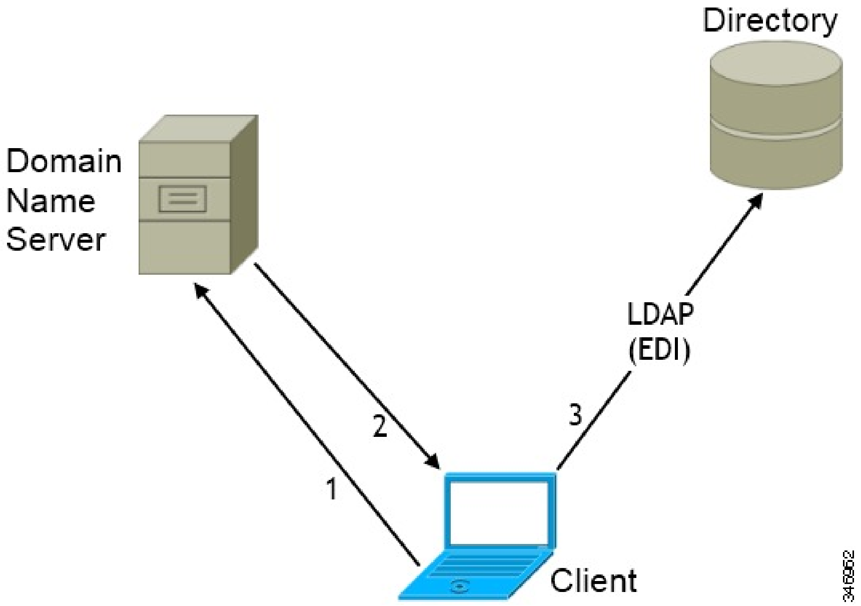
Enhanced Directory Integration

EDI uses native Microsoft Windows APIs to retrieve contact data from the directory service.

The following are the default settings for on-premises deployments with EDI:

- Cisco Jabber integrates with Active Directory as the contact source.

- Cisco Jabber automatically discovers and connects to a Global Catalog.



In the preceding diagram, the client does the following by default:

1. Gets the DNS domain from the workstation and looks up the SRV record for the Global Catalog.
2. Retrieves the address of the Global Catalog from the SRV record.
3. Connects to the Global Catalog with the logged in user's credentials.

Domain Name Retrieval

Cisco Jabber for Windows retrieves the fully qualified DNS domain from the `USERDNSDOMAIN` environment variable on the client workstation.

After the client gets the DNS domain, it can locate the Domain Name Server and retrieve SRV records.

If the USERDNSDOMAIN environment variable is not present, you can deploy the LdapUserDomain configuration parameter to specify which domain to execute the request for the LDAP service. If that parameter is not configured, then Jabber uses the domain from the email address screen.

In some instances, the value of the `USERDNSDOMAIN` environment variable does not resolve to the DNS domain that corresponds to the domain of the entire forest. For example, when an organization uses a sub-domain or resource domain. In this case, the `USERDNSDOMAIN` environment variable resolves to a child domain, not the parent domain. As a result, the client 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 options to enable Cisco Jabber for Windows to connect to a service in the parent domain:

- Ensure that the Global Catalog or LDAP directory server can access all users in the organization.
- Configure your DNS server to direct the client to a server that can access all users in the organization when Cisco Jabber for Windows requests a Global Catalog or LDAP directory server.
- Configure Cisco Jabber for Windows to use the FQDN of the domain controller.

Specify the FQDN of the domain controller as the value of the PrimaryServerName parameter in your client configuration as follows:

```
<PrimaryServerName>parent-domain-fqdn</PrimaryServerName>
```

Related Topics

Directory Connection Parameters

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

Directory Server Discovery

Cisco Jabber can automatically discover and connect to the directory server if:

- The workstation on which you install Cisco Jabber automatically detects the workstation by determining the user domain.
- The workstation retrieves the server connection address from the DNS SRV record.

Directory Server	SRV Record
Global Catalog	`_gc._msdcs._tcp.`*`domain.com`*
Domain Controller LDAP-based directory servers	`_ldap._msdcs._tcp.`*`domain.com`*

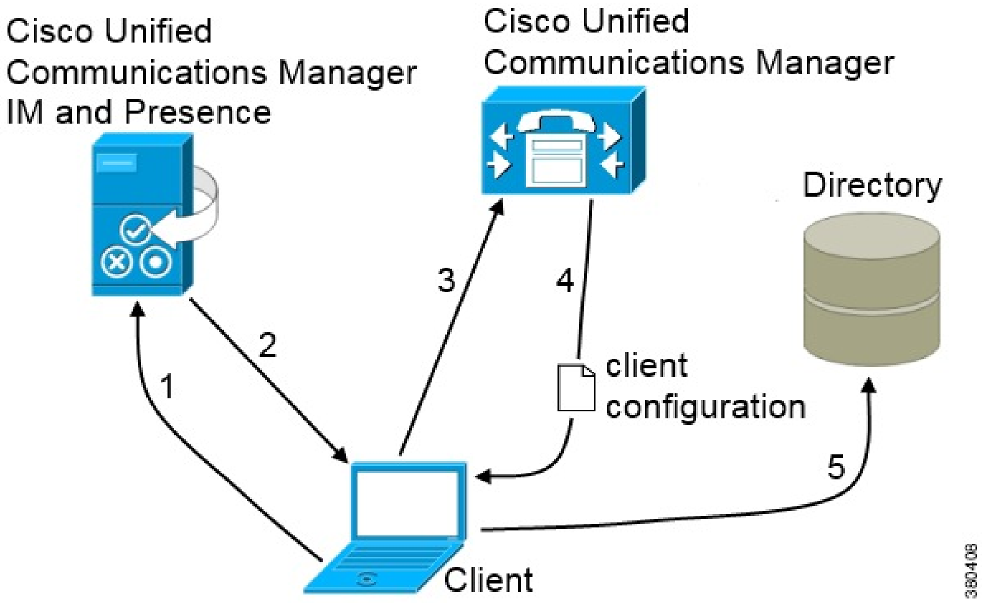
Basic Directory Integration

The client retrieves contact data from the directory service as follows.

1. The client connects to the Cisco Unified Communication Manager IM and Presence Service node.
2. The client gets the LDAP profile configuration section in the service profile from the Cisco Unified Communication Manager IM and Presence Service node.

   The service profile contains the location of Cisco Unified Communication Manager (TFTP) node. Depending on your configuration, the service profile can also contain the credentials to authenticate with the directory.
3. The client connects to the Cisco Unified Communication Manager node.
4. The client downloads the client configuration file from the Cisco Unified Communication Manager node.

   The client configuration file contains the location of the directory. Depending on your configuration, the client configuration file can also contain the credentials to authenticate with the directory.
5. The client uses the directory location and the authentication credentials to connect to the directory.


Cisco Unified Communications Manager IM and Presence
Cisco Unified Communications Manager
Directory
1
2
3
4
5
client configuration
Client
360408

Authentication with Contact Sources

BDI requires users to authenticate with the directory source to resolve contacts. You can use the following methods to authenticate with the contact source, in order of priority:

- Specify credentials in Cisco Unified Presence or Cisco Unified Communications Manager — Specify credentials in a profile on the server. The client can then retrieve the credentials from the server to authenticate with the directory. This method is the most secure option for storing and transmitting credentials.
- Set common credentials in the client configuration file — Specify a shared username and password in the client configuration file. The client can then authenticate with the directory server.

Important The client transmits and stores these credentials as plain text.

Use a well-known or public set of credentials for an account that has read-only permissions.

- Use anonymous binds — Configure the client to connect to the directory source with anonymous binds.

Specify LDAP Directory Configuration on Cisco Unified Presence

If your environment includes Cisco Unified Presence release 8.x, you can specify directory configuration in the LDAP profile. The client can then get the directory configuration from the server to authenticate with the directory source.

Complete the steps to create an LDAP profile that contains authentication credentials, and then assign that profile to users.

Procedure

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

Step 2 Select **Application** > **Cisco Unified Personal Communicator** > **LDAP Profile**.

Step 3 Select **Add New**.

Step 4 Specify a name and optional description for the profile.

Step 5 Specify a distinguished name for a user ID that is authorized to run queries on the LDAP server. Cisco Unified Presence uses this name for authenticated bind with the LDAP server.

Step 6 Specify a password that the client can use to authenticate with the LDAP server.

Step 7 Select **Add Users to Profile** and add the appropriate users to the profile.

Step 8 Select **Save**.

What to do next

Specify any additional BDI information in the client configuration file.

Specify LDAP Directory Configuration on Cisco Unified Communications Manager

If your environment includes Cisco Unified Communications Manager release 9.x and later, you can specify credentials when you add a directory service. The client can then get the configuration from the server to authenticate with the directory source.

Complete the steps to add a directory service, apply the directory service to the service profile, and specify the LDAP authentication configuration for the directory service.

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 **Directory** from the **UC Service Type** drop-down list.

Step 5 Select **Next**.

Step 6 Enter details for the directory service:

- Product Type — Select **Directory**
- Name — Enter a unique name for the directory service
- Hostname/IP Address — Enter the Hostname, IP Address, or FQDN of the directory server.
- Protocol Type — From the drop-down list, select:
  - TCP or UDP for Cisco Jabber for Windows
  - TCP or TLS for Cisco Jabber for iPhone or iPad
  - TCP or TLS for Cisco Jabber for Android

Step 7 Select **Save**.

Step 8 Apply the directory service to your service profile as follows:

a) Select **User Management** > **User Settings** > **Service Profile**.

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

b) Find and select your service profile.

The **Service Profile Configuration** window opens.

c) In the **Directory Profile** section, select up to three services from the **Primary**, **Secondary**, and **Tertiary** drop-down lists:

d) Specify the **Username** and **Password** that the client can use to authenticate with the LDAP server in the following fields:

e) Select **Save**.

Set Credentials in the Client Configuration

You can set credentials in the client configuration with the following parameters:

- BDIConnectionUsername
- BDIConnectionPassword

Important The client transmits and stores these credentials as plain text.

Use a well-known or public set of credentials for an account that has read-only permissions.

The following is an example configuration:

```
<Directory>
  <BDIConnectionUsername>admin@example.com</BDIConnectionUsername>
  <BDIConnectionPassword>password</BDIConnectionPassword>
</Directory>
```

Use Anonymous Binds

To use anonymous binds, you set the following parameters in the client configuration file:

Parameter	Value
DirectoryServerType	BDI
BDIPrimaryServerName	IP address FQDN
BDIEnableTLS	True
BDISearchBase1	Searchable organizational unit (OU) in the directory tree
BDIBaseFilter	Object class that your directory service uses; for example, inetOrgPerson

Parameter	Value
BDIPredictiveSearchFilter	UID or other search filter A search filter is optional.

The following is an example configuration:

```
<Directory>
  <DirectoryServerType>BDI</DirectoryServerType>
  <BDIPrimaryServerName>11.22.33.456</BDIPrimaryServerName>
  <BDIEnableTLS>True</BDIEnableTLS>
  <BDISearchBase1>ou=people,dc=cisco,dc=com</BDISearchBase1>
  <BDIBaseFilter>(&amp;(objectClass=inetOrgPerson)</BDIBaseFilter>
  <BDIPredictiveSearchFilter>uid</BDIPredictiveSearchFilter>
</Directory>
```

Cisco Unified Communications Manager User Data Service

User Data Service (UDS) is a REST interface on Cisco Unified Communications Manager that provides contact resolution.

UDS is used for contact resolution in the following cases:

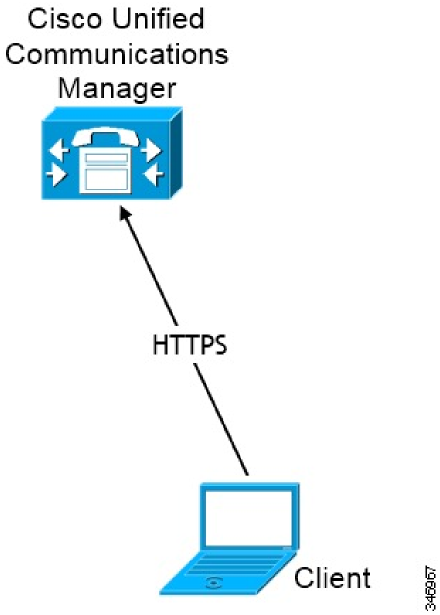
- If you set the DirectoryServerType parameter to use a value of UDS in the client configuration file.

  With this configuration, the client uses UDS for contact resolution when it is inside or outside of the corporate firewall.

- If you deploy Expressway for Remote and Mobile Access.

  With this configuration, the client automatically uses UDS for contact resolution when it is outside of the corporate firewall.

You synchronize contact data into Cisco Unified Communications Manager from a directory server. Cisco Jabber then automatically retrieves that contact data from UDS.



Enable Integration with UDS

To enable integration with UDS, perform the following steps:

Procedure

Step 1 Create your directory source in Cisco Unified Communications Manager.

Step 2 Synchronize the contact data to Cisco Unified Communications Manager.

After the synchronization occurs, your contact data resides in Cisco Unified Communications Manager.

Step 3 Specify UDS as the value of the DirectoryServerType parameter in your configuration file.

The following is an example configuration where UDS is the directory server type:

```
<Directory>
 <DirectoryServerType>UDS</DirectoryServerType>
</Directory>
```

Important This step is required only if you want to use UDS for all contact resolution (that is, both inside and outside the firewall). If you configure Expressway for Mobile and Remote Access, the client automatically uses UDS when outside the firewall, regardless of the value of the DirectoryServerType parameter. When using Expressway for Mobile and Remote Access, you can set the value of the DirectoryServerType parameter to either UDS or an LDAP-based contact source for use inside the firewall.

Step 4 For manual connections, specify the IP address of the Cisco Unified Communications Manager server to ensure that the client can discover the server.

The following is an example configuration for the Cisco Unified Communications Manager server:

```
<UdsServer>11.22.33.444</UdsServer>
```

Step 5 Configure the client to retrieve contact photos with UDS.

The following is an example configuration for contact photo retrieval:

```
<UdsPhotoUriWithToken>http://server_name.domain/%%uid%%.jpg</UdsPhotoUriWithToken>
```

Contact Resolution with Multiple Clusters

For contact resolution with multiple Cisco Unified Communications Manager clusters, synchronize all users on the corporate directory to each cluster. Provision a subset of those users on the appropriate 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 `cucm-cluster-na` and the 20,000 users in Europe on `cucm-cluster-eu`.

When users in Europe call users in North America, Cisco Jabber retrieves the contact details for the user in Europe from `cucm-cluster-na`.

When users in North America call users in Europe, Cisco Jabber retrieves the contact details for the user in North America from `cucm-cluster-eu`.

Client Availability

Users can define whether their availability reflects their calendar events by setting an option to let others know they are in a meeting from the **Status** tab of the **Options** window from the client. This option synchronizes events in your calendar with your availability. The client only displays **In a meeting** availability for supported integrated calendars.

The client supports using two sources for the **In a meeting** availability:

Note Cisco Jabber for mobile clients don't support this meeting integration.

- Microsoft Exchange and Cisco Unified Communication Manager IM and Presence Integration — Applies to on-premises deployments. The **Include Calendar information in my Presence Status** field in Cisco Unified Presence is the same as the **In a meeting** option in the client. Both fields update the same value in the Cisco Unified Communication Manager IM and Presence database.

  If users set both fields to different values, then the last field that the user sets takes priority. If users change the value of the **Include Calendar information in my Presence Status** field while the client is running, the users must restart the client for those changes to apply.

- Cisco Jabber Client — Applies to on-premises and cloud-based deployments. You must disable Cisco Unified Communication Manager IM and Presence and Microsoft Exchange integration for the client to set the **In a meeting** availability. The client checks if integration between Cisco Unified Communication

Manager IM and Presence and Microsoft Exchange is on or off. The client can only set availability if integration is off.

The following deployment scenarios describe how availability is created:

Deployment Scenario	You select In a meeting (according to my calendar)	You do not select In a meeting (according to my calendar)
You enable integration between Cisco Unified Communication Manager IM and Presence and Microsoft Exchange.	Cisco Unified Communication Manager IM and Presence sets availability status	Availability status does not change
You do not enable integration between Cisco Unified Communication Manager IM and Presence and Microsoft Exchange.	Client sets availability status	Availability status does not change
Cloud-based deployments	Client sets availability status	Availability status does not change

Additionally, the following table describes availability that is supported differently by each deployment scenarios:

Availability Enabled in the Client	Availability Enabled by Integrating Cisco Unified Communication Manager IM and Presence with Microsoft Exchange
Offline in a meeting availability is not supported.	**Offline in a meeting** availability is supported.
In a meeting availability is supported for non-calendar events.	**In a meeting** availability is not supported for non-calendar events.

Note Offline in a meeting availability refers to when the user is not logged in to the client but an event exists in the user's calendar.

Non-calendar events refer to events that do not appear in the user's calendar, such as instant meetings, **Offline**, or **On a call**.

Related Topics

Calendar Integration, on page 53

Multiple Resource Login

All Cisco Jabber clients register with one of the following central IM and Presence Service nodes when a user logs in to the system. This node tracks availability, contact lists, and other aspects of the IM and Presence Service environment.

- On-Premises Deployments: Cisco Unified Communications Manager IM and Presence Service.
- Cloud Deployments: Cisco Webex.

This IM and Presence Service node tracks all of the registered clients associated with each unique network user in the following order:

1. When a new IM session is initiated between two users, the first incoming message is broadcast to all of the registered clients of the receiving user.
2. The IM and Presence Service node waits for the first response from one of the registered clients.
3. The first client to respond then receives the remainder of the incoming messages until the user starts responding using another registered client.
4. The node then reroutes subsequent messages to this new client.

Note If there is no active resource when a user is logged into multiple devices, then priority is given to the client with the highest presence priority. If the presence priority is the same on all devices, then priority is given to the latest client the user logged in to.

Instant Message Encryption

Cisco Jabber uses Transport Layer Security (TLS) to secure Extensible Messaging and Presence Protocol (XMPP) traffic over the network between the client and server. Cisco Jabber encrypts point to point instant messages.

On-Premises Encryption

The following table summarizes the details for instant message encryption in on-premises deployments.

Connection	Protocol	Negotiation Certificate	Expected Encryption Algorithm
Client to server	XMPP over TLS v1.2	X.509 public key infrastructure certificate	AES 256 bit

Server and Client Negotiation

The following servers negotiate TLS encryption with Cisco Jabber using X.509 public key infrastructure (PKI) certificates with the following:

- Cisco Unified Communications Manager IM and Presence
- Cisco Unified Communications Manager

After the server and client negotiate TLS encryption, both the client and server generate and exchange session keys to encrypt instant messaging traffic.

The following table lists the PKI certificate key lengths for Cisco Unified Communications Manager IM and Presence Service.

Version	Key Length
Cisco Unified Communications Manager IM and Presence Service versions 9.0.1 and higher	2048 bit
Cisco Unified Presence version 8.6.4	2048 bit
Cisco Unified Presence versions lower than 8.6.4	1024 bit

XMPP Encryption

Cisco Unified Communications Manager IM and Presence Service uses 256-bit length session keys that are encrypted with the AES algorithm to secure instant message traffic between Cisco Jabber and the presence server.

If you require additional security for traffic between server nodes, you can configure XMPP security settings on Cisco Unified Communications Manager IM and Presence Service. See the following for more information about security settings:

- Cisco Unified Presence—*Configuring Security on Cisco Unified Presence*
- Cisco Unified Communications Manager IM and Presence Service—*Security configuration on IM and Presence*

Instant Message Logging

You can log and archive instant messages for compliance with regulatory guidelines. To log instant messages, you either configure an external database or integrate with a third-party compliance server. Cisco Unified Communications Manager IM and Presence Service does not encrypt instant messages that you log in external databases or in third party compliance servers. You must configure your external database or third party compliance server as appropriate to protect the instant messages that you log.

See the following for more information about compliance:

- Cisco Unified Presence— *Instant Messaging Compliance Guide*
- Cisco Unified Communications Manager IM and Presence Service—*Instant Messaging Compliance for IM and Presence Service*

For more information about encryption levels and cryptographic algorithms, including symmetric key algorithms such as AES or public key algorithms such as RSA, see *Next Generation Encryption* at this link https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html.

For more information about X.509 public key infrastructure certificates, see the *Internet X.509 Public Key Infrastructure Certificate and CRL Profile* document at this link https://www.ietf.org/rfc/rfc2459.txt.

Related Topics

Instant Messaging Compliance Guide
Configuring Security on Cisco Unified Presence
Instant Messaging Compliance for IM and Presence Service
Security configuration on IM and Presence
Internet X.509 Public Key Infrastructure Certificate and CRLProfile
Next Generation Encryption

Cloud-Based Encryption

The following table summarizes the details for instant message encryption in cloud-based deployments:

Connection	Protocol	Negotiation Certificate	Expected Encryption Algorithm
Client to server	XMPP within TLS	X.509 public key infrastructure certificate	AES 128 bit
Client to client	XMPP within TLS	X.509 public key infrastructure certificate	AES 256 bit

Server and Client Negotiation

The following servers negotiate TLS encryption with Cisco Jabber using X.509 public key infrastructure (PKI) certificates with the Cisco Webex Messenger service.

After the server and client negotiate TLS encryption, both the client and server generate and exchange session keys to encrypt instant messaging traffic.

XMPP Encryption

The Cisco Webex Messenger service uses 128-bit session keys that are encrypted with the AES algorithm to secure instant message traffic between Cisco Jabber and the Cisco Webex Messenger service.

You can optionally enable 256-bit client-to-client AES encryption to secure the traffic between clients.

Instant Message Logging

The Cisco Webex Messenger service can log instant messages, but it does not archive those instant messages in an encrypted format. However, the Cisco Webex Messenger service uses stringent data center security, including SAE-16 and ISO-27001 audits, to protect the instant messages that it logs.

The Cisco Webex Messenger service cannot log instant messages if you enable AES 256 bit client-to-client encryption.

For more information about encryption levels and cryptographic algorithms, including symmetric key algorithms such as AES or public key algorithms such as RSA, see *Next Generation Encryption* at this link https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html.

For more information about X.509 public key infrastructure certificates, see the *Internet X.509 Public Key Infrastructure Certificate and CRL Profile* document at this link https://www.ietf.org/rfc/rfc2459.txt.

Related Topics

- Client to Client Encryption
- Internet X.509 Public Key Infrastructure Certificate and CRLProfile
- Next Generation Encryption

Client-to-Client Encryption

By default, instant messaging traffic between the client and the Cisco WebEx Messenger service is secure. You can optionally specify policies in the Cisco WebEx Administration Tool to secure instant messaging traffic between clients.

The following policies specify client-to-client encryption of instant messages:

- **Support AES Encoding For IM**—Sending clients encrypt instant messages with the AES 256-bit algorithm. Receiving clients decrypt instant messages.
- **Support No Encoding For IM**—Clients can send and receive instant messages to and from other clients that do not support encryption.

The following table describes the different combinations that you can set with these policies.

Policy Combination	Client-to-Client Encryption	When the Remote Client Supports AES Encryption	When the Remote Client Does not Support AES Encryption
Support AES Encoding For IM = false **Support No Encoding For IM** = true	No	Cisco Jabber sends unencrypted instant messages. Cisco Jabber does not negotiate a key exchange. As a result, other clients do not send Cisco Jabber encrypted instant messages.	Cisco Jabber sends and receives unencrypted instant messages.
Support AES Encoding For IM = true **Support No Encoding For IM** = true	Yes	Cisco Jabber sends and receives encrypted instant messages. Cisco Jabber displays an icon to indicate instant messages are encrypted.	Cisco Jabber sends encrypted instant messages. Cisco Jabber receives unencrypted instant messages.
Support AES Encoding For IM = true **Support No Encoding For IM** = false	Yes	Cisco Jabber sends and receives encrypted instant messages. Cisco Jabber displays an icon to indicate instant messages are encrypted.	Cisco Jabber does not send or receive instant messages to the remote client. Cisco Jabber displays an error message when users attempt to send instant messages to the remote client.

Note Cisco Jabber does not support client-to-client encryption with group chats. Cisco Jabber uses client-to-client encryption for point-to-point chats only.

For more information about encryption and Cisco WebEx policies, see *About Encryption Levels* in the Cisco WebEx documentation.

Related Topics

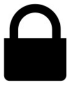
About Encryption Levels

Encryption Icons

Review the icons that the client displays to indicate encryption levels.

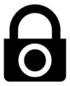
Lock Icon for Client to Server Encryption

In both on-premises and cloud-based deployments, Cisco Jabber displays the following icon to indicate client to server encryption:



Padlock Icon for Client to Client Encryption

In cloud-based deployments, Cisco Jabber displays the following icon to indicate client to client encryption:



Local Chat History

Chat history is retained after participants close the chat window and until participants sign out. If you do not want to retain chat history after participants close the chat window, set the Disable_IM_History parameter to true. This parameter is available to all clients except IM-only users.

For on-premises deployment of Cisco Jabber for Mac, if you select the **Save chat archives to:** option in the **Chat Preferences** window of Cisco Jabber for Mac, chat history is stored locally in the Mac file system and can be searched using Spotlight.

Cisco Jabber does not encrypt archived instant messages when local chat history is enabled.

For mobile clients, you can disable local chat history if you do not want unencrypted instant messages to be stored locally.

For desktop clients, you can restrict access to chat history by savings archives to the following directories:

- Windows, `%`*`USERPROFILE`*`%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\History\`*`uri`*`.db`
- Mac: `~/Library/Application Support/Cisco/Unified Communications/Jabber/CSF/History/`*`uri`*`.db`.

Quality of Service Configuration

Cisco Jabber supports the following methods for prioritizing and classifying Real-time Transport Protocol (RTP) traffic as it traverses the network:

- Set DSCP values in IP headers of RTP media packets

Set DSCP Values

Set Differentiated Services Code Point (DSCP) values in RTP media packet headers to prioritize Cisco Jabber 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.

Port Ranges on Cisco Unified Communications Manager

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

You set port ranges on the **SIP Profile Configuration** window for the Cisco Jabber for iPhone SIP profile on Cisco Unified Communications Manager.

You set port ranges on the **SIP Profile Configuration** window for the Cisco Jabber for Android SIP profile on Cisco Unified Communications Manager.

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

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

Define a Port Range on the SIP Profile

The client uses the port range to send RTP traffic across the network. The client divides the port range equally and uses the lower half for audio calls and the upper half for video calls. 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.

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**.

Related Topics

- 8.6.x: SIP Profile Configuration
- 9.0.x: SIP profile setup

How the Client Uses Port Ranges

Cisco Jabber 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

The following table describes the options for setting DSCP values:

Method for Setting DSCP Values	Microsoft Windows 7
Set DSCP values with Microsoft Group Policy	Yes
Set DSCP values on network switches and routers	Yes
Set DSCP values on Cisco Unified Communications Manager	No

Set DSCP Values on Cisco Unified Communications Manager

You can set DSCP values for audio media and video media on Cisco Unified Communications Manager. Cisco Jabber can then retrieve the DSCP values from the device configuration and apply them directly to the IP headers of RTP media packets.

Restriction For later operating systems such as Microsoft Windows 7, Microsoft implements a security feature that prevents applications from setting DSCP values on IP packet headers. For this reason, you should use an alternate method for marking DSCP values, such as Microsoft Group Policy.

For more information on configuring flexible DSCP values, refer to Configure Flexible DSCP Marking and Video Promotion Service Parameters.

Procedure

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

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

The **Service Parameter Configuration** window opens.

Step 3 Select the appropriate server and then select the **Cisco CallManager** service.

Step 4 Locate the **Clusterwide Parameters (System - QOS)** section.

Step 5 Specify DSCP values as appropriate and then select **Save**.

Set DSCP Values with Group Policy

If you deploy Cisco Jabber for Windows on a later 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	`CiscoJabber.exe`	`CiscoJabber.exe`	`CiscoJabber.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
DSCP value	46	34	24

Set DSCP Values on the Client

For some configurations, there is an option to enable differentiated services for calls in the Cisco Jabber for Mac client.

Important This option is enabled by default. Cisco recommends not disabling this option unless you are experiencing issues in the following scenarios:

- You can hear or see other parties, but you cannot be heard or seen
- You are experiencing unexpected Wi-Fi disconnection issues

Disabling differentiated service for calls may degrade audio and video quality.

Procedure

In Cisco Jabber for Mac, go to **Jabber > Preferences > Calls > Advanced** and select **Enable Differentiated Service for Calls**.

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 Jabber and Cisco Unified Communications Manager occurs through port 5060.

  You should mark signaling packets as AF31.

Protocol Handlers

Cisco Jabber registers the following protocol handlers with the operating system to enable click-to-call or click-to-IM functionality from web browsers or other applications:

- XMPP: or XMPP://

  Starts an instant message and opens a chat window in Cisco Jabber.
- IM: or IM://

  Starts an instant message and opens a chat window in Cisco Jabber.
- TEL: or TEL://

  Starts an audio or video call with Cisco Jabber.

  Note TEL is registered by Apple native phone. It cannot be used to cross launch Cisco Jabber for iPhone and iPad.
- CISCOTEL: or CISCOTEL://

  Starts an audio or video call with Cisco Jabber.
- SIP: or SIP://

  Starts an audio or video call with Cisco Jabber.

Registry Entries for Protocol Handlers

To register as a protocol handler, the client writes to the following locations in the Microsoft Windows registry:

- `HKEY_CLASSES_ROOT\tel\shell\open\command`
- `HKEY_CLASSES_ROOT\xmpp\shell\open\command`
- `HKEY_CLASSES_ROOT\im\shell\open\command`

In the case where two or more applications register as handlers for the same protocol, the last application to write to the registry takes precedence. For example, if Cisco Jabber registers as a protocol handler for XMPP: and then a different application registers as a protocol handler for XMPP:, the other application takes precedence over Cisco Jabber.

Protocol Handlers on HTML Pages

You can add protocol handlers on HTML pages as part of the `href` attribute. When users click the hyperlinks that your HTML pages expose, the client performs the appropriate action for the protocol.

TEL and IM Protocol Handlers

Example of the TEL: and IM: protocol handlers on an HTML page:

```
<html>
  <body>
    <a href="TEL:1234">Call 1234</a><br/>
    <a href="IM:msmith@domain">Send an instant message to Mary Smith</a>
  </body>
</html>
```

In the preceding example, when users click the hyperlink to call 1234, the client starts an audio call to that phone number. When users click the hyperlink to send an instant message to Mary Smith, the client opens a chat window with Mary.

CISCOTEL and SIP Protocol Handlers

Example of the CISCOTEL and SIP protocol handlers on an HTML page:

```
<html>
  <body>
    <a href="CISCOTEL:1234">Call 1234</a><br/>
    <a href="SIP:msmith@domain">Call Mary</a><br/>
    <a href="CISCOTELCONF:msmith@domain;amckenzi@domain">Weekly conference call</a>
  </body>
</html>
```

In the preceding example, when users click the *Call 1234* or *Call Mary* hyperlinks, the client starts an audio call to that phone number.

XMPP Protocol Handlers

Example of a group chat using the XMPP: protocol handler on an HTML page:

```
<html>
  <body>
    <a href="XMPP:msmith@domain;amckenzi@domain">Create a group chat with Mary Smith and
Adam McKenzie</a>
  </body>
</html>
```

In the preceding example, when users click the hyperlink to create a group chat with Mary Smith and Adam McKenzie, the client opens a group chat window with Mary and Adam.

Tip Add lists of contacts for the XMPP: and IM: handlers to create group chats. Use a semi-colon to delimit contacts, as in the following example:

```
XMPP:user_a@domain.com;user_b@domain.com;user_c@domain.com;user_d@domain.com
```

Add Subject Lines and Body Text

You can add subject lines and body text to any of the protocol handlers so that when users click on the hyperlink to create a person-to-person or group chat, the client opens a chat window with pre-populated subject line and body text.

Subject and body text can be added in any of the following scenarios:

- Using any supported protocol handler for instant messaging on the client
- For either person-to-person chats or for group chats
- Including a subject and body text, or one or the other

In this example, when users click on the link below it opens a person-to-person chat window with a pre-populated body text of **`I.T Desk`**:

```
xmpp:msmith@domain?message;subject=I.T.%20Desk
```

In this example, when users click on the link below it opens a **Start Group Chat** dialog box with a topic of **I.T Desk**, and the input box for the chat window is pre-populated with the text **`Jabber 10.5 Query`**:

```
im:user_a@domain.com;user_b@domain.com;user_c@domain.com?message;subject=I.T%20Desk;body=Jabber%2010.5%20Query
```

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.

Audio Bit Rates for Cisco Jabber Desktop Clients

The following audio bit rates apply to Cisco Jabber for Windows and Cisco Jabber for Mac.

Codec	RTP (kbits/second)	Actual bit rate (kbits/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

Audio Bit Rates for Cisco Jabber Mobile Clients

The following audio bit rates apply to Cisco Jabber for iPad and iPhone and Cisco Jabber for Android.

Codec	Codec bit rate (kbits/second)	Network Bandwidth Utilized (kbits/second)
g.711	64	80
g.722.1	32	48
g.722.1	24	40
g.729a	8	24

Video Bit Rates for Cisco Jabber Desktop Clients

The following video bit rates (with g.711 audio) apply to Cisco Jabber for Windows and Cisco Jabber for Mac. This table does not list all possible resolutions.

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 for Cisco Jabber.	512 x 288	320
w448p	768 x 448	570
w576p	1024 x 576	890
720p	1280 x 720	1300

Note The measured bit rate is the actual bandwidth used (RTP payload + IP packet overhead).

Video Bit Rates for Cisco Jabber for Android

The client captures and transmits video at 15 fps.

Resolution	Pixels	Bit Rate (kbits per second) with g.711 audio
w144p	256 x 144	290
w288p	512 x 288	340
w360p	640 x 360	415

Video	Resolution	Bandwidth
HD	1280 x 720	1024

Video	Resolution	Bandwidth
VGA	640 x 360	512
CIF	488x211	310

Note To send and receive HD video during calls:

- Configure the maximum bit rate for video calls higher than 1024 kbps in Cisco Unified Communications Manager.
- Enable DSCP on a router to transmit video RTP package with high priority.

Video Bit Rates for Cisco Jabber for iPhone and iPad

The client captures and transmits at 20 fps.

Resolution	Pixels	Bit rate (kbits/second) with g.711 audio
w144p	256 x 144	290
w288p	512 x 288	340
w360p	640 x 360	415
w720p	1280 x 720	1024

Presentation Video Bit Rates

Cisco Jabber captures at 8 fps and transmits at 2 to 8 fps.

The values in this table do not include audio.

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

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 Cisco Jabber allocates the maximum payload bit rate:

Audio	Interactive video (Main video)
Cisco Jabber uses the maximum audio bit rate	Cisco Jabber allocates the remaining bit rate as follows: The maximum video call bit rate minus the audio bit rate.

Bandwidth Performance Expectations for Cisco Jabber Desktop Clients

Cisco Jabber for Mac 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)
125 kbps under VPN	At bandwidth threshold for g.711. Sufficient bandwidth for g.729a and g.722.1.	Insufficient bandwidth for video.
384 kbps under VPN	Sufficient bandwidth for any audio codec.	w288p (512 x 288) at 30 fps
384 kbps in an enterprise network	Sufficient bandwidth for any audio codec.	w288p (512 x 288) at 30 fps
1000 kbps	Sufficient bandwidth for any audio codec.	w576p (1024 x 576) at 30 fps
2000 kbps	Sufficient bandwidth for any audio codec.	w720p30 (1280 x 720) at 30 fps

Cisco Jabber for Windows 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

Upload speed	Audio	Audio + Interactive video (Main video)	Audio + Presentation video (Desktop sharing video)	Audio + Interactive video + Presentation video
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.

Bandwidth Performance Expectations for Cisco Jabber for Android

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

Upload speed	Audio	Audio + Interactive Video (Main Video)
125 kbps under VPN	At bandwidth threshold for g.711. Insufficient bandwidth for video. Sufficient bandwidth for g.729a and g.722.1.	Insufficient bandwidth for video.
256 kbps	Sufficient bandwidth for any audio codec.	Transmission rate (Tx) — 256 x 144 at 15 fps Reception rate (Rx) — 256 x 144 at 30 fps
384 kbps under VPN	Sufficient bandwidth for any audio codec.	Tx — 640 x 360 at 15 fps Rx — 640 x 360 at 30 fps
384 kbps in an enterprise network	Sufficient bandwidth for any audio codec.	Tx — 640 x 360 at 15 fps Rx — 640 x 360 at 30 fps

Note Due to device limitations, the Samsung Galaxy SII and Samsung Galaxy SIII devices cannot achieve the maximum resolution listed in this table.

Bandwidth Performance Expectations for Cisco Jabber for iPhone and iPad

The client 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.

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

Upload speed	Audio	Audio + Interactive Video (Main Video)
125 kbps under VPN	At bandwidth threshold for g.711. Insufficient bandwidth for video. Sufficient bandwidth for g.729a and g.722.1.	Insufficient bandwidth for video.
290 kbps	Sufficient bandwidth for any audio codec.	256 x144 at 20 fps
415 kbps	Sufficient bandwidth for any audio codec.	640 x 360 at 20 fps
1024 kbps	Sufficient bandwidth for any audio codec.	1280 x 720 at 20 fps

Video Rate Adaptation

Cisco Jabber 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.

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

DNS Configuration

How the Client Uses DNS

Cisco Jabber uses domain name servers to do the following:

- Determine whether the client is inside or outside the corporate network.
- Automatically discover on-premises servers inside the corporate network.
- Locate access points for Expressway for Mobile and Remote Access on the public Internet.

How the Client Finds a Name Server

Cisco Jabberlooks for DNS records from:

- Internal name servers inside the corporate network.
- External name servers on the public Internet.

When the client’s host computer or device gets a network connection, the host computer or device also gets the address of a DNS name server from the DHCP settings. Depending on the network connection, that name server might be internal or external to the corporate network.

Cisco Jabber queries the name server that the host computer or device gets from the DHCP settings.

How the Client Gets a Services Domain

The services domain is discovered by the client in different ways.

New installation:

- User enters an address in the format `username@example.com` in the client user interface.
- User clicks on a configuration URL that includes the service domain. This option is only available in the following versions of the client:
    - Cisco Jabber for Android release 9.6 or later
    - Cisco Jabber for Mac release 9.6 or later
    - Cisco Jabber for iPhone and iPad release 9.6.1 or later
- The client uses installation switches in bootstrap files. This option is only available in the following version of the client:
    - Cisco Jabber for Windows release 9.6 or later

Existing installation:

- The client uses the cached configuration.
- User manually enters an address in the client user interface.

In hybrid deployments the domain required to discover Cisco Webex domain through Central Authentication Service (CAS) lookup may be different to the domain where the DNS records are deployed. In this scenario you set the ServicesDomain to be the domain used to discover Cisco Webex and set the VoiceServicesDomain to be the domain where DNS records are deployed. The voice services domain is configured as follows:

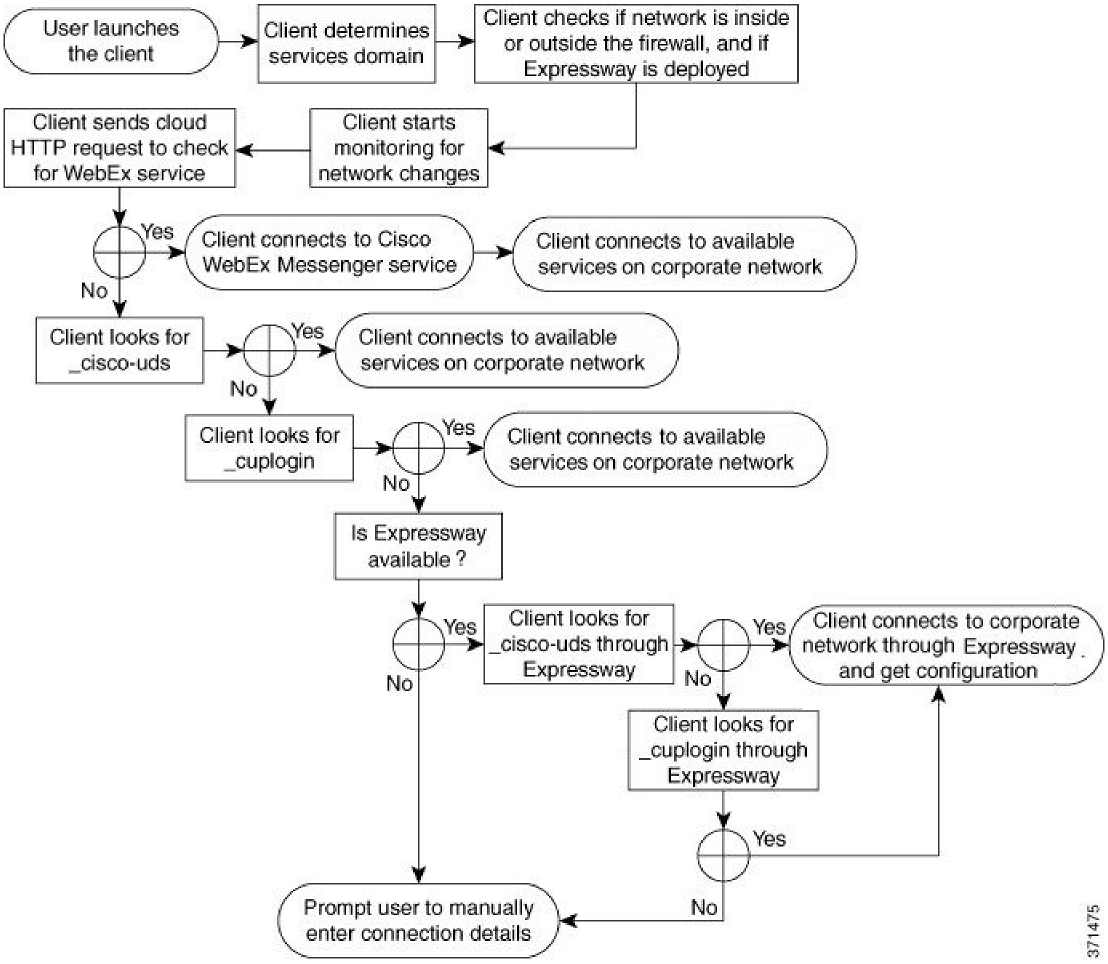
- The client uses the VoiceServicesDomain parameter in the configuration file. This option is available in clients that support the `jabber-config.xml` file.
- User clicks on a configuration URL that includes the VoiceServicesDomain. This option is available in the following clients:
    - Cisco Jabber for Android release 9.6 or later
    - Cisco Jabber for Mac release 9.6 or later
    - Cisco Jabber for iPhone and iPad release 9.6.1 or later
- The client uses the Voice_Services_Domain installation switch in the bootstrap files. This option is only available in the following version of the client:
    - Cisco Jabber for Windows release 9.6 or later

After Cisco Jabber gets the services domain, it queries the name server that is configured to the client computer or device.

How the Client Discovers Available Services

The following figure shows the flow that the client uses to connect to services.

Figure 6: Login Flow for Service Discovery


User launches the client
Client determines services domain
Client checks if network is inside or outside the firewall, and if Expressway is deployed
Client starts monitoring for network changes
Client sends cloud HTTP request to check for WebEx service
Yes
Client connects to Cisco WebEx Messenger service
Client connects to available services on corporate network
No
Client looks for _cisco-uds
Yes
Client connects to available services on corporate network
No
Client looks for _cuplogin
Yes
Client connects to available services on corporate network
No
Is Expressway available ?
Yes
Client looks for _cisco-uds through Expressway
Yes
Client connects to corporate network through Expressway and get configuration
No
No
Client looks for _cuplogin through Expressway
Yes
No
Prompt user to manually enter connection details
371475

To discover available services, the client does the following:

1. Checks if the network is inside or outside the firewall and if Expressway for Mobile and Remote Access is deployed. The client sends a query to the name server to get DNS Service (SRV) records.
2. Starts monitoring for network changes.

   When Expressway for Mobile and Remote Access is deployed, the client monitors the network to ensure that it can reconnect if the network changes from inside or outside the firewall.
3. Issues an HTTP query to a CAS URL for the Cisco Webex Messenger service.

   This query enables the client to determine if the domain is a valid Cisco Webex domain.

   When Expressway for Mobile and Remote Access is deployed, the client connects to Cisco Webex Messenger Service and uses Expressway for Mobile and Remote Access to connect to Cisco Unified Communications Manager. When the client launches for the first time the user will see a Phone Services Connection Error and will have to enter their credentials in the client options screen, subsequent launches will use the cached information.
4. Queries the name server to get DNS Service (SRV) records, unless the records exist in the cache from a previous query.

This query enables the client to do the following:

- Determine which services are available.
- Determine if it can connect to the corporate network through Expressway for Mobile and Remote Access.

Client Issues an HTTP Query

In addition to querying the name server for SRV records to locate available services, Cisco Jabber sends an HTTP query to the CAS URL for the Cisco Webex Messenger service. This request enables the client to determine cloud-based deployments and authenticate users to the Cisco Webex Messenger service.

When the client gets a services domain from the user, it appends that domain to the following HTTP query:

```
https://loginp.webexconnect.com/cas/FederatedSSO?org=
```

For example, if the client gets `example.com` as the services domain from the user, it issues the following query:

```
https://loginp.webexconnect.com/cas/FederatedSSO?org=example.com
```

That query returns an XML response that the client uses to determine if the services domain is a valid Cisco Webex domain.

If the client determines the services domain is a valid Cisco Webex domain, it prompts users to enter their Cisco Webex credentials. The client then authenticates to the Cisco Webex Messenger service and retrieves the configuration and UC services that are configured in Cisco Webex Org Admin.

If the client determines the services domain is not a valid Cisco Webex domain, it uses the results of the query to the name server to locate available services.

When the client sends the HTTP request to the CAS URL, it uses configured system proxies.

For the desktop clients, to configure a proxy in the **LAN Settings** of Internet Explorer, you must specify a `.pac` file URL as the automatic configuration script or specify an explicit proxy address under **Proxy server**.

For iOS clients, you can configure a proxy in the Wi-Fi settings of an iOS device, using one of the following methods:

1. Go to **Wi-Fi** > **HTTP PROXY** > **Auto** tab and use Web Proxy Auto-Discovery (WPAD) protocol lookup. Do not specify `.pac` file URL.
2. Specify a `.pac` file URL as the automatic configuration script in **Wi-Fi** > **HTTP PROXY** > **Auto** tab.
3. Specify an explicit proxy address in **Wi-Fi** > **HTTP PROXY** > **Manual** tab.

For Android clients, you can configure a proxy in the Wi-Fi settings of a Android device using one of the following methods:

1. Specify a `.pac` file URL as the automatic configuration script in **Wi-Fi Networks** > **Modify Network** > **Show Advanced Options** > **Proxy Settings** > **Auto** tab.

Note This method is only supported on devices with Android OS 5.0 and higher, and Cisco DX series devices.

2. Specify an explicit proxy address in **Wi-Fi Networks** > **Modify Network** > **Show Advanced Options** > **Proxy Settings** > **Auto** tab.

The following limitations apply when using a proxy for these HTTP requests:

- Proxy Authentication is not supported.
- Wildcards in the bypass list are not supported. Use `example.com` instead of `*.example.com`.
- Web Proxy Auto-Discovery (WPAD) protocol lookup is only supported for iOS devices.
- Cisco Jabber supports proxy for HTTP request using HTTP CONNECT, but does not support proxy when using HTTPS CONNECT.

Client Queries the Name Server

When the client queries a name server, it sends separate, simultaneous requests to the name server for SRV records.

The client requests the following SRV records in the following order:

- `_cisco-uds`
- `_cuplogin`
- `_collab-edge`

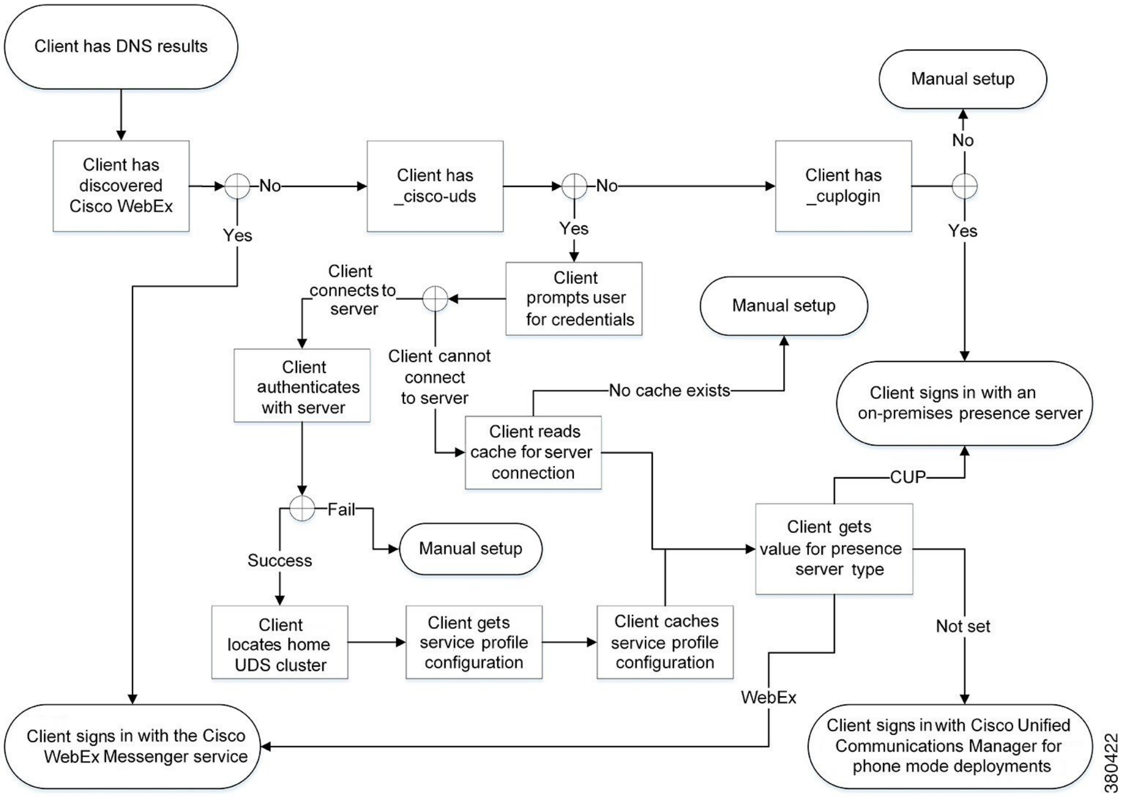
If the name server returns:

- `_cisco-uds`—The client detects it is inside the corporate network and connects to Cisco Unified Communications Manager.
- `_cuplogin`—The client detects it is inside the corporate network and connects to Cisco Unified Presence.
- `_collab-edge`—The client attempts to connect to the internal network through Expressway for Mobile and Remote Access and discover services
- None of the SRV records—The client prompts users to manually enter setup and sign-in details.

Client Connects to Internal Services

The following figure shows how the client connects to internal services:

Figure 7: Client Connecting to Internal Services


Client has DNS results
Client has discovered Cisco WebEx
No
Yes
Client has _cisco-uds
No
Yes
Client has _cuplogin
No
Yes
Manual setup
Client prompts user for credentials
Client connects to server
Client cannot connect to server
Client authenticates with server
Manual setup
No cache exists
Client reads cache for server connection
Client signs in with an on-premises presence server
CUP
Fail
Manual setup
Success
Client gets value for presence server type
Client locates home UDS cluster
Client gets service profile configuration
Client caches service profile configuration
Not set
WebEx
Client signs in with the Cisco WebEx Messenger service
Client signs in with Cisco Unified Communications Manager for phone mode deployments
380422

When connecting to internal services, the goals are to determine the authenticator, sign users in, and connect to available services.

Three possible authenticators can get users past the sign-in screen, as follows:

- Cisco Webex Messenger service—Cloud-based or hybrid cloud-based deployments.
- Cisco Unified Presence—On-premises deployments in the default product mode. The default product mode can be either full UC or IM only.
- Cisco Unified Communications Manager—On-premises deployments in phone mode.

The client connects to any services it discovers, which varies depending on the deployment.

1. If the client discovers that the CAS URL lookup indicates a Cisco Webex user, the client does the following:
    1. Determines that the Cisco Webex Messenger service is the primary source of authentication.
    2. Automatically connects to the Cisco Webex Messenger service.
    3. Prompts the user for credentials.
    4. Retrieves client and service configuration.
2. If the client discovers a `_cisco-uds` SRV record, the client does the following:
    1. Prompts the user for credentials to authenticate with Cisco Unified Communications Manager.
    2. Locates the user's home cluster.

Locating the home cluster enables the client to automatically get the user's device list and register with Cisco Unified Communications Manager.

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

See the appropriate version of the *Cisco Unified Communications Manager Features and Services Guide* to learn how to configure ILS.

3. Retrieves the service profile.

   The service profile provides the client with the authenticator as well as client and UC service configuration.

   The client determines the authenticator from the value of the Product type field in the IM and presence profile, as follows:

   - Cisco Unified Communications Manager—Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service is the authenticator.
   - WebEx (IM and Presence)—Cisco Webex Messenger service is the authenticator.

     Note As of this release, the client issues an HTTP query in addition to the query for SRV records. The HTTP query allows the client to determine if it should authenticate to the Cisco Webex Messenger service.

     As a result of the HTTP query, the client connects to the Cisco Webex Messenger service in cloud-based deployments. Setting the value of the **Product type** field to WebEx does not effect if the client has already discovered the WebEx service using a CAS lookup.

   - Not set—If the service profile does not contain an IM and Presence Service configuration, the authenticator is Cisco Unified Communications Manager.

4. Sign in to the authenticator.

   After the client signs in, it can determine the product mode.

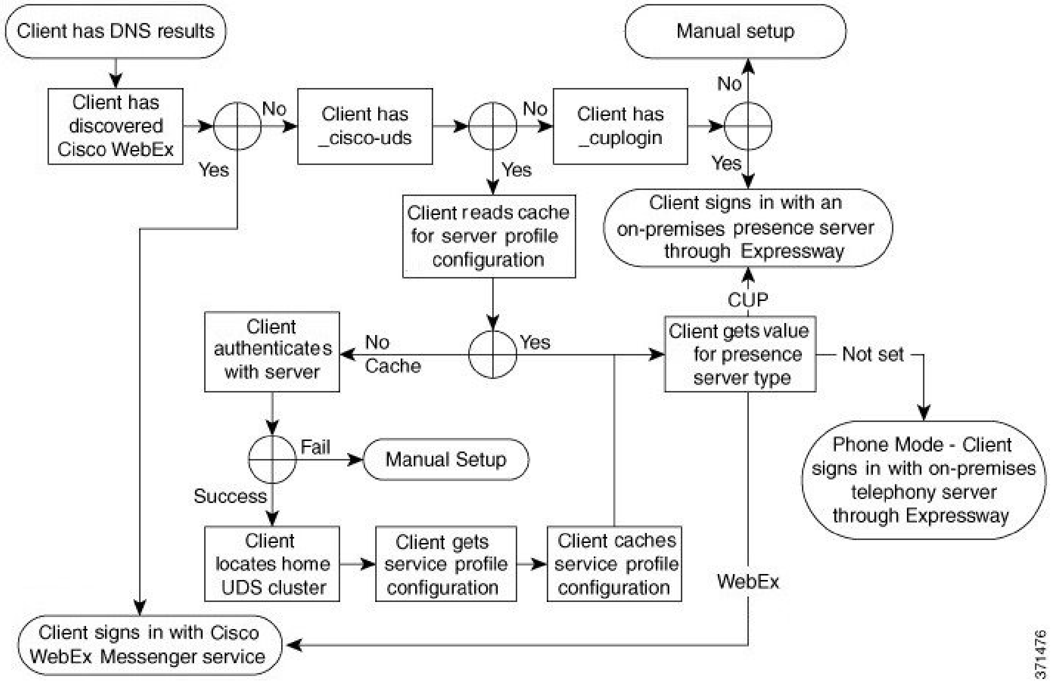
3. If the client discovers a `_cuplogin` SRV record, the client does the following:
   1. Determines that Cisco Unified Presence is the primary source of authentication.
   2. Automatically connects to the server.
   3. Prompts the user for credentials.
   4. Retrieves client and service configuration.

Client Connects through Expressway for Mobile and Remote Access

If the name server returns the `_collab-edge` SRV record, the client attempts to connect to internal servers through Expressway for Mobile and Remote Access.

The following figure shows how the client connects to internal services when the client is connected to the network through Expressway for Mobile and Remote Access:

Figure 8: Client Connects through Expressway for Mobile and Remote Access


Client has DNS results
Client has discovered Cisco WebEx
No
Yes
Client has _cisco-uds
No
Yes
Client has _cuplogin
No
Yes
Manual setup
Client reads cache for server profile configuration
Client signs in with an on-premises presence server through Expressway
CUP
Client authenticates with server
No Cache
Yes
Client gets value for presence server type
Not set
Phone Mode - Client signs in with on-premises telephony server through Expressway
Fail
Manual Setup
Success
Client locates home UDS cluster
Client gets service profile configuration
Client caches service profile configuration
WebEx
Client signs in with Cisco WebEx Messenger service
371476

When the name server returns the `_collab-edge` SRV record, the client gets the location of the Cisco Expressway-E server. The Cisco Expressway-E server then provides the client with the results of the query to the internal name server.

Note The Cisco Expressway-C server looks up the internal SRV records and provides the records to the Cisco Expressway-E server.

After the client gets the internal SRV records, which must include the `_cisco-uds`SRV record, it retrieves service profiles from Cisco Unified Communications Manager. The service profiles then provide the client with the user's home cluster, the primary source of authentication, and configuration.

Domain Name System Designs

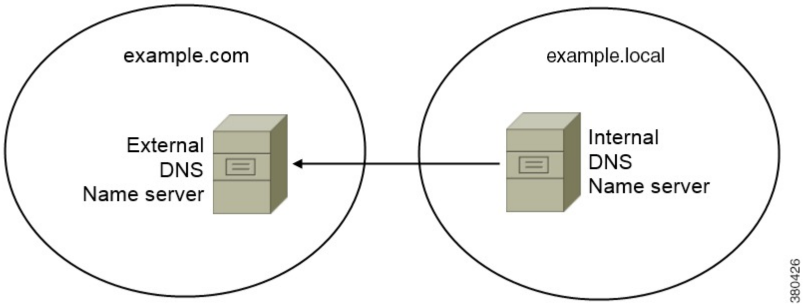
Where you deploy DNS service (SRV) records depends on the design of your DNS namespace. Typically there are two DNS designs:

- Separate domain names outside and inside the corporate network.
- Same domain name outside and inside the corporate network.

Separate Domain Design

The following figure shows a separate domain design:

Figure 9: Separate Domain Design



An example of a separate domain design is one where your organization registers the following external domain with an Internet name authority: `example.com`.

Your company also uses an internal domain that is one of the following:

- A subdomain of the external domain, for example, `example.local`.
- A different domain to the external domain, for example, `exampledomain.com`.

Separate domain designs have the following characteristics:

- The internal name server has zones that contain resource records for internal domains. The internal name server is authoritative for the internal domains.
- The internal name server forwards requests to the external name server when a DNS client queries for external domains.
- The external name server has a zone that contains resource records for your organization's external domain. The external name server is authoritative for that domain.
- The external name server can forward requests to other external name servers. However, the external name server cannot forward requests to the internal name server.

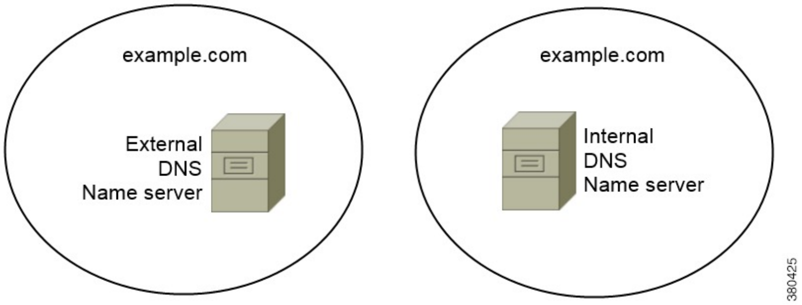
Same Domain Design

An example of a same domain design is one where your organization registers `example.com` as an external domain with an Internet name authority. Your organization also uses `example.com` as the name of the internal domain.

Single Domain, Split-Brain

The following figure shows a single domain with a split-brain domain design.

Figure 10: Single Domain, Split-Brain



Two DNS zones represent the single domain; one DNS zone in the internal name server and one DNS zone in the external name server.

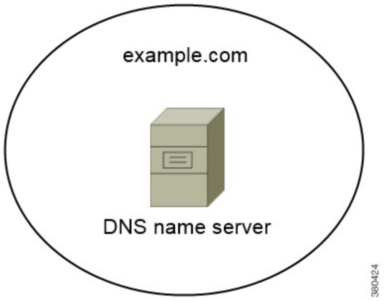
Both the internal name server and the external name server are authoritative for the single domain but serve different communities of hosts.

- Hosts inside the corporate network access only the internal name server.
- Hosts on the public Internet access only the external name server.
- Hosts that move between the corporate network and the public Internet access different name servers at different times.

Single Domain, Not Split-Brain

The following figure shows a single domain that does not have a split-brain domain design.

Figure 11: Single Domain, Not Split-Brain



In the single domain, not split-brain design, internal and external hosts are served by one set of name servers and can access the same DNS information.

Important This design is not common because it exposes more information about the internal network to potential attackers.

Deploy SRV Records

The client queries name servers for records in the services domain. The services domain is determined as described in How the Client Discovers Available Services, on page 89.

You must deploy SRV records in each DNS zone for those service domains if your organization has multiple subsets of users who use different service domains.

Deploy SRV Records in a Separate Domain Structure

In a separate name design there are two domains, an internal domain and an external domain. The client queries for SRV records in the services domain. The internal name server must serve records for the services domain. However in a separate name design, a zone for the services domain might not exist on the internal name server.

If the services domain is not currently served by the internal name server, you can:

- Deploy records within an internal zone for the services domain.
- Deploy records within a pinpoint subdomain zone on the internal name server.

Use an Internal Zone for a Services Domain

If you do not already have a zone for the services domain on the internal name server, you can create one. This method makes the internal name server authoritative for the services domain. Because it is authoritative, the internal name server does not forward queries to any other name server.

This method changes the forwarding relationship for the entire domain and has the potential to disrupt your internal DNS structure. If you cannot create an internal zone for the services domain, you can create a pinpoint subdomain zone on the internal name server.

Use a Pinpoint Subdomain Zone

DNS record lookup on the Cisco internal fixed pinpoint subdomain is a legacy feature for service discovery that is only available with the following versions of Cisco Jabber:

- Cisco Jabber for Windows 9.6.x
- Cisco Jabber for iPhone and iPad 9.6.0

Support of the fixed pinpoint subdomain has been replaced in later versions of Cisco Jabber by the support of the new **VoiceServicesDomain** configuration key.

Example configuration using Service Discovery to replace pinpoint subdomains:

- Internal DNS authoritative for : example.local
- External DNS authoritative for : example.com

```
Set VoiceServicesDomain=cisco-uc.example.com
```

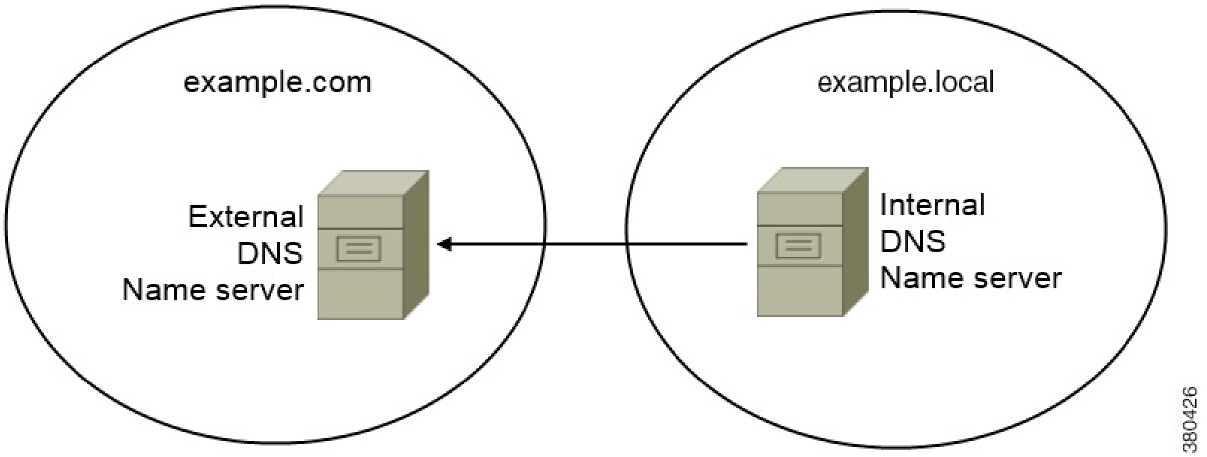
Create a zone on both the internal and external DNS server for `cisco-uc.example.com`.

Create the following SRV records as needed:

- `_cisco-uds._tcp.cisco-uc.example.com` (on Internal DNS)
- `_cuplogin._tcp.cisco-uc.example.com` (on Internal DNS)

You can create a pinpoint subdomain and zone on the internal name server. The pinpoint zone provides a dedicated location to serve specific records for the pinpoint subdomain. As a result, the internal name server becomes authoritative for that subdomain. The internal name server does not become authoritative for the parent domain, so the behavior of queries for records in the parent domain does not change.

The following diagram illustrates configuration created by the procedure.



In this configuration, the following SRV records are deployed with the internal DNS name server:

- `_cisco-uds._tcp.example.com`
- `_cuplogin._tcp.example.com`

Procedure

Step 1 Create a new zone on the internal name server.

Important You must use the following name for the pinpoint subdomain zone: `cisco-internal.`*`services-domain`*.

The pinpoint subdomain zone responds to queries from hosts on the internal network. However, the domain is a subdomain of the external domain. The first part of the name is a fixed value that the client expects, `cisco-internal`.

Step 2 Deploy the `_cisco-uds` and `_cuplogin` SRV records in the pinpoint subdomain zone.

- Before creating a pinpoint subdomain zone
    - The external name server contains a zone for the parent external domain, `example.com`.
    - The internal name server contains a zone for the parent internal domain, `example.local`.
    - The Cisco Jabber Services Domain is `example.com`.
- After creating a pinpoint subdomain zone — The external name server contains a zone for the parent external domain, `example.com`. Internal name server contains the following:
    - Zone for the parent internal domain, `example.local`.
    - Zone for the pinpoint subdmain zone, `cisco-internal.example.com`.

- The internal name server serves the `_cisco-uds` and `_cuplogin` SRV records from `cisco-internal.example.com`.

When the client queries the name server for SRV records, it issues additional queries if the name server does not return `_cisco-uds` or `_cuplogin`.

The additional queries check for the `cisco-internal.`*`domain-name`* pinpoint subdomain zone.

For example, Adam McKenzie's services domain is `example.com` when he starts the client. The client then issues the following query:

```
_cisco-uds._tcp.example.com
_cuplogin._tcp.example.com
_collab-edge._tls.example.com
```

If the name server does not return `_cisco-uds` or `_cuplogin` SRV records, the client then issues the following query:

```
_cisco-uds._tcp.cisco-internal.example.com
_cuplogin._tcp.cisco-internal.example.com
```

SRV Records

Understand which SRV records you should deploy and review examples of each SRV record.

External Records

The following table lists the SRV record you must provision on external name servers as part of the configuration for Expressway for Mobile and Remote Access:

Service Record	Description
`_collab-edge`	Provides the location of the Cisco Expressway-E server. **Note** You must use the fully qualified domain name (FQDN) as the hostname in the SRV record. The client requires the FQDN to use the cookie that the Cisco Expressway-E server provides.

The following is an example of the `_collab-edge` SRV record:

```
_collab-edge._tls.example.com   SRV service location:
          priority       = 3
          weight         = 7
          port           = 8443
          svr hostname   = xpre1.example.com
_collab-edge._tls.example.com   SRV service location:
          priority       = 4
          weight         = 8
          port           = 8443
          svr hostname   = xpre2.example.com
_collab-edge._tls.example.com   SRV service location:
          priority       = 5
          weight         = 0
          port           = 8443
          svr hostname   = xpre3.example.com
```

Internal Records

The following table lists the SRV records you can provision on internal name servers so the client can discover services:

Service Record	Description
`_cisco-uds`	Provides the location of Cisco Unified Communications Manager release 9 and later. **Remember** In an environment with multiple Cisco Unified Communications Manager clusters, you must configure the Intercluster Lookup Service (ILS). ILS enables the client to find the user's home cluster and discover services.
`_cuplogin`	Provides the location of Cisco Unified Presence.

Note You should use the fully qualified domain name (FQDN) as the hostname in the SRV record.

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
```

The following is an example of the `_cuplogin` SRV record:

```
_cuplogin._tcp.example.com      SRV service location:
          priority       = 8
          weight         = 50
          port           = 8443
          svr hostname   = cup3.example.com
_cuplogin._tcp.example.com      SRV service location:
          priority       = 5
          weight         = 100
          port           = 8443
          svr hostname   = cup1.example.com
_cuplogin._tcp.example.com      SRV service location:
          priority       = 7
          weight         = 4
          port           = 8443
          svr hostname   = cup2.example.com
```

CHAPTER 3

Deployment Scenarios

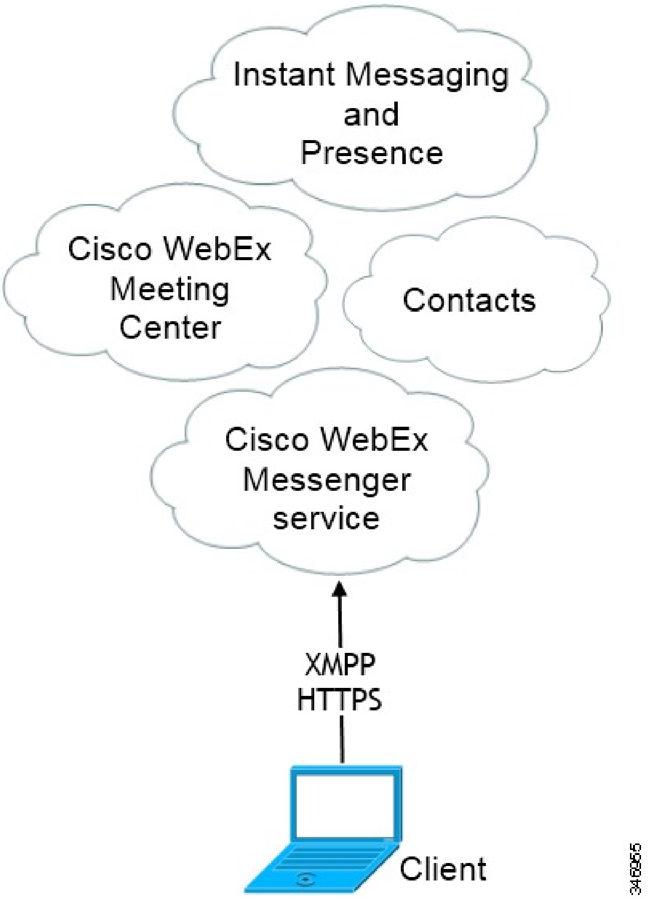
Cloud-Based Deployments

A cloud-based deployment is one in which Cisco Webex hosts services. You manage and monitor your cloud-based deployment with the Cisco Webex Administration Tool.

Cloud-Based Diagram

The following diagram illustrates the architecture of a cloud-based deployment:

Figure 12: Cloud-Based Architecture


Instant Messaging and Presence
Cisco WebEx Meeting Center
Contacts
Cisco WebEx Messenger service
XMPP
HTTPS
Client
346955

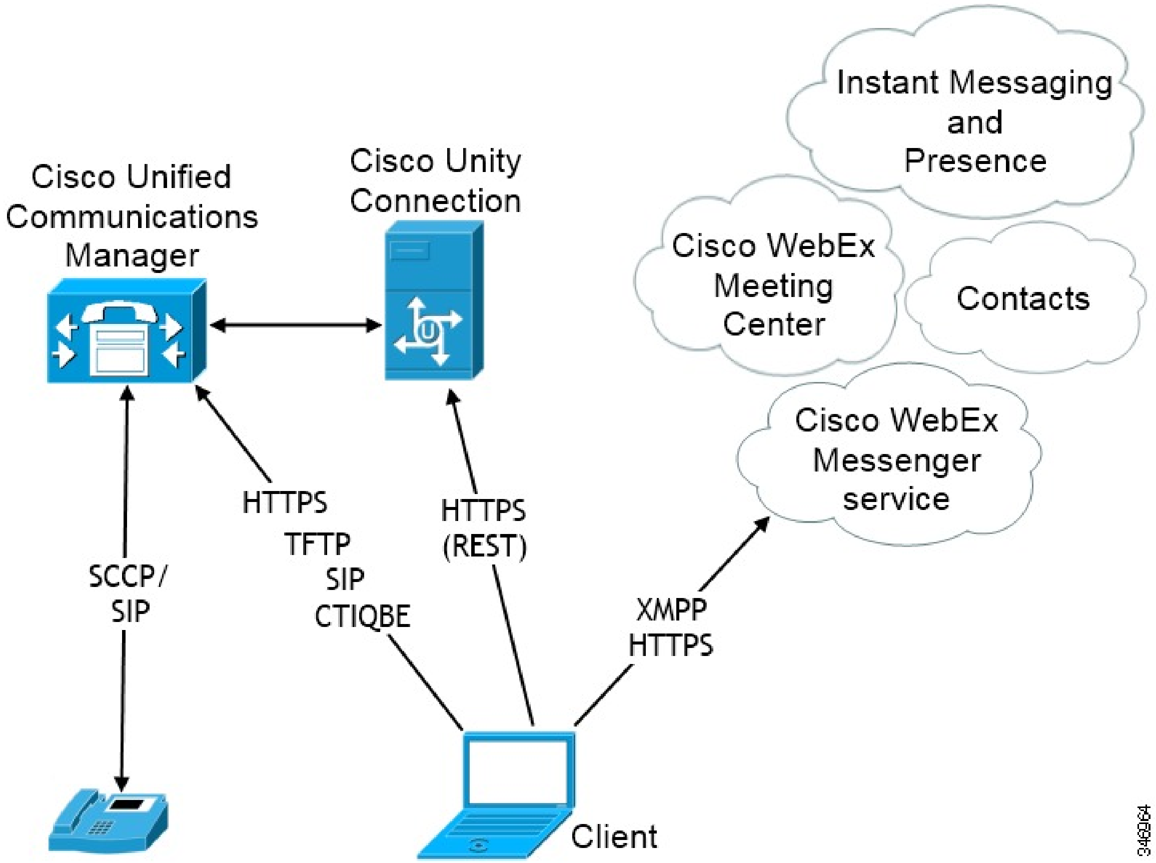
The following are the services available in a cloud-based deployment:

- Contact Source — The Cisco WebEx Messenger service provides contact resolution.
- Presence — The Cisco WebEx Messenger service lets users publish their availability and subscribe to other users' availability.
- Instant Messaging — The Cisco WebEx Messenger service lets users send and receive instant messages.
- Conferencing — Cisco WebEx Meeting Center provides hosted meeting capabilities.

Hybrid Cloud-Based Diagram

The following diagram illustrates the architecture of a hybrid cloud-based deployment:

Figure 13: Hybrid Cloud-Based Architecture


Instant Messaging and Presence
Cisco Unified Communications Manager
Cisco Unity Connection
Cisco WebEx Meeting Center
Contacts
Cisco WebEx Messenger service
HTTPS
TFTP
SIP
CTIQBE
HTTPS (REST)
SCCP/ SIP
XMPP HTTPS
Client
346964

The following are the services available in a hybrid cloud-based deployment:

- Contact Source — The Cisco WebEx Messenger service provides contact resolution.
- Presence — The Cisco WebEx Messenger service lets users can publish their availability and subscribe to other users' availability.
- Instant Messaging — The Cisco WebEx Messenger service lets users send and receive instant messages.
- Conferencing — Cisco WebEx Meeting Center provides hosted meeting capabilities.
- Audio Calls — Users place audio calls through desk phone devices or on their computers through Cisco Unified Communications Manager.
- Video — Users place video calls through Cisco Unified Communications Manager.
- Voicemail — Users send and receive voice messages through Cisco Unity Connection.

On-Premises Deployments

An on-premises deployment is one in which you set up, manage, and maintain all services on your corporate network.

Product Modes

The default product mode is one in which the user's primary authentication is to an IM and presence server.

You can deploy the client in the following modes:

- Full UC — To deploy full UC mode, enable instant messaging and presence capabilities, provision voicemail and conferencing capabilities, and provision users with devices for audio and video.
- IM-Only — To deploy IM-only mode, enable instant messaging and presence capabilities. Do not provision users with devices.
- Phone Mode — In Phone mode, the user's primary authentication is to Cisco Unified Communications Manager. To deploy phone mode, provision users with devices for audio and video capabilities. You can also provision users with additional services such as voicemail.

Default Mode Diagrams

Review architecture diagrams for on-premises deployments in the default product mode.

Full Unified Communications Diagrams

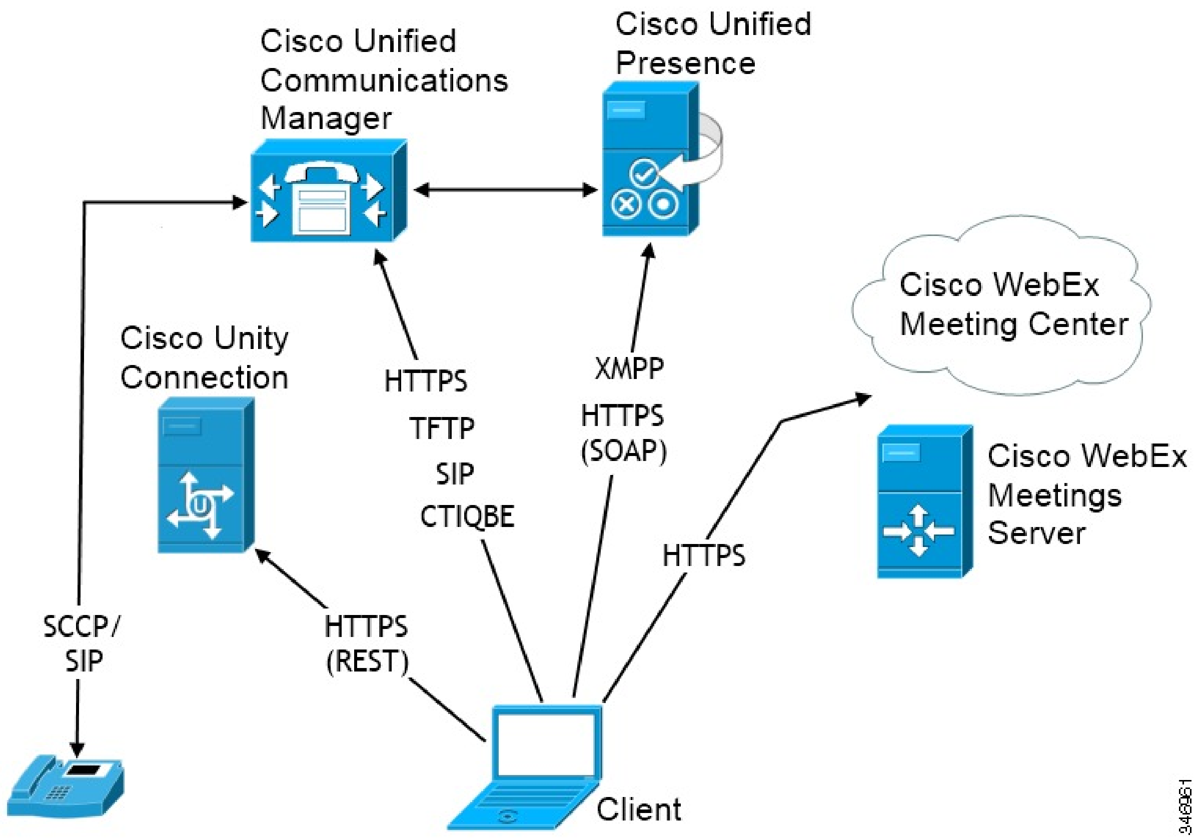
This section contains architecture diagrams for on-premises deployments with full Unified Communications capabilities.

Remember Both full Unified Communications and IM-only deployments require an IM and Presence Service node as the user's primary authentication source. However, IM-only deployments require only IM and Presence Service capabilities. You do not need to provision users with devices in an IM-only deployment.

Cisco Unified Presence

The following diagram illustrates the architecture of an on-premises deployment that includes Cisco Unified Presence.

Figure 14: On-Premises Architecture



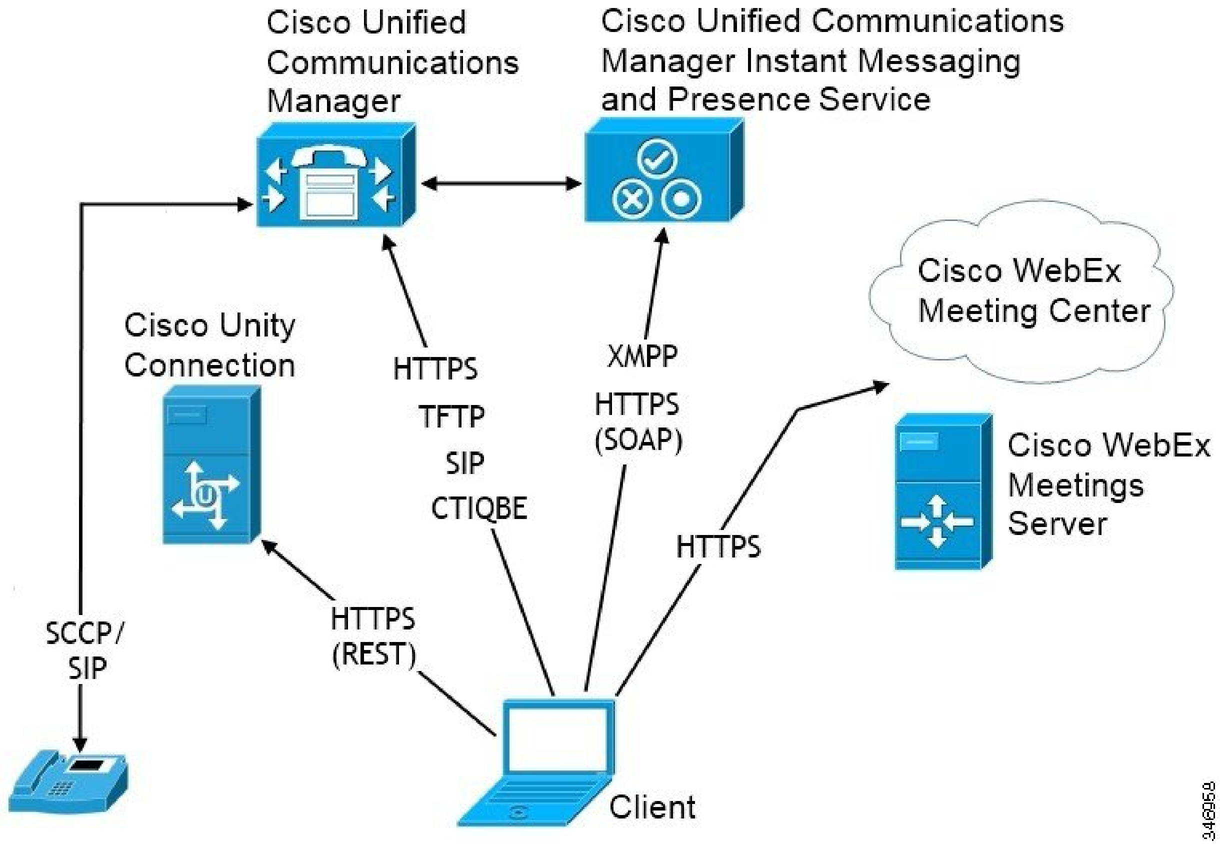
The following are the services available in an on-premises deployment:

- Presence — Publish availability and subscribe to other users' availability through Cisco Unified Presence.
- IM — Users send and receive IMs through Cisco Unified Presence.
- Audio Calls — Place audio calls through desk phone devices or computers through Cisco Unified Communications Manager.
- Video — Place video calls through Cisco Unified Communications Manager.
- Voicemail — Send and receive voice messages through Cisco Unity Connection.
- Conferencing — Integrate with one of the following:
  - Cisco WebEx Meeting Center — Provides hosted meeting capabilities.
  - Cisco WebEx Meetings Server — Provides on-premises meeting capabilities.

Cisco Unified Communications Manager IM and Presence Service

The following diagram illustrates the architecture of an on-premises deployment that includes Cisco Unified Communications Manager IM and Presence Service.

Figure 15: On-Premises Architecture


Cisco Unified Communications Manager
Cisco Unified Communications Manager Instant Messaging and Presence Service
Cisco WebEx Meeting Center
Cisco Unity Connection
HTTPS
TFTP
SIP
CTIQBE
XMPP
HTTPS (SOAP)
Cisco WebEx Meetings Server
HTTPS
SCCP/ SIP
HTTPS (REST)
Client
346958

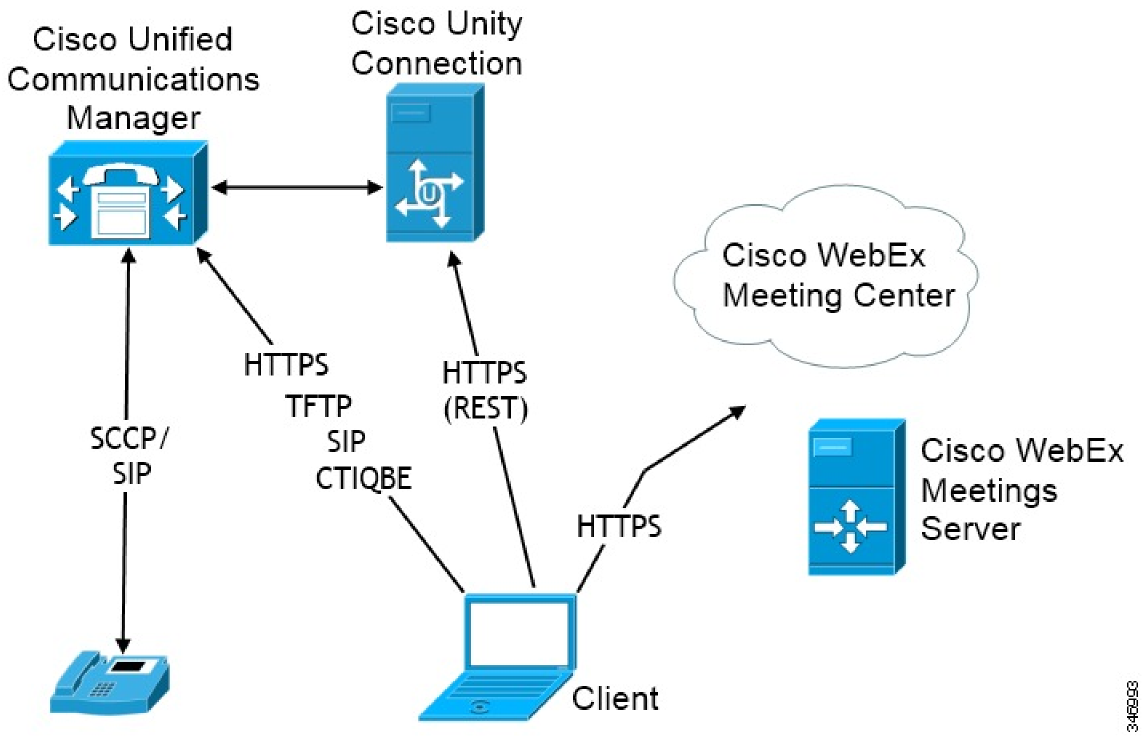
The following are the services available in an on-premises deployment:

- Presence — Publish availability and subscribe to other users' availability through Cisco Unified Communications Manager IM and Presence Service.
- IM — Send and receive IMs through Cisco Unified Communications Manager IM and Presence Service.
- Audio Calls — Place audio calls through desk phone devices or on computers through Cisco Unified Communications Manager.
- Video — Place video calls through Cisco Unified Communications Manager.
- Voicemail — Send and receive voice messages through Cisco Unity Connection.
- Conferencing — Integrate with one of the following:
  - Cisco WebEx Meeting Center — Provides hosted meeting capabilities.
  - Cisco WebEx Meetings Server — Provides on-premises meeting capabilities.

Phone Mode

The following diagram illustrates the architecture of an on-premises deployment for phone mode.

Figure 16: Phone Mode Architecture


Cisco Unified Communications Manager
Cisco Unity Connection
Cisco WebEx Meeting Center
Cisco WebEx Meetings Server
SCCP/ SIP
HTTPS
TFTP
SIP
CTIQBE
HTTPS (REST)
HTTPS
Client
346993

The following are the services available in a phone mode deployment:

- Audio Calls — Place audio calls through desk phone devices or computers through Cisco Unified Communications Manager
- Video — Place video calls through Cisco Unified Communications Manager.
- Voicemail — Send and receive voice messages through Cisco Unity Connection.
- Conferencing — Integrate with one of the following:
  - Cisco WebEx Meeting Center — Provides hosted meeting capabilities.
  - Cisco WebEx Meetings Server — Provides on-premises meeting capabilities.

  Conferencing is not supported in this mode by Cisco Jabber for Android.

Cisco AnyConnect Deployments

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

The Cisco AnyConnect environment includes the following components:

- Cisco Adaptive Security Appliance — Provides a service to secure remote access.

- Cisco AnyConnect Secure Mobility Client — Establishes a secure connection to Cisco Adaptive Security Appliance from the user's device.

This section provides information that you should consider when deploying the Cisco Adaptive Security Appliance (ASA) with the Cisco AnyConnect Secure Mobility Client. Cisco AnyConnect is the supported VPN for Cisco Jabber for Android and Cisco Jabber for iPhone and iPad. If you use an unsupported VPN client, ensure that you install and configure the VPN client using the relevant third-party documentation.

For Samsung devices running Android OS 4.4.x, use Samsung AnyConnect version 4.0.01128 or later. For Android OS version above 5.0, you must use Cisco AnyConnect software version later than 4.0.01287.

Cisco AnyConnect provides remote users with secure IPsec (IKEv2) or SSL VPN connections to the Cisco 5500 Series ASA. Cisco AnyConnect can be deployed to remote users from the ASA or using enterprise software deployment systems. When deployed from the ASA, remote users make an initial SSL connection to the ASA by entering the IP address or DNS name in the browser of an ASA configured to accept clienteless SSL VPN connections. The ASA then presents a login screen in the browser window, if the user satisfies the login and authentication, it downloads the client that matches the computer operating system. After downloading, the client installs and configures itself and establishes an IPsec (IKEv2) or SSL connection to the ASA.

For information about requirements for Cisco Adaptive Security Appliance and Cisco AnyConnect Secure Mobility Client, see the *Software Requirements* topic.

Related Topics

Navigating the Cisco ASA Series Documentation
Cisco AnyConnect Secure Mobility Client

Application Profiles

After you download the Cisco AnyConnect Secure Mobility Client to their device, the ASA must provision a configuration profile to the application.

The configuration profile for the Cisco AnyConnect Secure Mobility Client includes VPN policy information such as the company ASA VPN gateways, the connection protocol (IPSec or SSL), and on-demand policies.

You can provision application profiles for Cisco Jabber for iPhone and iPad in one of the following ways:

ASDM

We recommend that you use the profile editor on the ASA Device Manager (ASDM) to define the VPN profile for the Cisco AnyConnect Secure Mobility Client.

When you use this method, the VPN profile is automatically downloaded to the Cisco AnyConnect Secure Mobility Client after the client establishes the VPN connection for the first time. You can use this method for all devices and OS types, and you can manage the VPN profile centrally on the ASA.

For more information, see the *Creating and Editing an AnyConnect Profile* topic of the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for your release.

iPCU

You can provision iOS devices using an Apple configuration profile that you create with the iPhone Configuration Utility (iPCU). Apple configuration profiles are XML files that contain information such as device security policies, VPN configuration information, and Wi-Fi, mail, and calendar settings.

The high-level procedure is as follows:

1. Use iPCU to create an Apple configuration profile.

   For more information, see the iPCU documentation.

2. Export the XML profile as a .mobileconfig file.

3. Email the .mobileconfig file to users.

   After a user opens the file, it installs the AnyConnect VPN profile and the other profile settings to the client application.

MDM

You can provision iOS devices using an Apple configuration profile that you create with third-party Mobile Device Management (MDM) software. Apple configuration profiles are XML files that contain information such as device security policies, VPN configuration information, and Wi-Fi, mail, and calendar settings.

The high-level procedure is as follows:

1. Use MDM to create the Apple configuration profiles.

   For information on using MDM, see the Apple documentation.

2. Push the Apple configuration profiles to the registered devices.

To provision application profiles for Cisco Jabber for Android, use the profile editor on the ASA Device Manager (ASDM) to define the VPN profile for the Cisco AnyConnect Secure Mobility Client. The VPN profile is automatically downloaded to the Cisco AnyConnect Secure Mobility Client after the client establishes the VPN connection for the first time. You can use this method for all devices and OS types, and you can manage the VPN profile centrally on the ASA. For more information, see the *Creating and Editing an AnyConnect Profile* topic of the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for your release.

Automate VPN Connection

When users open Cisco Jabber from outside the corporate Wi-Fi network, Cisco Jabber needs a VPN connection to access the Cisco UC application servers. You can set up the system to allow Cisco AnyConnect Secure Mobility Client to automatically establish a VPN connection in the background, which helps ensure a seamless user experience.

Note VPN will not be launched because Expressway for Mobile and Remote Access has the higher connection priority even if VPN is set to automatic connection.

Set Up Trusted Network Connection

The Trusted Network Detection feature enhances the user experience by automating the VPN connection based on the user's location. When the user is inside the corporate Wi-Fi network, Cisco Jabber can reach the Cisco UC infrastructure directly. When the user leaves the corporate Wi-Fi network, Cisco Jabber automatically detects that it is outside the trusted network. After this occurs, Cisco AnyConnect Secure Mobility Client initiates the VPN to ensure connectivity to the UC infrastructure.

Note The Trusted Network Detection feature works with both certificate- and password-based authentication. However, certificate-based authentication provides the most seamless user experience.

Procedure

Step 1 Using ASDM, open the Cisco AnyConnect client profile.

Step 2 Enter the list of Trusted DNS Servers and Trusted DNS Domain Suffixes that an interface can receive when the client is within a corporate Wi-Fi network. The Cisco AnyConnect client compares the current interface DNS servers and domain suffix with the settings in this profile.

Note You must specify all your DNS servers to ensure that the Trusted Network Detection feature works properly. If you set up both the TrustedDNSDomains and TrustedDNSServers, sessions must match both settings to be defined as a trusted network.

For detailed steps for setting up Trusted Network Detection, see the *Trusted Network Detection* section in the *Configuring AnyConnect Features* chapter (Release 2.5) or *Configuring VPN Access* (releases 3.0 or 3.1) of the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for your release.

Set Up Connect On-Demand VPN

The Apple iOS Connect On Demand feature enhances the user experience by automating the VPN connection based on the user's domain.

When the user is inside the corporate Wi-Fi network, Cisco Jabber can reach the Cisco UC infrastructure directly. When the user leaves the corporate Wi-Fi network, Cisco AnyConnect automatically detects if it is connected to a domain that you specify in the AnyConnect client profile. If so, the application initiates the VPN to ensure connectivity to the UC infrastructure. All applications on the device including Cisco Jabber can take advantage of this feature.

Note Connect On Demand supports only certificate-authenticated connections.

The following options are available with this feature:

- **Always Connect** — Apple iOS always attempts to initiate a VPN connection for domains in this list.
- **Connect If Needed** — Apple iOS attempts to initiate a VPN connection to the domains in the list only if it cannot resolve the address using DNS.
- **Never Connect** — Apple iOS never attempts to initiate a VPN connection to domains in this list.

Attention Apple plans to remove the Always Connect option in the near future. After the Always Connect option is removed, users can select the Connect If Needed option. In some cases, Cisco Jabber users may have issues when using the Connect If Needed option. For example, if the hostname for the Cisco Unified Communications Manager is resolvable outside the corporate network, iOS will not trigger a VPN connection. The user can work around this issue by manually launching Cisco AnyConnect Secure Mobility Client before making a call.

Procedure

Step 1 Use the ASDM profile editor, iPCU, or MDM software to open the AnyConnect client profile.

Step 2 In the AnyConnect client profile, under the Connect if Needed section, enter your list of on-demand domains.

The domain list can include wild-card options (for example, cucm.cisco.com, cisco.com, and *.webex.com).

Set Up Automatic VPN Access on Cisco Unified Communications Manager

Before you begin

- The mobile device must be set up for on-demand access to VPN with certificate-based authentication. For assistance with setting up VPN access, contact the providers of your VPN client and head end.
- For requirements for Cisco AnyConnect Secure Mobility Client and Cisco Adaptive Security Appliance, see the *Software Requirements* topic.
- For information about setting up Cisco AnyConnect, see the *Cisco AnyConnect VPN Client Maintain and Operate Guides*.

Procedure

Step 1 Identify a URL that will cause the client to launch VPN on Demand.

a) Use one of the following methods to identify a URL that will cause the client to launch VPN on Demand.

- Connect if Needed
    - Configure Cisco Unified Communications Manager to be accessed through a domain name (not an IP address) and ensure that this domain name is not resolvable outside the firewall.
    - Include this domain in the “Connect If Needed” list in the Connect On Demand Domain List of the Cisco AnyConnect client connection.
- Always Connect
    - Set the parameter in step 4 to a nonexistent domain. A nonexistent domain causes a DNS query to fail when the user is inside or outside the firewall.

- Include this domain to the “Always Connect” list in the Connect On Demand Domain List of the Cisco AnyConnect client connection.

  The URL must include only the domain name. Do not include a protocol or a path (for example, use “cm8ondemand.company.com” instead of “https://cm8ondemand.company.com/vpn”.

b) Enter the URL in Cisco AnyConnect and verify that a DNS query on this domain fails.

Step 2 Open the **Cisco Unified CM Administration** interface.

Step 3 Navigate to the device page for the user.

Step 4 In the **Product Specific Configuration Layout** section, in the **On-Demand VPN URL** field, enter the URL that you identified and used in Cisco AnyConnect in Step 1.

The URL must be a domain name only, without a protocol or path.

Step 5 Select **Save**.

When Cisco Jabber opens, it initiates a DNS query to the URL (for example, ccm-sjc-111.cisco.com). If this URL matches the On-Demand domain list entry that you defined in this procedure (for example, cisco.com), Cisco Jabber indirectly initiates the AnyConnect VPN connection.

What to do next

- Test this feature.
  - Enter this URL into the Internet browser on the iOS device and verify that VPN launches automatically. You should see a VPN icon in the status bar.
  - Verify that the iOS device can connect to the corporate network using VPN. For example, access a web page on your corporate intranet. If the iOS device cannot connect, contact the provider of your VPN technology.
  - Verify with your IT department that your VPN does not restrict access to certain types of traffic (for example, if the administrator set the system to allow only email and calendar traffic).
- Verify that you set up the client to connect directly to the corporate network.

Set Up Certificate-Based Authentication

Cisco recommends that you use certificate-based authentication for negotiating a secure connection to Cisco Adaptive Security Appliance from Cisco AnyConnect Secure Mobility Client.

ASA supports certificates issued by standard Certificate Authority (CA) servers such as Cisco IOS CA, Microsoft Windows 2003, Windows 2008R2, Entrust, VeriSign, and RSA Keon. This topic gives you a, high-level procedure for setting up ASA for certificate-based authentication. See the *Configuring Digital Certificates* topic in the appropriate ASA configuration guide for step-by-step instructions.

Procedure

Step 1 Import a root certificate from the CA to the ASA.

Step 2 Generate an identity certificate for the ASA.

Step 3 Use the ASA identity certificate for SSL authentication.

Step 4 Configure a Certificate Revocation List (CRL) or an Online Certificate Status Protocol (OCSP).

Step 5 Configure the ASA to request client certificates for authentication.

What to do next

After you set up certificate-based authentication on ASA, you must distribute certificates to your users. You can use one of the following methods:

- *Distribute Certificates with SCEP*
- *Distribute Client Certificate with Mobileconfig File*

Distribute Certificates with SCEP

You can use Simple Certificate Enrollment Protocol (SCEP) on Microsoft Windows Server to securely issue and renew certificates for client authentication.

To distribute certificates with SCEP, you must install the SCEP module on Microsoft Windows Server. See the following topics for more information:

- *ASA 8.X: AnyConnect SCEP Enrollment Configuration Example*
- *Simple Certificate Enrollment Protocol (SCEP) Add-on for Certificate Services*

Distribute Client Certificate with Mobileconfig File

Use this procedure to create a mobile configuration file that includes a certificate. You can use this file to distribute the certificate to users.

Procedure

Step 1 Use the iPCU software to create a `mobileconfig` file and include the certificate (`.pfx`) file.

Step 2 Forward the `mobileconfig` file to the user.

Step 3 Use the Cisco ISE native supplicant provisioning process to distribute user certificates.

Step 4 Use the Enterprise MDM software to provision and publish certificates to registered devices.

Session Parameters

You can configure ASA session parameters to improve performance for secure connections. For the best user experience, you should configure the following ASA session parameters:

- Datagram Transport Layer Security (DTLS) — DTLS is an SSL protocol that provides a data path that prevents latency and data loss.
- Auto Reconnect — Auto reconnect, or session persistence, lets Cisco AnyConnect Secure Mobility Client recover from session disruptions and re-establish sessions.

- Session Persistence — This parameter allows the VPN session to recover from service disruptions and re-establish the connection.
- Idle Timeout — Idle timeout defines a period of time after which ASA terminates secure connections, if no communication activity occurs.
- Dead-Peer Detection (DTD) — DTD ensures that ASA and Cisco AnyConnect Secure Mobility Client can quickly detect failed connections.

Set ASA Session Parameters

Cisco recommends that you set up the ASA session parameters as follows to optimize the end user experience for Cisco AnyConnect Secure Mobility Client.

Procedure

Step 1 Set up Cisco AnyConnect to use DTLS.

For more information, see the *Enabling Datagram Transport Layer Security (DTLS) with AnyConnect (SSL) Connections* topic in the *Configuring AnyConnect Features Using ASDM* chapter of the *Cisco AnyConnect VPN Client Administrator Guide, Version 2.0*.

Step 2 Set up session persistence (auto-reconnect).

a) Use ASDM to open the VPN client profile.
b) Set the **Auto Reconnect Behavior** parameter to **Reconnect After Resume**.

For more information, see the *Configuring Auto Reconnect* topic in the *Configuring AnyConnect Features* chapter (Release 2.5) or *Configuring VPN Access* chapter (releases 3.0 or 3.1) of the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for your release.

Step 3 Set the idle timeout value.

a) Create a group policy that is specific to Cisco Jabber clients.
b) Set the idle timeout value to 30 minutes.

For more information, see the *vpn-idle-timeout* section of the *Cisco ASA 5580 Adaptive Security Appliance Command Reference* for your release

Step 4 Set up Dead Peer Detection (DPD).

a) Disable server-side DPD.
b) Enable client-side DPD.

For more information, see the *Enabling and Adjusting Dead Peer Detection* topic of the *Configuring VPN* chapter of the *Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6*.

Group Policies and Profiles

You should use the ASA Device Manager (ASDM) to create group policies, client profiles, and connection profiles. Create your group policies first and then apply those policies to the profiles. Using the ASDM to create profiles ensures that Cisco AnyConnect Secure Mobility Client downloads the profiles after it establishes a connection to ASA for the first time. The ASDM also lets you manage and maintain your policies and profiles in a central location.

See the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for instructions on creating policies and profiles with the ASDM.

Trusted Network Detection

Trusted Network Detection is a feature that automates secure connections based on user location. When users leave the corporate network, Cisco AnyConnect Secure Mobility Client automatically detects that it is outside the trusted network and then initiates secure access.

You configure Trusted Network Detection on ASA as part of the client profile. For more information, see the *Trusted Network Detection* topic in the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for your release.

Tunnel Policies

Tunnel policies configure how Cisco AnyConnect Secure Mobility Client directs traffic over a secure connection and include the following:

- Full Tunnel Policy — Lets you send all traffic over the secure connection to the ASA gateway.
- Split Include Policy with Network ACL — Enables you to restrict secure connections based on destination IP addresses. For example, in an on-premises deployment, you can specify the IP addresses for Cisco Unified Communications Manager, Cisco Unified Presence, your TFTP server, and other servers to restrict the secure connection only to your client's traffic.
- Split Exclude Policy — Allows you to exclude certain traffic from the secure connection. You can allow client traffic over the secure connection and then exclude traffic from specific destination subnets.

Deployment with Single Sign-On

You can enable your services with Security Assertion Markup Language (SAML) single sign-on (SSO). SAML SSO can be used in on-premises, cloud, or hybrid deployments.

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

1. The user starts the Cisco Jabber client. If you configure your Identity Provider (IdP) to prompt your users to sign in using a web form, the form is displayed within the client.
2. The Cisco Jabber client sends an authorization request to the service that it is connecting to, such as Cisco Webex Messenger service, 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 contains username and password fields.
    - Kerberos for Integrated Windows Authentication (IWA) (Windows only)
    - Smart card authentication (Windows only)
    - Basic HTTP authentication method in which client offers the username and password when making an 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 log in to the service.

Authentication Methods

The authentication mechanism impacts how a user signs on. For example, if you use Kerberos, the client does not prompt users for credentials, because your users already provided authentication to gain access to the desktop.

User Sessions

Users sign in for a *session*, which gives them a predefined period to use Cisco Jabber services. To control how long sessions last, you configure cookie and token timeout parameters.

Configure the IdP timeout parameters with an appropriate amount of time to ensure that users are not prompted to log in. For example, when Jabber users switch to an external Wi-Fi, are roaming, their laptops hibernate, or their laptop goes to sleep due to user inactivity. Users will not have to log in after resuming the connection, provided the IdP session is still active.

When a session has expired and Jabber is not able to silently renew it, because user input is required, the user is prompted to reauthenticate. This can occur when the authorization cookie is no longer valid.

If Kerberos or a Smart card is used, no action is needed to reauthenticate, unless a PIN is required for the Smart card; there is no risk of interruption to services, such as voicemail, incoming calls, or instant messaging.

Enable SAML SSO in the Client

Before you begin

- If you do not use Cisco Webex Messenger, 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*.

- If you use Cisco Webex Messenger, enable SSO on Cisco Webex Messenger Services to support Cisco Unified Communications Applications and Cisco Unity Connection—For more information about enabling SAML SSO on this service, read about *Single Sign-On* in the *Cisco Webex Messenger Administrator's Guide*.

  For more information about enabling SAML SSO on this service, read about `Single Sign-On` in the *Cisco Webex Messenger Administrator's Guide*.

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 *Configure Service Discovery for Remote Access*.

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 Jabber 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 Jabber username and password. To disable SSO for a Cisco Jabber user, set the value of the SSO_Enabled parameter to FALSE.

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

Related Topics

SAML SSO Deployment Guide for Cisco Unified Communications Applications, Release 10.5
Managing SAML SSO in Cisco Unity Connection
Cisco WebEx Messenger Services Single Sign-On
Certificate Validation

CHAPTER 4

Configuration and Installation Workflows

Server Configuration Workflows for Cloud-Based Deployments

Cloud-Based Deployment Using CUCM 9.x and Later

Procedure

	Command or Action	Purpose
Step 1	Configure IM and Presence Service for Cloud-Based Deployments, on page 145.	
Step 2	Configure Voice and Video Communication for On-Premises Deployments, on page 150.	
Step 3	Configure Voicemail for an On-Premises Deployment with Cisco Unified Communications Manager Release 9.x and Later, on page 238.	
Step 4	Configure Conferencing for Cloud-Based Deployments, on page 264.	
Step 5	Configure the Clients, on page 317..	
Step 6	Certificate Requirements for Cloud-Based Servers, on page 312.	Ensure these certificates are on your server.
Step 7	Configure Service Discovery.	
Step 8	Install the Clients, on page 383.	

Cloud-Based Deployment Using CUCM 8.x

Procedure

	Command or Action	Purpose
Step 1	Configure IM and Presence Service for Cloud-Based Deployments, on page 145.	
Step 2	Configure Voice and Video Communication for On-Premises Deployments, on page 150.	
Step 3	Configure Voicemail for an On-Premises Deployment with Cisco Unified Communications Manager Release 8.6, on page 247.	
Step 4	Configure Conferencing for Cloud-Based Deployments, on page 264.	
Step 5	Configure the Clients, on page 317.	
Step 6	Certificate Requirements for Cloud-Based Servers, on page 312.	Ensure these certificates are on your server.
Step 7	Configure Service Discovery.	
Step 8	Install the Clients, on page 383.	

Server Configuration Workflows for On-Premises Deployments

Deployment and Installation Workflow for an On-Premises Deployment with CUCM 9.x and Later

Procedure

	Command or Action	Purpose
Step 1	Configure IM and Presence Service for On-Premises Deployments with Cisco Unified Communications Manager 9.x and Later, on page 130.	
Step 2	Configure Voice and Video Communication for Cloud-Based Deployments, on page 149.	Configure via WebEx.
Step 3	Configure Voicemail for Cloud-Based Deployments, on page 237.	Configure via WebEx.
Step 4	Configure conferencing.	

	Command or Action	Purpose
	• To configure onsite, Configure On-Premises Conferencing using WebEx Meetings Server, on page 255. • To configure offsite, Configure Cloud-Based Conferencing Using WebEx Meeting Center, on page 259.	
Step 5	Configure the Clients, on page 317.	
Step 6	Get Certificates Signed by Certificate Authority, on page 308.	If there is a delay after you request CSRs, you may wish to request them before configuring services, and then apply the certificates prior to installing the client.
Step 7	Configure Service Discovery.	
Step 8	Install the Clients, on page 383.	

Deployment and Installation Workflow for an On-Premises Deployment with CUCM 8.6 and CUP

Procedure

	Command or Action	Purpose
Step 1	Configure IM and Presence Service for On-Premises Deployments with Cisco Unified Communications Manager 8.x and Cisco Unified Presence, on page 131.	
Step 2	Configure Voice and Video Communication for Cloud-Based Deployments, on page 149.	Configure via WebEx.
Step 3	Configure Voicemail for Cloud-Based Deployments, on page 237	Configure via WebEx.
Step 4	Configure conferencing. • To configure onsite conferencing, Configure On-Premises Conferencing using WebEx Meetings Server, on page 255. • To configure offsite conferencing, Configure Cloud-Based Conferencing Using WebEx Meeting Center, on page 259.	
Step 5	Configure the Clients, on page 317.	
Step 6	Get Certificates Signed by Certificate Authority, on page 308.	If there is a delay after you request CSRs, you may wish to request them before configuring

	Command or Action	Purpose
		services, and then apply the certificates prior to installing the client.
Step 7	Configure Service Discovery.	
Step 8	Install the Clients, on page 383.	

Deployment and Installation Workflow for Phone Only Mode with CUCM 9.x and Later

Procedure

	Command or Action	Purpose
Step 1	Set Up Directory Synchronization and Authentication, on page 360.	Configure synchronization and authentication with your corporate directory server.
Step 2	Configure Voice and Video Communication, on page 149.	Configure voice and video communication for your deployment.
Step 3	Configure Voicemail, on page 237.	Configure voicemail for your deployment.
Step 4	Configure Conferencing, on page 255.	Configure conferencing for your deployment.
Step 5	Configure the Clients, on page 317.	User experience and client features are controlled using a configuration file. Creation of a configuration file is integral part of application deployment.
Step 6	Install the Clients, on page 383.	Additional client customization can be performed during the installation of Cisco Jabber for Windows and Cisco Jabber for Mac.

Server Configuration Workflows for User-Based Configuration

This section describes how to configure an on-premises deployment of Cisco Jabber using Cisco Unified Communications Manager 9.x and later based on the central action of user creation. This section is divided into three parts:

- Pre-user creation tasks
- User creation tasks
- Post-user creation tasks

Pre-User Creation Workflow

Before you begin

This workflow assumes you have already successfully installed and deployed Cisco Unified Communications Manager, Cisco Unity Connection, and any other supporting services. It is beyond the scope of this document to describe the installation and configuration of these services. Refer to the appropriate documentation suites for information on these tasks before continuing.

Procedure

	Command or Action	Purpose
Step 1	Planning Considerations, on page 5.	Plan your deployment by considering what types of technologies you'll need to use to service your users.
Step 2	Hardware Requirements, on page 38.	Plan your deployment by considering if your current hardware meets Cisco Jabber requirements.
Step 3	Software Requirements, on page 44.	Plan your deployment by considering if you current software meets Cisco Jabber requirements.
Step 4	Contact Sources, on page 63.	Plan your deployment by considering which contact source type you'll use with Cisco Jabber.

User Creation Workflow

Before you begin

This section covers individual tasks pertaining to user and device creation. See the *Cisco Unified Communications Manager Bulk Administration Guide* for your release of Cisco Unified Communications Manager for information about the bulk creation of users and device assignment.

Procedure

	Command or Action	Purpose
Step 1	Set Up Directory Synchronization and Authentication, on page 360.	Configure synchronization and authentication with your corporate directory server.
Step 2	Configure IM and Presence Service, on page 129.	Configure IM and Presence Service for your deployment.
Step 3	Configure Voice and Video Communication, on page 149.	Configure voice and video communication for your deployment.
Step 4	Configure Voicemail, on page 237.	Configure voicemail for your deployment.
Step 5	Configure Conferencing, on page 255.	Configure conferencing for your deployment.

Post-User Creation Workflow

Before you begin

This section covers tasks that are performed after users and devices have been provisioned.

Procedure

	Command or Action	Purpose
Step 1	Configure the Clients, on page 317.	User experience and client features are controlled using a configuration file. Creation of a configuration file is integral part of application deployment.
Step 2	Install the Clients, on page 383.	Additional client customization can be performed during the installation of Cisco Jabber for Windows and Cisco Jabber for Mac.

PART II

Infrastructure Configuration

CHAPTER 5

Configure IM and Presence Service

Configure IM and Presence Service for an On-Premises Deployment

Configure IM and Presence Service for On-Premises Deployments with Cisco Unified Communications Manager 10.5 and Later

Procedure

	Command or Action	Purpose
Step 1	Activate and Start Essential Services, on page 131	
Step 2	Create a Service Profile, on page 132	
Step 3	Prepopulate Contact Lists in Bulk, on page 132	
Step 4	Enable Message Settings, on page 133	
Step 5	Enable File Transfer, on page 135	
Step 6	Prompts for Presence Subscription Requests, on page 135	
Step 7	Temporary Presence, on page 136	
Step 8	Configure Presence in Microsoft SharePoint 2010 and 2013, on page 139	
Step 9	Configure Users with IM and Presence Service, on page 139	

	Command or Action	Purpose
Step 10	Enable Presence for Calendar Events, on page 141	
Step 11	Configure Persistent Chat, on page 141	

Configure IM and Presence Service for On-Premises Deployments with Cisco Unified Communications Manager 9.x and Later

Procedure

	Command or Action	Purpose
Step 1	Activate and Start Essential Services, on page 131	
Step 2	Create a Service Profile, on page 132	
Step 3	Prepopulate Contact Lists in Bulk, on page 132	
Step 4	Enable Message Settings, on page 133	
Step 5	Enable File Transfers and Screen Captures, on page 134	
Step 6	Prompts for Presence Subscription Requests, on page 135	
Step 7	Temporary Presence, on page 136	
Step 8	Add an IM and Presence Service, on page 137	
Step 9	Apply an IM and Presence Service, on page 138	
Step 10	Configure Presence in Microsoft SharePoint 2010 and 2013, on page 139	
Step 11	Configure Users with IM and Presence Service, on page 139	
Step 12	Enable Presence for Calendar Events, on page 141	
Step 13	Configure Persistent Chat, on page 141	

Configure IM and Presence Service for On-Premises Deployments with Cisco Unified Communications Manager 8.x and Cisco Unified Presence

Procedure

	Command or Action	Purpose
Step 1	Activate and Start Essential Services, on page 131	
Step 2	Prepopulate Contact Lists in Bulk, on page 132	
Step 3	Enable Message Settings, on page 133	
Step 4	Specify Capabilities Assignments, on page 133	
Step 5	Prompts for Presence Subscription Requests, on page 135	
Step 6	Configure Presence in Microsoft SharePoint 2010 and 2013, on page 139	
Step 7	Temporary Presence, on page 136	
Step 8	Enable Presence for Calendar Events, on page 141	

Activate and Start Essential Services

Essential services enable communication between servers and provide capabilities to the client.

Procedure

Step 1 Open the **Cisco Unified IM and Presence Serviceability** interface.

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

Step 3 Select the appropriate server from the **Server** drop-down list.

Step 4 Ensure the following services are started and activated:

- **Cisco SIP Proxy**
- **Cisco Sync Agent**
- **Cisco XCP Authentication Service**
- **Cisco XCP Connection Manager**
- **Cisco XCP Text Conference Manager**
- **Cisco Presence Engine**

Step 5 Select **Tools** > **Control Center - Network Services**.

Step 6 Select the appropriate server from the **Server** drop-down list.

Step 7 Ensure **Cisco XCP Router Service** is running.

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 users. The client can then retrieve settings for available services from the service profile.

Before you begin

Activate and Start Essential Services, on page 131

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) Select **Make this the default service profile for the system**, if appropriate.

Note For phone mode, in the **IM and Presence Profile** section ensure that the **Primary** field has **<None>** selected.

Step 5 Select **Save**.

Prepopulate Contact Lists in Bulk

You can pre-populate user contact lists with the Bulk Administration Tool (BAT).

In this way you can prepopulate contact lists for users so that they automatically have a set of contacts after the initial launch of the client.

Cisco Jabber supports up to 300 contacts in a client contact list.

Procedure

	Command or Action	Purpose
Step 1	Create a CSV file that defines the contact list you want to provide to users.	
Step 2	Use the BAT to import the contact list in bulk to a set of users.	For more information about using BAT and the format of the CSV file, see the *Deployment Guide for Cisco Unified Communications Manager IM & Presence* for your release.

Enable Message Settings

Enable and configure instant messaging capabilities.

Before you begin

Prepopulate Contact Lists in Bulk, on page 132.

Procedure

Step 1 Open the **Cisco Unified CM IM and Presence Administration** interface.

Step 2 Select **Messaging** > **Settings**.

Step 3 Select the following options:

- **Enable instant messaging**
- **Allow clients to log instant message history**
- **Allow cut & paste in instant messages**

Step 4 Select other messaging settings as appropriate.

Step 5 Select **Save**.

Important Cisco Jabber does not support the following settings on the **Presence Settings** window on Cisco Unified Communications Manager IM and Presence Service release 9.0.x:

- **Use DND status when user is on the phone**
- **Use DND status when user is in a meeting**

What to do next

- If you have Cisco Unified Communications Manager IM and Presence Service release 9.x and later, Add an IM and Presence Service, on page 137.
- If you have Cisco Unified Presence Release 8.6, Specify Capabilities Assignments, on page 133.

Specify Capabilities Assignments

Complete the steps in this task to provide users with instant messaging and presence capabilities when using Cisco Unified Presence.

Before you begin

Enable Message Settings, on page 133

Procedure

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

Step 2 Select **System** > **Licensing** > **Capabilities Assignment**.

The **Find and List Capabilities Assignments** window opens.

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

Step 4 Select the appropriate users from the list.

The **Capabilities Assignment Configuration** window opens.

Step 5 Select both of the following in the **Capabilities Assignment Configuration** section:

- **Enable CUP**
- **Enable CUPC**

Step 6 Select **Save**.

Enable File Transfers and Screen Captures

This applies to Cisco Unified Communication Manager IM and Presence Service 9.x, 10.0.x, and 10.5.1. You can enable or disable file transfers and screen captures using the Cisco XCP Router service on Cisco Unified Communications Manager IM and Presence Service. File transfers and screen captures parameter is enabled by default.

File transfers and screen captures are supported for both desktop and mobile clients.

Procedure

Step 1 Open the **Cisco Unified CM IM and Presence Administration** interface.

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

Step 3 Select the appropriate server from the **Server** drop-down list.

Step 4 Select **Cisco XCP Router** from the **Service** drop-down list.

The **Service Parameter Configuration** window opens.

Step 5 Locate the **Enable file transfer** parameter.

Step 6 Select the appropriate value from the **Parameter Value** drop-down list.

Remember If you disable the setting on Cisco Unified Communications Manager IM and Presence Service, you must also disable file transfers and screen captures in the client configuration.

Step 7 Select **Save**.

Enable File Transfer

Cisco Jabber 10.5 supports peer-to-peer file transfer and transfering screen captures on Cisco Unified Communications Manager IM and Presence Service release 10.5(2) or later.

Procedure

Step 1 Open the **Cisco Unified CM IM and Presence Administration** interface.

Step 2 Select **Messaging** > **File Transfer**.

Step 3 In the **File Transfer Configuration** section, select **Peer-to-Peer**.

Step 4 Select **Save**.

Prompts for Presence Subscription Requests

Applies to: All clients

You can enable or disable prompts for presence subscription requests from contacts within your organization. The client always prompts users for presence subscription requests from contacts outside your organization.

Users specify privacy settings in the client as follows:

Inside Your Organization

Users can choose to allow or block contacts from inside your organization.

- If users choose to allow presence subscription requests and
  - you select **Allow users to view the availability of other users without being prompted for approval**, the client automatically accepts all presence subscription requests without prompting users.
  - you do not select **Allow users to view the availability of other users without being prompted for approval**, the client prompts users for all presence subscription requests.
- If users choose to block contacts, only their existing contacts can see their availability status. In other words, only those contacts who have already subscribed to the user's presence can see their availability status.

Note When searching for contacts in your organization, users can see the temporary availability status of all users in the organization. However, if User A blocks User B, User B cannot see the temporary availability status of User A in the search list.

Outside Your Organization

Users can choose the following options for contacts from outside your organization:

- Have the client prompt them for each presence subscription request.

- Block all contacts so that only their existing contacts can see their availability status. In other words, only those contacts who have already subscribed to the user's presence can see their availability status.

Before you begin

This feature is supported for on-premises deployments and is only available on Cisco Unified Communications Manager, release 8.x or later.

Procedure

Step 1 Open the **Cisco Unified CM IM and Presence Administration** interface.

Step 2 Select **Presence** > **Settings**.

The **Presence Settings** window opens.

Step 3 Select **Allow users to view the availability of other users without being prompted for approval** to disable prompts and automatically accept all presence subscription requests within your organization.

This option has the following values:

- Selected—The client does not prompt users for presence subscription requests. The client automatically accepts all presence subscription requests without prompting the users.
- Cleared—The client prompts users to allow presence subscription requests. This setting requires users to allow other users in your organization to view their availability status.

Step 4 Select **Save**.

Temporary Presence

Applies to: All clients

Disable temporary presence to increase privacy control. When you configure this parameter, Cisco Jabber displays availability status only to contacts in a user's contact list.

Before you begin

This feature is supported for on-premises deployment and requires Cisco Unified Communications Manager, release 9.x or later.

Procedure

Step 1 Open the **Cisco Unified CM IM and Presence Administration** interface.

Step 2 Select **Presence** > **Settings** > **Standard Configuration**.

Step 3 Uncheck **Enable ad-hoc presence subscriptions** and then select **Save**.

Cisco Jabber does not display temporary presence. Users can see availability status only for contacts in their contact list.

Disable Temporary Presence in Cisco Unified Presence

Disable temporary presence to increase privacy control. When you configure this parameter, Cisco Jabber displays availability status only to contacts in a user's contact list.

Before you begin

This feature is supported for on-premises deployment and requires Cisco Unified Communications Manager, release 8.x or later.

Procedure

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

Step 2 Select **Presence** > **Settings**.

Step 3 Uncheck **Enable ad-hoc presence subscriptions** and then select **Save**.

Cisco Jabber does not display temporary presence. Users can see availability status only for contacts in their contact list.

Add an IM and Presence Service

Provide users with IM and Presence Service capabilities.

Procedure

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

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

The **Find and List UC Services** window opens.

Step 3 Select **Add New**.

The **UC Service Configuration** window opens.

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

Step 5 Select **Next**.

Step 6 Provide details for the IM and Presence Service as follows:

a) Select **Unified CM (IM and Presence)** from the **Product Type** drop-down list.

b) Specify a name for the service in the **Name** field.

The name you specify displays when you add the service to a profile. Ensure the name you specify is unique, meaningful, and easy to identify.

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

d) Specify the instant messaging and presence service address in the **Host Name/IP Address** field.

Important The service address must be a fully qualified domain name or IP address.

Step 7 Select **Save**.

Apply an IM and Presence Service

After you add an IM and Presence 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

Add an IM and Presence Service, on page 137

Procedure

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

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

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

Step 3 Find and select your service profile.

The **Service Profile Configuration** window opens.

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

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

Step 5 Click **Save**.

Step 6 Add users to the service profile.

a) Select **User Management** > **End User**.

The **Find and List Users** dialog box opens.

b) Specify the appropriate filters in the **Find User where** field and then select **Find** to find a user.

c) Click the user in the list.

The **End User Configuration** window appears.

d) Under the **Service Settings** area, check the **Home Cluster** check box.

e) Check the **Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)** check box.

f) Select your service profile from the **UC Service Profile** drop-down list.

Step 7 Click **Save**.

Configure Presence in Microsoft SharePoint 2010 and 2013

If your organization defines users' profiles where their IM address is different from their email address, then additional configuration is required to enable presence integration between the client and Microsoft SharePoint 2010 and 2013.

Before you begin

- For Cisco Jabber for Windows clients only.
- Ensure that all sites are in sync with Microsoft SharePoint Central Administration (CA).
- Ensure that synchronization between Microsoft SharePoint and Active Directory is set up.

Procedure

Step 1 If you have Microsoft SharePoint 2013, update the SharePoint CA profile pages for users with the following information:

a) For the **SIP Address** profile field, leave it blank.
b) In the **Work email** profile field, enter the user profile. For example, `john4mail@example.pst`.

Step 2 If you have Microsoft SharePoint 2010, update the SharePoint CA profile pages for users with the following information:

a) For the **SIP Address** profile field, enter the user profile. For example, `john4mail@example.pst`
b) In the **Work email** profile field, leave it blank.

Configure Users with IM and Presence Service

You can enable users for IM and Presence.

Configure Users Individually

Enable instant messaging and presence service and add your service profile to individual users.

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 username from the list.

The **End User Configuration** window opens.

Step 5 Locate the **Service Settings** section and do the following:

a) Select **Home Cluster**.

b) Select **Enable User for Unified CM IM and Presence**.

c) Select your service profile from the **UC Service Profile** drop-down list.

Important Cisco Unified Communications Manager release 9.x only—If the user has only instant messaging and presence capabilities (IM only), select **Use Default**. Cisco Unified Communications Manager release version 9.x applies the default service profile regardless of what you select from the **UC Service Profile** drop-down list.

Step 6 Select **Save**.

Configure Users in Bulk

Enable instant messaging and presence and add your service profile to multiple users.

Procedure

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

Step 2 Select **Bulk Administration** > **Users** > **Update Users** > **Query**.

The **Find and List Users To Update** 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 **Next**.

The **Update Users Configuration** window opens.

Step 5 Select both of the **Enable User for Unified CM IM and Presence** check boxes.

Important There are two check boxes for **Enable User for Unified CM IM and Presence**. To disable instant messaging and presence, you select one check box. To enable instant messaging and presence, you select both check boxes.

Step 6 Select the **UC Service Profile** check box and then select your service profile from the drop-down list.

Important Cisco Unified Communications Manager release 9.x only — If the user has only instant messaging and presence capabilities (IM only), you must select **Use Default**.

For IM only users — Cisco Unified Communications Manager release 9.x always applies the default service profile regardless of what you select from the **UC Service Profile** drop-down list.

Step 7 In the **Job Information** section, specify if you want to run the job immediately or at a later time.

Step 8 Select **Submit**.

Enable Presence for Calendar Events

To enable presence status for calendar events, users must individually enable a preference in the **Cisco Unified CM IM and Presence User Options** page.

Important

- This feature is not available for the Cisco Jabber mobile clients.
- This preference is disabled by default.
- As of this release, users must enable the preference individually after deployment. You cannot enable this preference for multiple users with a bulk task.

Procedure

Step 1 Log in to the **Cisco Unified CM IM and Presence User Options** page.

The user options page is located at: `https://`*`server_name`*`:`*`port_number`*`/cupuser/showHome.do`

Step 2 Select **User Options** > **Preferences**.
The **Preferences** page opens.

Step 3 Navigate to the **Calendar Settings** section of the **Preferences** page.

Step 4 Select **On** from the drop-down menu for the **Include Calendar information in my Presence Status** field.

Step 5 Select **Save**.

Step 6 Log out and close the **Cisco Unified CM IM and Presence User Options** page.

Calendar events change the user's availability status in the client. For example, when meetings occur in the calendar, the availability status is automatically set to **In a meeting**.

Configure Persistent Chat

Persistent chat must be enabled and configured on Cisco Unified Communications Manager IM and Presence Service before it can be used by the client.

Before you begin

For Cisco Jabber desktop clients Persistent chat is available on Cisco Unified Communications Manager IM and Presence Service 10.0 and later.

Refer to *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* for your release for information on the database configuration necessary to support the persistent chat feature. Database configuration must be performed before continuing with this task.

Local chat message archiving must be enabled for persistent chat. Local chat message archiving is enabled on Cisco Unified Communications Manager IM and Presence Service using the **Allow clients to log instant message history** setting, for more information, see the *Enable Message Settings* topic from the *On-Premises Deployment Guide*.

Procedure

Step 1 Open the **Cisco Unified CM IM and Presence Administration** interface.

Step 2 Select **Messaging** > **Group Chat and Persistent Chat**.

Step 3 Select **Enable Persistent Chat**.

Step 4 Ensure the settings **How many users can be in a room at one time** and **How many hidden users can be in a room at one time** under the **Occupancy Settings** section contain the same, non-zero value.

Step 5 Configure the remaining settings as appropriate for your persistent chat deployment. We recommend the persistent chat settings in the following table.

Persistent Chat Setting	Recommended Value	Notes
System automatically manages primary group chat server aliases	Disabled	
Enable persistent chat	Enabled	
Archive all room joins and exits	Administrator Defined	This value is not currently used by for persistent chat.
Archive all room messages	Enabled	
Allow only group chat system administrators to create persistent chat rooms	Administrator Defined	Cisco recommends using the value Enabled unless Cisco Unified Personal Communicator is deployed in the enterprise environment.
Maximum number of persistent chat rooms allowed	Administrator Defined	
Number of connections to the database	Default Value	
Database connection heartbeat interval (seconds)	Default Value	
Timeout value for persistent chat rooms (minutes)	Default Value	
Maximum number of rooms allowed	Default Value	
Rooms are for members only by default	Disabled	
Room owners can change whether or not rooms are for members only	Enabled	Cisco Jabber requires this value to be Enabled.
Only moderators can invite people to members-only rooms	Enabled	Cisco Jabber requires this value to be Enabled.
Room owners can change whether or not only moderators can invite people to members-only rooms	Enabled	
Users can add themselves to rooms as members	Disabled	This value is not currently used by Cisco Jabber for persistent chat.

Persistent Chat Setting	Recommended Value	Notes
Room owners can change whether users can add themselves to rooms as members	Disabled	This value is not currently used by Cisco Jabber for persistent chat.
Members and administrators who are not in a room are still visible in the room	Enabled	Cisco Jabber requires this value to be Enabled.
Room owners can change whether members and administrators who are not in a room are still visible in the room	Enabled	
Rooms are backwards-compatible with older clients	Disabled	This value is not currently used by Cisco Jabber for persistent chat.
Room owners can change whether rooms are backwards-compatible with older clients	Disabled	This value is not currently used by Cisco Jabber for persistent chat.
Rooms are anonymous by default	Disabled	This value is not currently supported by Cisco Jabber for persistent chat. Cisco Jabber cannot join anonymous rooms.
Room owners can change whether or not rooms are anonymous	Disabled	This value is not currently supported by Cisco Jabber for persistent chat. Cisco Jabber cannot join anonymous rooms.
Lowest participation level a user can have to invite others to the room	Default Value	This value is not currently used by Cisco Jabber for persistent chat.
Room owners can change the lowest participation level a user can have to invite others to the room	Disabled	This value is not currently used by Cisco Jabber for persistent chat.
How many users can be in a room at one time	Administrator Defined	Cisco recommends using the default value.
How many hidden users can be in a room at one time	Administrator Defined	
Default maximum occupancy for a room	Default Value	
Room owners can change default maximum occupancy for a room	Default Value	
Lowest participation level a user can have to send a private message from within the room	Default Value	
Room owners can change the lowest participation level a user can have to send a private message from within the room	Default Value	

Persistent Chat Setting	Recommended Value	Notes
Lowest participation level a user can have to change a room's subject	Moderator	
Room owners can change the lowest participation level a user can have to change a room's subject	Disabled	
Remove all XHTML formatting from messages	Disabled	This value is not currently used by Cisco Jabber for persistent chat.
Room owners can change XHTML formatting setting	Disabled	This value is not currently used by Cisco Jabber for persistent chat.
Rooms are moderated by default	Disabled	This value is not currently used by Cisco Jabber for persistent chat.
Room owners can change whether rooms are moderated by default	Default Value	This value is not currently used by Cisco Jabber for persistent chat.
Maximum number of messages that can be retrieved from the archive	Default Value	
Number of messages in chat history displayed by default	Administrator Defined	Cisco recommends a value between 15 and 50. The **Number of messages in chat history displayed by default** setting does not apply retroactively to persistent chat rooms. Rooms created before the setting is changed will continue to use their originally configured value.
Room owners can change the number of messages displayed in chat history	Default Value	This value is not currently used by Cisco Jabber for persistent chat.

Note Persistent Chat rooms inherit their settings at the time of creation. Values changed after a room is created only apply to rooms created after the change has taken effect.

What to do next

Ensure you configure any client-specific parameters for persistent chat. For more information, see the Client parameters section of the latest *Parameters Reference Guide for Cisco Jabber*.

Enable file transfer in chat rooms. For more information, see *Enable File Transfer and Screen Captures for Group Chats and Chat Rooms*.

Related Topics

Client Parameters, on page 336

Configure IM and Presence Service for Cloud-Based Deployments

Procedure

	Command or Action	Purpose
Step 1	Configure IM and Presence Service, on page 145	
Step 2	Configure Presence in Microsoft SharePoint 2010 and 2013, on page 139	
Step 3	Configure Privacy Options, on page 146	

Configure IM and Presence Service

When users successfully authenticate to the Cisco WebEx Messenger service, they get IM and Presence Service capabilities. You can optionally configure IM and Presence Service federation with the Cisco WebEx Administration Tool.

Configure Presence in Microsoft SharePoint 2010 and 2013

If your organization defines users' profiles where their IM address is different from their email address, then additional configuration is required to enable presence integration between the client and Microsoft SharePoint 2010 and 2013.

Before you begin

- For Cisco Jabber for Windows clients only.
- Ensure that all sites are in sync with Microsoft SharePoint Central Administration (CA).
- Ensure that synchronization between Microsoft SharePoint and Active Directory is set up.

Procedure

Step 1 If you have Microsoft SharePoint 2013, update the SharePoint CA profile pages for users with the following information:

a) For the **SIP Address** profile field, leave it blank.
b) In the **Work email** profile field, enter the user profile. For example, `john4mail@example.pst`.

Step 2 If you have Microsoft SharePoint 2010, update the SharePoint CA profile pages for users with the following information:

a) For the **SIP Address** profile field, enter the user profile. For example, `john4mail@example.pst`

b) In the **Work email** profile field, leave it blank.

Configure Privacy Options

You can specify the default settings for presence subscription requests in cloud-based deployments.

Procedure

Step 1 Open the Cisco WebEx Administration Tool.

Step 2 Select the **Configuration** tab.

Step 3 Select **General IM** in the **Connect Client** section.
The **General IM** pane opens.

Step 4 Select the appropriate options for contact list requests as follows:

Option	Description
Select **Allow users to set "Options for contact list requests"**	**Accept requests automatically from contacts in my organization** automatically becomes the default option to configure how the client handles presence subscription requests. Users can change the default option in the **Options** window.
Do not select **Allow users to set "Options for contact list requests"**	You configure how the client handles presence subscription requests. Users cannot change this configuration. The settings are not available in the **Options** window. Select one of the following options: • **Accept requests automatically from all contacts** • **Accept requests automatically from contacts in my organization** • **Prompt me for each request**

The options for configuring how the client handles contact list requests are as follows:

- Accept requests automatically from all contacts — The client automatically accepts presence subscription requests from any domain. If you specify this setting, users from any domain can automatically add users to their contact list and view their availability status.
- Accept requests automatically from contacts in my organization — The client automatically accepts presence subscription requests only from users in the domains you specify. To specify a domain, select **Domain(s)** in the **System Settings** section on the **Configuration** tab.

  Note When searching for contacts in your organization, users can see the temporary availability status of all users in the organization. However, if User A blocks User B, User B cannot see the temporary availability status of User A in the search list.

- Prompt me for each request — The client prompts users to accept each presence subscription request.

Step 5 Select **Save**.

CHAPTER 6

Configure Voice and Video Communication

Configure Voice and Video Communication for Cloud-Based Deployments

Procedure

	Command or Action	Purpose
Step 1	Configure Audio and Video Services, on page 149	
Step 2	Add Teleconferencing Service Name Accounts, on page 149	

Configure Audio and Video Services

Integrate your on-premises Unified Communications environment with the Cisco WebEx Administration Tool. See the following topics for more information:

- *Getting started with Cisco Unified Communications Manager for Click to Call*
- *Creating Unified Communications Clusters*

What to do next

Add Teleconferencing Service Name Accounts, on page 149

Add Teleconferencing Service Name Accounts

Users can make teleconference calls with either the default Cisco WebEx audio service or a third-party teleconference provider.

To integrate the third-party teleconference provider audio services with Cisco WebEx, you must add teleconferencing service name accounts. After you add those accounts, users can make teleconference calls with the third-party provider audio services.

For more information about adding teleconferencing service name accounts, see the *Cisco WebEx Site Administration User's Guide*.

Before you begin

Configure Audio and Video Services, on page 149

Configure Voice and Video Communication for On-Premises Deployments

Procedure

	Command or Action	Purpose
Step 1	Create Software Phone Devices, on page 151	
Step 2	Create Desk Phone Devices, on page 184	
Step 3	Create CTI Remote Devices, on page 190	Complete this task only if you have Cisco Unified Communications Manager 9.x and later.
Step 4	Set Up a CTI Gateway, on page 196	
Step 5	Silent Monitoring and Call Recording, on page 197	Complete this task only if you have Cisco Unified Communications Manager 8.6.
Step 6	URI Dialing, on page 198	Complete this task only if you have Cisco Unified Communications Manager 9.x and later.
Step 7	Call Pickup, on page 201	
Step 8	Hunt Group, on page 206	
Step 9	Configure User Associations, on page 210	
Step 10	Specify Your TFTP Server Address, on page 211	
Step 11	Reset Devices, on page 213	Only if installing Cisco Jabber for Mac
Step 12	Create a CCMCIP Profile, on page 214	
Step 13	Dial Plan Mapping, on page 215	
Step 14	Set Up Mobile Connect, on page 216	
Step 15	Move to Mobile, on page 222	
Step 16	Dial via Office, on page 226	

	Command or Action	Purpose
Step 17	Voicemail Avoidance, on page 232	

Create Software Phone Devices

Procedure

	Command or Action	Purpose
Step 1	Choose one of the following to create a CSF device: • If you have Cisco Unified Communications Manager 9.x or later, complete this task:Create CSF Devices, on page 151. • If you have Cisco Unified Communications Manager 8.6(2), complete this task:Create CSF Devices on 8.6(2) and Later, on page 152.	
Step 2	Install Cisco Options Package File for Devices, on page 155	
Step 3	Create SIP Profiles, on page 156	
Step 4	Setting up System SIP Parameters, on page 157	
Step 5	Create TCT Devices, on page 157	
Step 6	Create TAB Devices, on page 161	
Step 7	Create BOT Devices, on page 162	
Step 8	Add Directory Number to the Device for Mobile Applications, on page 167	
Step 9	Video Desktop Sharing, on page 168	
Step 10	Set Up Secure Phone Capabilities, on page 168	
Step 11	Add Directory Number to the Device for Desktop Applications, on page 166	

Create CSF Devices

Complete the steps in this task to create CSF devices.

Note A CSF should not be associated to multiple users if you intend to use different service profiles for those users.

Multiple lines are not supported on 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 Set the **Owner User ID** field to the appropriate user.

Important On Cisco Unified Communications Manager version 9.x, the client uses the **Owner User ID** field to get service profiles for users. For this reason, each user must have a device and the **User Owner ID** field must be associated with the user.

If you do not associate users with devices and set the **Owner User ID** field to the appropriate user, the client cannot retrieve the service profile that you apply to the user.

Step 7 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.

See the *Set Up Secure Phone Capabilities* for instructions on configuring secure CSF devices.

Step 8 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

Install Cisco Options Package File for Devices, on page 155

Create CSF Devices on 8.6(2) and Later

The steps in this section describe how to create CSF devices on Cisco Unified Communications Manager version 8.6(2) and later. CSF devices provide users with software phone capabilities.

As part of the task of creating CSF devices, you can enable video desktop sharing using Binary Floor Control Protocol (BFCP). Cisco Unified Communications Manager handles the BFCP packets that users transmit when using video desktop sharing capabilities. For this reason, you configure Cisco Unified Communications Manager to allow BFCP presentation sharing. On Cisco Unified Communications Manager version 8.6(2) and later, you must apply a COP file to add an option to allow BFCP presentation sharing on CSF devices. You must then enable BFCP presentation sharing on the CSF devices.

Note

- Cisco Unified Communications Manager supports BFCP presentation sharing on version 8.6(1) and later only. You cannot enable BFCP, or provision users with video desktop sharing capabilities, on versions earlier than 8.6(1).
- 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.
- In hybrid cloud-based deployments, both Cisco WebEx and Cisco Unified Communications Manager provide desktop sharing functionality.
  - If users initiate desktop sharing sessions during an instant messaging session, Cisco WebEx provides desktop sharing capabilities.
  - If users initiate desktop sharing sessions during an audio or video conversation, Cisco Unified Communications Manager provides desktop sharing capabilities.

Tip

As of Cisco Unified Communications Manager version 8.6(2), you must enable BFCP on the SIP trunk to allow video desktop sharing capabilities between nodes in 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.

What to do next

Install Cisco Options Package File for Devices, on page 155

Apply COP File for BFCP Capabilities

You must apply `cmterm-bfcp-e.8-6-2.cop.sgn` to configure video desktop sharing on Cisco Unified Communication Manager release 8.6.2 and later. This COP file adds an option to enable BFCP on the CSF device.

Note

- You must install the COP file each time you upgrade. For example, if you configure video desktop sharing on Cisco Unified Communication Manager Release 8.6.2 .20000-1 and then upgrade to Cisco Unified Communication Manager Release 8.6.2 .20000-2, you must apply the COP file on Cisco Unified Communication Manager Release 8.6.2 .20000-2.
- If you configure video desktop sharing on Cisco Unified Communication Manager Release 8.6.1 and then upgrade to Cisco Unified Communication Manager release 8.6.2, you must apply the COP file on Cisco Unified Communication Manager release 8.6.2 before you can configure video desktop sharing.

Procedure

Step 1 Download the Cisco Jabber administration package from Cisco.com.

Step 2 Copy `cmterm-bfcp-e.8-6-2.cop.sgn` from the Cisco Jabber administration package to your file system.

Step 3 Open the **Cisco Unified Communications Manager Administration** interface.

Step 4 Upload and apply `cmterm-bfcp-e.8-6-2.cop.sgn`.

Step 5 Restart the server as follows:

a) Open the **Cisco Unified OS Administration** interface.
b) Select **Settings** > **Version**.
c) Select **Restart**.
d) Repeat the preceding steps for each node in the cluster, starting with your presentation server.

The COP add the **Allow Presentation Sharing using BFCP** field to the **Protocol Specific Information** section on the **Phone Configuration** window for CSF 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 Configuration Settings* topic in the Cisco Unified Communications Manager documentation for more information about the configuration settings on the **Phone Configuration** window.

See the *Set Up Secure Phone Capabilities* for instructions on configuring secure CSF devices.

Step 7 Select **Allow Presentation Sharing using BFCP** in the **Protocol Specific Information** section to enable video desktop sharing.

Video desktop sharing using BFCP is not supported if **Trusted Relay Point** or **Media Termination Point** are enabled on the software phone device.

Step 8 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.

Install Cisco Options Package File for Devices

To make Cisco Jabber available as a device in Cisco Unified Communications Manager, you must install a device-specific Cisco Options Package (COP) file on all your Cisco Unified Communications Manager nodes.

Perform this procedure at a time of low usage; it can interrupt service.

General information about installing COP files is available in the “Software Upgrades” chapter in the *Cisco Unified Communications Operating System Administration Guide* for your release.

Procedure

Step 1 Download the device COP file.

a) Locate the device COP file.

- Go to the software downloads site.
- Locate the device COP file for your release.

b) Click **Download Now**.

c) Note the MD5 checksum.

You will need this information later.

d) Click **Proceed with Download** and follow the instructions.

Step 2 Place the COP file on an FTP or SFTP server that is accessible from your Cisco Unified Communications Manager nodes.

Step 3 Install this COP file on the Publisher node in your Cisco Unified Communications Manager cluster:

a) Open the **Cisco Unified OS Administration** interface.
b) Select **Software Upgrades** > **Install/Upgrade**.
c) Specify the location of the COP file and provide the required information.

   For more information, see the online help.

d) Select **Next**.
e) Select the device COP file.
f) Select **Next**.
g) Follow the instructions on the screen.
h) Select **Next**.

   Wait for the process to complete. This process can take some time.

i) Reboot Cisco Unified Communications Manager at a time of low usage.
j) Let the system fully return to service.

   Note To avoid interruptions in service, make sure each node returns to active service before you perform this procedure on another server.

Step 4 Install the COP file on each Subscriber node in the cluster.

Use the same process you used for the Publisher, including rebooting the node.

Create SIP Profiles

This procedure is required only when you use Cisco Unified Communication Manager release 9 or earlier and are configuring devices for mobile clients. Use the default SIP profile provided for desktop clients.

If you use Cisco Unified Communication Manager release 9 or earlier, before you create and configure devices for mobile clients, you must create a SIP profile that allows Cisco Jabber to stay connected to Cisco Unified Communication Manager while Cisco Jabber runs in the background.

If you use Cisco Unified Communication Manager Release 10, choose the **Standard SIP Profile for Mobile Device** default profile when you create and configure devices for mobile clients.

Before you begin

Install Cisco Options Package File for Devices, on page 155

Procedure

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

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

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

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

- Find the default SIP profile and create a copy that you can edit.

- Select **Add New** and create a new SIP profile.

Step 4 In the new SIP profile, set the following values:

- **Timer Register Delta** to 120
- **Timer Register Expires** to 720
- **Timer Keep Alive Expires** to 720
- **Timer Subscribe Expires** to 21600
- **Timer Subscribe Delta** to 15

Step 5 Select **Save**.

What to do next

Setting up System SIP Parameters, on page 157

Setting up System SIP Parameters

If you are connected to a low-bandwidth network and finding it difficult to take an incoming call on your mobile device, you can set the system SIP parameters to improve the condition. Increase the SIP Dual Mode Alert Timer value to ensure that calls to the Cisco Jabber extension are not prematurely routed to the mobile-network phone number.

Before you begin

This configuration is only for mobile clients.

Cisco Jabber must be running to receive work calls.

Procedure

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

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

Step 3 Select the node.

Step 4 Select the **Cisco CallManager (Active)** service.

Step 5 Scroll to the **Clusterwide Parameters (System - Mobility)** section.

Step 6 Increase the **SIP Dual Mode Alert Timer** value to 10000 milliseconds.

Step 7 Select **Save**.

Note If, after you increase the SIP Dual Mode Alert Timer value, incoming calls that arrive in Cisco Jabber are still terminated and diverted using Mobile Connect, you can increase the SIP Dual Mode Alert Timer value again in increments of 500 milliseconds.

Create TCT Devices

Complete the steps in this task to create TCT devices for Cisco Jabber for iPhone users.

Restriction The maximum number of participants for ad-hoc conferences is limited to six, which is the maximum number of calls for TCT devices.

Before you begin

Specify the organization top domain name to support registration between Cisco Jabber and the Cisco Unified Communications Manager. In **Unified CM Administration** interface, select **System** > **Enterprise Parameters**. Under the **Clusterwide Domain Configuration** section, enter the organization top domain name. For example, cisco.com.

Setting up System SIP Parameters, on page 157

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 Dual Mode for iPhone** from the **Phone Type** drop-down list and then select **Next**.

Step 5 Specify configuration settings on the **Phone Configuration** window as appropriate. See the *TCT Device Configuration Settings* topic below for information about the specific settings that are required for TCT devices.

RestrictionMultiple lines are not supported on TCT devices.

Step 6 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.

Step 7 Select **Apply Config**.

What to do next

Create TAB Devices, on page 161

TCT Device Configuration Settings

Use the following tables to set up TCT devices on the **Phone Configuration** window.

Restrictions and requirements that are not specific to Cisco Jabber may apply to these values. If you require additional information about any option on the **Phone Configuration** window, see the online help in the **Cisco Unified CM Administration** interface.

Table 7: Device Information Settings

Setting	Description
Device Name	The Device Name: • Can represent only one device. If a single user has Cisco Jabber on multiple devices (for example, an iPhone and an iPod Touch), configure separate Cisco Dual Mode for iPhone devices for each in Cisco Unified Communications Manager. • Must start with TCT. • Must be uppercase. • Can contain up to 15 characters total. • Can include only A to Z, 0 to 9, dot (.), dash (-), or underscore (_). Cisco recommends that the device name include the username of the user so it is easy to remember (for example, the recommended device name of user jsmith is TCTJSMITH).
Phone Button Template	Select Standard Dual Mode for iPhone.
Media Resource Group List	Set up the on-hold music to ensure that if a user puts a call on hold, the other party hears on-hold music. This step prevents confusion for the other party. **Note** You must select an option in the **Media Resource Group List** to ensure that users can merge the audio for calls. These settings are not specific to this device. For more information about these settings, see the Cisco Unified Communications Manager documentation.
User Hold MOH Audio Source	
Network Hold MOH Audio Source	
Primary Phone	If this user has a desk phone, select the desk phone. Selecting the primary phone sets the device as an adjunct in the Cisco Unified Communications Manager for licensing purposes.

Table 8: Protocol-Specific Information Settings

Setting	Description
Device Security Profile	Select **Cisco Dual Mode for iPhone - Standard SIP Non-Secure Profile**.

Setting	Description
SIP Profile	Cisco Unified Communications Manager Release 9 and earlier — Select the SIP profile you created in the *Create SIP Profiles* topic. Cisco Unified Communications Manager Release 10 — Select the default profile for mobile devices: **Standard SIP Profile for Mobile Device** If the default profile for mobile devices does not suit your environment, you can create a custom SIP profile.
Other settings in the preceding sections	As appropriate to your deployment. Values that are not described in this document are not specific to Cisco Jabber but you may need to enter them for the device to work properly.

Information in this section is downloaded to the iOS device during initial setup, to automatically set up the client.

Table 9: Product Specific Configuration Layout Settings

Setting	Description
Emergency Numbers	Numbers that, when dialed on an iPhone, connect using the native phone application and the mobile network of the device. If dialed on an iPod, these numbers connect using VoIP calling. For example, 911, 999, 112. These numbers are prepopulated. Update if necessary.
Preset Wi-Fi Networks	The SSIDs for Wi-Fi networks. Cisco Jabber triggers Connect on Demand to Cisco AnyConnect Secure Mobility Client if users are not on a Wi-Fi network listed in this field, or if they are on a mobile data network. Separate multiple SSIDs with forward slash (/). Example: SalesOffice1/CorporateWiFi
On-Demand VPN URL	Enter the URL that you want to use to initiate on-demand VPN.
Default Ringtone	Select **Loud** or **Normal**.
Video Capabilities	Default is set to **Enabled**, which allows users to make and receive video calls.

The following Product Specific Configuration Layout settings are not supported in this release. Leave these settings blank:

- Allow End User Configuration Editing
- iPhone Country Code
- Cisco Usage and Error Tracking
- SIP Digest settings:
    - Enable SIP Digest Authentication

  - SIP Digest Username
- Sign In Feature
- Voicemail settings:
  - Voicemail Username
  - Voicemail Server
  - Voicemail Message Store Username
  - Voicemail Message Store
- Directory settings:
  - Directory Lookup Rules URL
  - Application Dial Rules URL
  - Enable LDAP User Authentication
  - LDAP Username
  - LDAP Password
  - LDAP Server
  - Enable LDAP SSL
  - LDAP Search Base
  - LDAP Field Mappings
  - LDAP Photo Location

Create TAB Devices

Use this procedure to create a softphone device for use with a tablet.

Note Multiple lines are not supported on TAB devices.

Before you begin

Create TCT Devices, on page 157

Procedure

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

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

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

Step 3 Select **Add New**.

Step 4 Select **Cisco Jabber for Tablet** from the **Phone Type** dropdown list and select **Next**.

The **Phone Configuration** window opens.

Step 5 Specify a name for the device in the Device Name field. You should use the format **TAB *username*** for tablet device names. For example, you create a device for a user named Tanya Adams, whose username is tadams. In this case, you should specify ***TABTADAMS*** as the device name.

Note Tablet Phone Device names must be in uppercase.

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 this 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

Create BOT Devices, on page 162

Create BOT Devices

Complete the steps in this task to create BOT devices for Cisco Jabber for Android users.

Restriction The maximum number of participants for ad-hoc conferences is limited to three, which is the maximum number of calls for BOT devices.

Before you begin

- Verify that the Device Pool that you plan to assign to the Cisco Jabber for Android device is associated with a region that includes support for one of the following codecs: G.711 mu-law, G.711 a-law, G.722.1, or G.729a.
- Specify the organization top domain name to support registration between Cisco Jabber and the Cisco Unified Communications Manager. In **Cisco Unified CM Administration** interface, select **System** > **Enterprise Parameters**. Under the Clusterwide Domain Configuration section, enter the organization top domain name. For example, cisco.com.
- Create TAB Devices, on page 161

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 Dual Mode for Android from the **Phone Type** drop-down list and then select **Next**.

Step 5 Specify configuration settings on the **Phone Configuration** window as appropriate. See the *BOT Device Configuration Settings* topic below for information about the specific settings that are required for BOT devices.

RestrictionMultiple lines are not supported on BOT devices.

Step 6 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.

Step 7 Select **Apply Config**.

What to do next

Add Directory Number to the Device for Mobile Applications, on page 167

BOT Device Configuration Settings

Use the following tables to set up BOT devices on the **Phone Configuration** window.

Restrictions and requirements that are not specific to Cisco Jabber for Android may apply to these values. If you require additional information about any option on the **Phone Configuration** window, see the online help in the **Cisco Unified CM Administration** interface.

Table 10: Device Information Settings

Setting	Description
Device Name	The Device Name: • Can represent only one device. If a single user has Cisco Jabber for Android on multiple devices, configure separate Cisco Dual Mode for Android devices for each in Cisco Unified Communications Manager. • Must start with BOT. • Must be uppercase. • Can contain up to 15 characters total. • Can include only the following characters: A to Z, 0 to 9, dot (.), dash (-), or underscore (_). Cisco recommends that the device name include the username of the user so it is easy to remember (for example, the recommended device name of user jsmith is BOTJSMITH).
Phone Button Template	Select Standard Dual Mode for Android.

Setting	Description
Media Resource Group List	Set up the on-hold music to ensure that if a user puts a call on hold, the other party hears on-hold music. This step prevents confusion for the other party. **Note** You must select an option in the **Media Resource Group List** to ensure that users can merge the audio for calls. **Note** Cisco Jabber for Android does not support Multicast Music on Hold. Ensure that the Media Resource Group List that you apply to the BOT device does not contain multicast-enabled Media Resource Groups. These settings are not specific to this device. For more information about these settings, see the Cisco Unified Communications Manager documentation.
User Hold MOH Audio Source	
Network Hold MOH Audio Source	
Primary Phone	If this user has a desk phone, select the desk phone. Selecting the primary phone sets the device as an adjunct in Cisco Unified Communications Manager for licensing purposes.
Owner User ID	Select the user. The value must match the Mobility User ID.

Table 11: Protocol-Specific Information Settings

Setting	Description
Device Security Profile	Select **Cisco Dual Mode for Android - Standard SIP Non-Secure Profile**.
SIP Profile	Cisco Unified Communications Manager Release 9 and earlier — Select the SIP profile you created in *Create SIP Profiles* topic. Cisco Unified Communications Manager Release 10 — Select the default profile for mobile devices: Standard SIP Profile for Mobile Device. If the default profile for mobile devices does not suit your environment, you can create a custom SIP profile.
Other settings in the preceding sections	As appropriate to your deployment. Values that are not described in this document are not specific to Cisco Jabber but you may need to enter them for the device to work properly.

Information in this section is downloaded to the Android device during initial setup, to automatically set up the client.

Table 12: Product Specific Configuration Layout Settings

Setting	Description
Emergency Numbers	The Emergency Numbers setting is not supported in this release. Leave this setting blank. **Important** For Release 9.6, emergency calls are placed through Cisco Unified Communications Manager. Ensure that Cisco Unified Communications Manager is set up to properly route emergency calls.
Device Ringtone Volume	Select an option if you want to prevent users from silencing incoming Cisco Jabber for Android calls. • **Native** — (Default) Select this option if you want to allow the user to set any ringtone volume on the Android device, including silent mode or vibrate. • **Low**, **Medium**, or **High** — Select one of these options to specify the *minimum* ringtone volume on the user's device. Users can specify a louder ringtone volume than the minimum on their device.
Device Ringtone	Select a ringtone option: • **Native Ringtone** — (Default) Cisco Jabber for Android uses the ringtone that the user sets for the native phone application on the Android device. • **Cisco Ringtone** — Cisco Jabber for Android uses only the Cisco ringtone (even if the user sets a different ringtone for the native phone application on the Android device).
Video Capabilities	Default is set to **Enabled**, which allows users to make and receive video calls.

The following Product Specific Configuration Layout settings are not supported in this release. Leave these settings blank:

- SIP Digest settings:
  - Enable SIP Digest Authentication
  - SIP Digest Username
- Voicemail settings:
  - Voicemail Username
  - Voicemail Server
  - Voicemail Message Store Username

  - Voicemail Message Store

- Directory settings:
  - Directory Lookup Rules URL
  - Application Dial Rules URL
  - Enable LDAP User Authentication
  - LDAP Username
  - LDAP Password
  - LDAP Server
  - Enable LDAP SSL
  - LDAP Search Base
  - LDAP Field Mappings
  - LDAP Photo Location
  - Domain Name
  - Preset Wi-Fi Networks

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.

Add Directory Number to the Device for Mobile Applications

Before you begin

Create BOT Devices, on page 162

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.

This can be a new DN. A desk phone with the same DN is not required.

Step 4 Select one of the following options to set the No Answer Ring Duration (seconds) setting.

Option	Description
Default	Set the value to 12 seconds.
If DVO is enabled	Start with a value of 24 seconds. This value allows time for Cisco Jabber to ring before calls go to voicemail. If you enable DVO and remote destination features, this value is dependent on local mobile voice network connection speeds. Adjust your settings accordingly. **Note** If you increase the value of this setting, see the related cautions for this setting in the online help in Cisco Unified Communications Manager.
If users have a PIN on the device	Start with the default value. You may need to increase this setting to ensure that users have enough time to enter the PIN and answer the call before the call goes to voicemail. **Note** If you increase the value of this setting, see the related cautions for this setting in the online help in Cisco Unified Communications Manager.

Step 5 In the Multiple Call/Call Waiting Settings on Device section, in the **Busy Trigger** field, ensure that the value is set to 3.

Step 6 Specify all other required configuration settings as appropriate.

Step 7 Select **Save**.

What to do next

Video Desktop Sharing, on page 168

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.

Note Cisco Jabber for mobile clients can only receive BFCP.

Note

- 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.
- In hybrid cloud-based deployments, both Cisco WebEx and Cisco Unified Communications Manager provide desktop sharing functionality.
  - If users initiate desktop sharing sessions during an instant messaging session, Cisco WebEx provides desktop sharing capabilities.
  - If users initiate desktop sharing sessions during an audio or video conversation, Cisco Unified Communications Manager provides desktop sharing capabilities.
- Video desktop sharing using BFCP is not supported if **Trusted Relay Point** or **Media Termination Point** are enabled on the software phone device.
- Video desktop sharing using BFCP is not supported during Cisco Jabber multi-party conference calls unless Cisco TelePresence MCU is deployed.

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

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

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

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

Before you begin

Video Desktop Sharing, on page 168

What to do next

Add Directory Number to the Device for Desktop Applications, on page 166

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**.
- TFTP Encrypted Config — Select this checkbox to encrypt the CSF device configuration file that resides on the TFTP server.
- Authentication Mode — Select By Authentication String.
- Key Size (Bits) — Select the appropriate key size for the certificate.

  Note Key size refers to the bit length of the public and private keys that the client generates during the CAPF enrollment process.

  The client has been tested using authentication strings with 1024 bit length keys. The client requires more time to generate 2048 bit length keys than 1024 bit length keys. As a result, if you select 2048, you should expect it to take longer to complete the CAPF enrollment process.

  Cisco Jabber for Mac 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.

  Cisco Jabber for iPgone and iPad 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.

  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.

Configure TCT and TAB Devices

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

Procedure

Step 1 Open the TCT or TAB 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 TCT or TAB 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 TCT or TAB devices. You must complete the secure phone set up for users to be able to access their TCT or TAB devices.

What to do next

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

Configure BOT Devices

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

Procedure

Step 1 Open the BOT 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 BOT device from the list.
   The **Phone Configuration** window opens.

Step 2 Locate the Protocol Specific Information section.

Step 3 Select the phone security profile from the Device Security Profile drop-down list.

Step 4 Select **Save**.

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

What to do next

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

Specify Certificate Settings

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

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

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

Procedure

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

Step 2 Specify values as follows:

- Certificate Operation — Select **Install/Upgrade**.
- Authentication Mode — Select **By Authentication String**.
- Key Size (Bits) — Select the same key size that you set in the phone security profile.
- Operation Completes By — Specify an expiration value for the authentication string or leave as default.

Step 3 Select **Save**.

Step 4 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

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 for Cisco Jabber for Windows

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.	Can be 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 the following 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 nodes.

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 sign 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.

For example, you set up secure phone capabilities on a CSF device to which both Cisco Jabber for Windows version 9.2 and Cisco Jabber for Windows version 9.1 register. However, Cisco Jabber for Windows version 9.1 does not support secure phone capabilities. In this scenario, you must create two different CSF devices, one secure CSF device for Cisco Jabber for Windows version 9.2 and another CSF device that is not secure for Cisco Jabber for Windows version 9.1.

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 sign 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.

Secure Phone Details for Cisco Jabber for Mac

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 the following 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 Manage provide the ability to display the lock icon. If the version of Cisco Unified Communications Manage 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 Manage 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 Manage.

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 information 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 nodes.

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 keychain.

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.

“For example, you set up secure phone capabilities on a CSF device. Two versions of Cisco Jabber register the device. However, one version of Cisco Jabber does not support secure phone capabilities. In this scenario, you must create two different CSF devices, one secure CSF device for Cisco Jabber that supports secure phone capabilities and another CSF device that is not secure for the other Cisco Jabber ”

Multiple Users on a Shared Mac OS Account

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

You should ensure that multiple users who share the same Mac account have CSF devices with unique names. Users cannot register their CSF devices if they share the same Mac 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 sign in to the same Mac 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 Mac user. When a user logs in to their Mac 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 Mac users.

Secure Phone Details for Cisco Jabber for iPhone and iPad

Secure Connections

If you enable secure phone capabilities, then:

- SIP connections between TCT or TAB 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 or AES 256 or SHA encryption.
- Mutual TLS ensures that only TCT or TAB devices with the correct certificates can register to Cisco Unified Communications Manager. Likewise, TCT or TAB devices can register only to Cisco Unified Communications Manager instances that provide the correct certificate.

If you enable secure phone capabilities for users, their TCT or TAB 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

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' TCT or TAB 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 TCT or TAB 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 the following 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 from outside the corporate network.

Secure phone capabilities can be used through Expressway for Mobile and Remote Access by installing the Cisco Expressway-C certificate and configuring the Secure Profile Domain as the Phone Security Profile in Cisco Unified Communications Manager.

When users connect 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 TCT or TAB 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 nodes.

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 device trust store.

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.

TCT and TAB 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 TCT devices with secure phone capabilities. User C has a TCT device without secure phone capabilities. In this case, the call is not secure for all users.

Secure Phone Details for Cisco Jabber for Android

Secure Connections

If you enable secure phone capabilities, then:

- SIP connections between BOT or TAB 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 BOT devices with the correct certificates can register to Cisco Unified Communications Manager. Likewise, BOT devices can register only to Cisco Unified Communications Manager instances that provide the correct certificate.

If you enable secure phone capabilities for users, their BOT 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

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' BOT 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 BOT 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 the following 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 from outside the corporate network.

Secure phone capabilities can be used through Expressway for Mobile and Remote Access by installing the Cisco Expressway-C certificate and configuring the Secure Profile Domain as the Phone Security Profile in Cisco Unified Communications Manager.

When users connect 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 BOT 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 nodes.

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 device trust store.

Conference Calls

For audio or video conference calls or multi-party calls, you must set up a secure multimedia conferencing bridge using a Multipoint Control Unit (MCU). When setting up the MCU, you must ensure that you create a secure SIP Trunk Security Profile and set the Device Security Mode to Encrypted. For more information, see the Conference Bridge setup chapter in the *Cisco Unified Communications Manager Administration Guide* for your release.

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 Set the **Owner User ID** field to the appropriate user.

Important On Cisco Unified Communications Manager version 9.x, the client uses the **Owner User ID** field to get service profiles for users. For this reason, each user must have a device and the **User Owner ID** field must be associated with the user.

If you do not associate users with devices and set the **Owner User ID** field to the appropriate user, the client cannot retrieve the service profile that you apply to the user.

Step 7 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 8 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 9 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**.

Create CTI Remote Devices

CTI remote devices let users control calls on devices other than software phone devices or desk phone devices such as Cisco IP phones.

Extend and Connect Capabilities

Cisco Unified Communications Manager Extend and Connect capabilities let users control calls on devices such as public switched telephone network (PSTN) phones and private branch exchange (PBX) devices.

Note Cisco recommends that you use extend and connect capabilities with Cisco Unified Communications Manager 9.1(1) and later only.

Provisioning CTI Remote Devices

Dedicated Device

You can provision users with dedicated CTI remote devices. For example, each user has a PSTN phone at their workstation. You want to allow the users to make calls with their PSTN phones using the client. You do not plan to provision users with software phone devices or desk phone devices.

To provision CTI remote devices as dedicated devices, you should add remote destinations through the **Cisco Unified CM Administration** interface. This ensures that users can automatically control their phones and place calls when they start the client.

Alternative Device

You can provision CTI remote devices so that users can specify an alternative phone number to their software phone device or desk phone device. For example, each user can work remotely from home. In this case, users can specify their home phone numbers as remote destinations. This allows the users to control home phones with the client.

If you plan to provision CTI remote devices as an alternative device, you should not add remote destinations. Users can add, edit, and delete remote destinations through the client interface.

Enable Users to Modify Remote Destinations

When a user logs in, the client retrieves the user's device list from Cisco Unified Communications Manager.

If that device list contains a software phone device or desk phone device, the client automatically lets users add, edit, and delete remote destinations through the client interface.

If that device list contains only a CTI remote device, the client does not let users add, edit, and delete remote destinations. You must enable users to add, edit, and delete remote destinations in the client configuration.

Using CTI Remote Devices with the Client

If a user is signed in to the client and sets a remote device as active, that device rings when the user receives incoming calls. Additionally, the client routes outgoing calls to the active device when the user is signed in.

If a user is not signed in to the client, and that user receives an incoming call to the directory number, all devices set as remote destinations ring.

Limitations and Known Issues

This section describes limitations and known issues that currently exist for Cisco Unified Communications Manager extend and connect capabilities.

- You can create only one remote destination per user. Do not add two or more remote destinations for a user.
- Two or more users cannot use the same remote destination.
- Users cannot use the same remote destination for multiple devices.
- You cannot provision extend and connect capabilities for devices that you configure as endpoints on the Cisco Unified Communications Manager cluster.
- Incoming calls incorrectly ring on remote devices if the following occurs:
  1. A user adds a number for a remote destination.

     Cisco Unified Communications Manager routes incoming calls to that remote destination. The user can control the call session with the client.
  2. The user changes their phone. For example, the user selects their software phone.

     Cisco Unified Communications Manager routes incoming calls to the user's software phone. However, if the user does not answer incoming calls on the software phone within 4 or 5 seconds, the user's remote destination also rings.

  To resolve this issue, users must delete numbers for remote destinations when they change their phones.

Enable User Mobility

This task is only for desktop clients.

You must enable user mobility to provision CTI remote devices. If you do not enable mobility for users, you cannot assign those users as owners of CTI remote devices.

Before you begin

This task is applicable only if:

- You plan to assign Cisco Jabber for Mac or Cisco Jabber for Windows users to CTI remote devices.
- You have Cisco Unified Communication Manager release 9.x and later.

Procedure

Step 1 Select **User Management** > **End User**.

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

Step 2 Specify the appropriate filters in the **Find User where** field to and then select **Find** to retrieve a list of users.

Step 3 Select the user from the list.

The **End User Configuration** window opens.

Step 4 Locate the **Mobility Information** section.

Step 5 Select **Enable Mobility**.

Step 6 Select **Save**.

Create CTI Remote Devices

CTI remote devices are virtual devices that monitor and have call control over a user's remote destination.

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 **CTI Remote Device** from the **Phone Type** drop-down list and then select **Next**.

The **Phone Configuration** window opens.

Step 5 Select the appropriate user ID from the **Owner User ID** drop-down list.

Note Only users for whom you enable mobility are available from the **Owner User ID** drop-down list. For more information, see Enable SAML SSO in the Client.

Cisco Unified Communications Manager populates the **Device Name** field with the user ID and a **CTIRD** prefix; for example, **CTIRDusername**

Step 6 Edit the default value in the **Device Name** field, if appropriate.

Step 7 Ensure you select an appropriate option from the **Rerouting Calling Search Space** drop-down list in the **Protocol Specific Information** section.

The **Rerouting Calling Search Space** drop-down list defines the calling search space for re-routing and ensures that users can send and receive calls from the CTI remote device.

Step 8 Specify all other configuration settings on the **Phone Configuration** window as appropriate.

See the *CTI remote device setup* topic in the System Configuration Guide for Cisco Unified Communications Manager documentation for more information.

Step 9 Select **Save**.

The fields to associate directory numbers and add remote destinations become available on the **Phone Configuration** window.

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.

Add a Remote Destination

Remote destinations represent the CTI controllable devices that are available to users.

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

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

Note

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

Procedure

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

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

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

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

Step 4 Select the CTI remote device from the list.

The **Phone Configuration** window opens.

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

Step 6 Select **Add a New Remote Destination**.

The **Remote Destination Information** window opens.

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

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

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

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

Step 9 Specify all other values as appropriate.

Step 10 Select **Save**.

What to do next

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

1. Repeat the steps to open the **Phone Configuration** window for the CTI remote device.
2. Locate the **Associated Remote Destinations** section.

3. Verify the remote destination is available.
4. Select **Apply Config**.

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

When users select a remote destination in the client, it displays as the value of **Active Remote Destination**.

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

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

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**.

Set Up a CTI Gateway

The client requires a CTI gateway to communicate with Cisco Unified Communications Manager and perform certain functions such as desk phone control.

Add a CTI Gateway Server

This task is applicable only if you have CUCM 8.6 with CUP.

The client requires a CTI gateway to communicate with Cisco Unified Communications Manager and perform certain functions such as desk phone control. The first step to set up a CTI gateway is to add a CTI gateway server on Cisco Unified Presence.

Procedure

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

Step 2 Select **Application** > **Cisco Jabber** > **CTI Gateway Server**.

Note In some versions of Cisco Unified Presence, this path is as follows: **Application** > **Cisco Unified Personal Communicator** > **CTI Gateway Server**.

The **Find and List CTI Gateway Servers** window opens.

Step 3 Select **Add New**.

The **CTI Gateway Server Configuration** window opens.

Step 4 Specify the required details on the **CTI Gateway Server Configuration** window.

Step 5 Select **Save**.

What to do next

Create a CTI Gateway Profile, on page 197

Create a CTI Gateway Profile

After you add a CTI gateway server, you must create a CTI gateway profile and add that server to the profile.

Before you begin

Add a CTI Gateway Server, on page 196

Procedure

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

Step 2 Select **Application** > **Cisco Jabber** > **CTI Gateway Profile**.

Note In some versions of Cisco Unified Presence, this path is as follows: **Application** > **Cisco Unified Personal Communicator** > **CTI Gateway Profile**.

Step 3 In the **CTI Gateway Profile Configuration** window, specify the required details.

Step 4 Select **Add Users to Profile** and add the appropriate users to the profile.

Step 5 Select **Save**.

Silent Monitoring and Call Recording

Applies to: Cisco Jabber for Windows, Cisco Jabber for Android, Cisco Jabber for iOS

This feature is supported for on-premises deployment and requires Cisco Unified Communications Manager 8.6.

You can set up extra audio path functions for devices such as silent monitoring and call recording.

Note This feature is currently supported on Cisco Jabber for Windows only.

To enable silent monitoring and call recording, see the *Monitoring and Recording* section of the *Cisco Unified Communications Manager Features and Services Guide* for step-by-step instructions.

Notes:

- Cisco Jabber does not provide any interface to begin silent monitoring or call recording. Use the appropriate software to silently monitor or record calls.
- Cisco Jabber does not currently support monitoring notification tone or recording notification tone.
- You can use silent monitoring and call recording functionality only. Cisco Jabber does not support other functionality such as barging or whisper coaching.
- You might need to download and apply a device package to enable monitoring and recording capabilities on the device, depending on your version of Cisco Unified Communications Manager. Before you start configuring the server, do the following:
    1. Open the **Phone Configuration** window for the device on which you plan to enable silent monitoring and call recording.
    2. Locate the **Built In Bridge** field.

       If the **Built In Bridge** field is not available on the **Phone Configuration** window, download and apply the most recent device packages.

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 *Parameters Reference* Guide.

Applies to: All clients

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.

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

Applies to: Cisco Jabber for Windows, Cisco Jabber for Mac

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.

You can let a user log in to hunt groups by configuring EnableHuntGroup parameter. For more information, see the latest *Parameters Reference Guide for Cisco Jabber*.

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.

Hunt group features supported by the Cisco Jabber clients:

Features	Mobile Clients	Desktop Clients
Log in to hunt group and log out of hunt group	Not supported	Supported
Call, answer, and decline	Supported	Supported

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.

Before you begin

Create and configure Cisco Jabber devices.

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 **Service Settings** section.

Step 6 Select **Home Cluster**.

Step 7 Select the appropriate service profile for the user from the **UC Service Profile** drop-down list.

Step 8 Locate the **Device Information** section.

Step 9 Select **Device Association**.

The **User Device Association** window opens.

Step 10 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 11 Select **Save Selected/Changes**.

Step 12 Select **User Management** > **End User** and return to the **Find and List Users** window.

Step 13 Find and select the same user from the list.

The **End User Configuration** window opens.

Step 14 Locate the **Permissions Information** section.

Step 15 Select **Add to Access Control Group**.

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

Step 16 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**

Remember If you are provisioning users with secure phone capabilities, do not assign the users to the **Standard CTI Secure Connection** group.

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 17 Select **Add Selected**.

The **Find and List Access Control Groups** window closes.

Step 18 Select **Save** on the **End User Configuration** window.

Specify Your TFTP Server Address

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

Attention 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.

Specify Your TFTP Server on Cisco Unified Communications Manager IM and Presence Service

If you are using Cisco Unified Communications Manager release 9.x, then you do not need to follow the steps below.

Procedure

Step 1 Open the **Cisco Unified CM IM and Presence Administration** interface.

Step 2 Select **Application** > **Legacy Clients** > **Settings**.

The **Legacy Client Settings** window opens.

Step 3 Locate the **Legacy Client Security Settings** section.

Step 4 Specify the IP address of your primary and backup TFTP servers in the following fields:

- **Primary TFTP Server**
- **Backup TFTP Server**
- **Backup TFTP Server**

Step 5 Select **Save**.

Specify Your TFTP Server on Cisco Unified Presence

If you are using Cisco Unified Communications Manager release 8.x, complete the steps to specify the address of your TFTP server on Cisco Unified Presence. If you are using Cisco Unified Communications Manager release 9.x, then you do not need to follow the steps below.

Procedure

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

Step 2 Select **Application** > **Cisco Jabber** > **Settings**.

Note In some versions of Cisco Unified Presence, this path is as follows: **Application** > **Cisco Unified Personal Communicator** > **Settings**.

The **Cisco Jabber Settings** window opens.

Step 3 Locate the fields to specify TFTP servers in one of the following sections, depending on your version of Cisco Unified Presence:

- **Cisco Jabber Security Settings**
- **CUPC Global Settings**

Step 4 Specify the IP address of your primary and backup TFTP servers in the following fields:

- **Primary TFTP Server**
- **Backup TFTP Server**

- **Backup TFTP Server**

Note Ensure that you enter the fully qualified domain name (FQDN) or IP address for the TFTP servers rather than a host name.

Step 5 Select **Save**.

Specify TFTP Servers in Phone Mode

If you deploy the client in phone mode you can provide the address of the TFTP server as follows:

- 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.

Specify TFTP Servers with the Cisco WebEx Administration Tool

If the client connects to the Cisco WebEx Messenger service, you specify your TFTP server address with the Cisco WebEx Administrator Tool.

Procedure

Step 1 Open the Cisco WebEx Administrator Tool.

Step 2 Select the **Configuration** tab.

Step 3 Select **Unified Communications** in the **Additional Services** section.
The **Unified Communications** window opens.

Step 4 Select the **Clusters** tab.

Step 5 Select the appropriate cluster from the list.
The **Edit Cluster** window opens.

Step 6 Select **Advanced Server Settings** in the **Cisco Unified Communications Manager Server Settings** section.

Step 7 Specify the IP address of your primary TFTP server in the **TFTP Server** field.

Step 8 Specify the IP address of your backup TFTP servers in the **Backup Server #1** and **Backup Server #2** fields.

Step 9 Select **Save**.
The **Edit Cluster** window closes.

Step 10 Select **Save** in the **Unified Communications** window.

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

The client gets device lists for users from the CCMCIP server.

Note 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.

Before you begin

Reset Devices, on page 213

Procedure

Step 1 Open the **Cisco Unified CM IM and Presence Administration** interface.

Step 2 Select **Application** > **Legacy Clients** > **CCMCIP Profile**.

Step 3 In the **Find and List CCMCIP Profiles** window, select **Add New**.

Step 4 In the **CCMCIP Profile Configuration** window, specify service details in the CCMCIP profile as follows:

a) Specify a name for the profile in the **Name** field.

b) Specify the fully qualified domain name or IP address of your primary CCMCIP service in the **Primary CCMCIP Host** field.

c) Specify the fully qualified domain name or IP address of your backup CCMCIP service in the **Backup CCMCIP Host** field.

d) Leave the default value for **Server Certificate Verification**.

Cisco Unified Communications Manager release 9.x and earlier—If you enable Cisco Extension Mobility, the `Cisco Extension Mobility` service must be activated on the Cisco Unified Communications Manager nodes that are used for CCMCIP. For information about Cisco Extension Mobility, see the *Feature and Services* guide for your Cisco Unified Communications Manager release.

Step 5 Add users to the CCMCIP profile as follows:

a) Select **Add Users to Profile**.

b) In the **Find and List Users** dialog, specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.

c) Select the appropriate users from the list.

d) Select **Add Selected**.

The selected users are added to the CCMCIP profile.

Step 6 Select **Save**.

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.

Set Up Mobile Connect

Mobile connect, formerly known as Single Number Reach (SNR), allows the native mobile phone number to ring when someone calls the work number if:

- Cisco Jabber is not available.

  After Cisco Jabber becomes available again and connects to the corporate network, the Cisco Unified Communications Manager returns to placing VoIP calls rather than using mobile connect.

- The user selects the **Mobile Voice Network** calling option.
- The user selects the **Autoselect** calling option and the user is outside of the Wi-Fi network.

To set up mobile connect, perform the following procedures:

1. Enable mobile connect. See the *Enable Mobile Connect* topic.
2. Specify one or more remote phone numbers to which mobile connect connects using one or both of the following procedures:
   - (Preferred) To specify the mobile phone number of the mobile device, see the *Add Mobility Identity* topic.
   - (Optional) To specify alternate phone numbers, see the *Add Remote Destination (Optional)* topic.

     Alternate numbers can be any type of phone number, such as home phone numbers, conference room numbers, desk phone numbers, or a mobile phone number for a second mobile device.
3. Test your settings:
   - Exit Cisco Jabber on the mobile device. For instructions, see the User Guide for your release.
   - Call the Cisco Jabber extension from another phone.
   - Verify that the native mobile network phone number rings and that the call connects when you answer it.

Enable Mobile Connect

Use the following procedure to enable single number reach for your users.

Before you begin

Make sure that the user has a device already assigned to them.

Procedure

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

Step 2 Search for and delete any existing remote destination or mobility Identity that is already set up with the mobile phone number as follows:

a) Select **Device** > **Remote Destination**.
b) Search for the destination number.
c) Delete the destination number.

Step 3 Configure the end user for single number reach as follows:

a) Go to **User Management** > **End User**, search for the user and click their name.
b) In the **Mobility Information** section, check the **Enable Mobility** check box.
c) On Cisco Unified Communications Manager Release 9.0 and earlier, specify the Primary User Device.
d) Click **Save**.

Step 4 Create their remote destination profile.

a) Go to **Device** > **Device Settings** > **Remote Destination Profile** > **Add New**.

b) Enter the required values and click **Save**.

c) Click **Add a New Directory Number** and enter the directory number of the desk phone to associate with the remote destination profile.

d) Click **Save**.

e) Click **Add a New Remote Destination**, enter the number for your remote destination in **Destination number** and choose the **User ID**.

f) Click **Enable Unified Mobility** features, and click the following options:

- **Enable Single Number Reach**
- **Enable Move to Mobile**

g) Click **Save**.

Step 5 Configure the device settings for mobile connect as follows:

a) Navigate to **Device** > **Phone**.

b) Search for the device that you want to configure.

c) Select the device name to open the **Phone Configuration** window.

d) Enter the following information:

Setting	Information
Softkey Template	Choose a softkey template that includes the **Mobility** button. For information about setting up softkey templates, see the related information in the *Cisco Unified Communications Manager Administration Guide* for your release. This documentation can be found in the maintenance guides list.
Mobility User ID	Select the user.
Owner User ID	Select the user. The value must match the mobility user ID.

Setting	Information
Rerouting Calling Search Space	Choose a Rerouting Calling Search Space that includes both of the following: • The partition of the desk phone extension of the user. This requirement is used by the system to provide the Dial via Office feature, not for routing calls. • A route to the mobile phone number. The route to the mobile phone number (that is, the Gateway/Trunk partition) must have a higher preference than the partitions of the enterprise extension that is associated with the device. **Note** Cisco Jabber allows users to specify a callback number for Dial via Office-Reverse calls that is different from the mobile phone number of the device, and the Rerouting Calling Search Space controls which callback numbers are reachable. If the user sets up the DvO Callback Number with an alternate number, ensure that you set up the trunk Calling Search Space (CSS) to route to destination of the alternate phone number.

e) Select **Save**.

Add Mobility Identity

Use this procedure to add a mobility identity to specify the mobile phone number of the mobile device as the destination number. This destination number is used by features such as Dial via Office or mobile connect.

You can specify only one number when you add a mobility identity. If you want to specify an alternate number such as a second mobile phone number for a mobile device, you can set up a remote destination. The mobility identity configuration characteristics are identical to those of the remote destination configuration.

Procedure

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

Step 2 Navigate to the device that you want to configure as follows:

a) Select **Device** > **Phone**.
b) Search for the device that you want to configure.
c) Select the device name to open the **Phone Configuration** window.

Step 3 In the **Associated Mobility Identity** section, select **Add a New Mobility Identity**.

Step 4 Enter the mobile phone number as the destination number.

You must be able to rout this number to an outbound gateway. Generally, the number is the full E.164 number.

Note If you enable the Dial via Office — Reverse feature for a user, you must enter a destination number for the user's mobility identity.

If you enable Dial via Office — Reverse and leave the destination number empty in the mobility identity:

- The phone service cannot connect if the user selects the **Autoselect** calling option while using a mobile data network and VPN.
- The phone service cannot connect if the user selects the **Mobile Voice Network** calling option on any type of network.
- The logs do not indicate why the phone service cannot connect.

Step 5 Enter the initial values for call timers.

These values ensure that calls are not routed to the mobile service provider voicemail before they ring in the client on the mobile device. You can adjust these values to work with the end user's mobile network. For more information, see the online help in Cisco Unified Communications Manager.

The following is an example of mobility Identity timers' information in Cisco Unified Communications Manager 9.x.

Setting	Suggested Initial Value
Answer Too Soon Timer	3000
Answer Too Late Timer	20000
Delay Before Ringing Timer	0 **Note** This setting does not apply to DvO-R calls.

The following is an example of mobility Identity timers' information in Cisco Unified Communications Manager 10.x.

Setting	Suggested Initial Value
Wait * before ringing this phone when my business line is dialed.*	0.0 seconds
Prevent this call from going straight to this phone's voicemail by using a time delay of * to detect when calls go straight to voicemail.*	3.0 seconds
Stop ringing this phone after * to avoid connecting to this phone's voicemail.*	20.0 seconds

Step 6 Do one of the following:

- Cisco Unified Communications Manager release 9 or earlier — Check the **Enable Mobile Connect** check box.

- Cisco Unified Communications Manager release 10 — Check the **Enable Single Number Reach** check box.

Step 7 If you are setting up the Dial via Office feature, in the Mobility Profile drop-down list, select one of the following options.

Option	Description
Leave blank	Choose this option if you want users to use the Enterprise Feature Access Number (EFAN).
Mobility Profile	Choose the mobility profile that you just created if you want users to use a mobility profile instead of an EFAN.

Step 8 Set up the schedule for routing calls to the mobile number.

Step 9 Select **Save**.

Add Remote Destination (Optional)

Use this procedure to add a remote destination to specify any alternate number as the destination number. The Mobility Identity configuration characteristics are identical to those of the remote destination configuration.

Alternate numbers can be any type of phone number, such as home phone numbers, conference room numbers, desk phone numbers, or multiple mobile phone numbers for additional mobile devices. You can add more than one remote destination.

Procedure

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

Step 2 Navigate to the device that you want to configure as follows:

a) Select **Device** > **Phone**.
b) Search for the device that you want to configure.
c) Select the device name to open the **Phone Configuration** window.

Step 3 In the **Associated Remote Destinations** section, select **Add a New Remote Destination**.

Step 4 Enter the desired phone number as the Destination Number.

You must be able to rout the number to an outbound gateway. Generally, the number is the full E.164 number.

Step 5 Enter the initial values for the following call timers:

a) **Answer Too Soon Timer**—Enter 3000
b) **Answer Too Late Timer**— Enter 20000
c) **Delay Before Ringing Timer**—0

This setting does not apply to DvO-R calls.

These values ensure that calls are not routed to the mobile service provider voicemail before they ring in the client on the mobile device. For more information, see the online help in Cisco Unified Communications Manager.

Step 6 Do one of the following:

- If you have Cisco Unified Communications Manager Version 9 or earlier, check the **Enable Mobile Connect** check box.
- If you have Cisco Unified Communications Manager Version 10, check the **Enable Single Number Reach** check box.

Step 7 Set up the schedule for routing calls to the mobile number.

Step 8 Select **Save**.

Move to Mobile

Applies to: Cisco Jabber for Android, Cisco Jabber for iOS

Users can transfer an active VoIP call from Cisco Jabber to their mobile phone number on the mobile network. This feature is useful when a user on a call leaves the Wi-Fi network (for example, leaving the building to walk out to the car), or if there are voice quality issues over the Wi-Fi network.

There are two ways to enable this feature. You can also disable it.

Implementation Method	Description	Instructions
Handoff DN	The mobile device calls Cisco Unified Communications Manager using the mobile network. This method requires a Direct Inward Dial (DID) number. The service provider must deliver the DID digits exactly as configured. Alternately, for Cisco IOS gateways with H.323 or SIP communication to Cisco Unified Communications Manager, you can use Cisco IOS to manipulate the inbound called-party number at the gateway, presenting the digits to Cisco Unified Communications Manager exactly as configured on the handoff DN. This method does not work for iPod Touch devices.	See the *Enable Handoff from VoIP to Mobile Network* topic.
Mobility Softkey	Cisco Unified Communications Manager calls the phone number of the PSTN mobile service provider for the mobile device.	See the *Enable Transfer from VoIP to Mobile Network* topic.

Implementation Method	Description	Instructions
None of the above	Disable this feature if you do not want to make it available to users.	Select **Disabled** for the **Transfer to Mobile Network** option in the **Product Specific Configuration Layout** section of the TCT device page. Select **Disabled** for the **Transfer to Mobile Network** option in the **Product Specific Configuration Layout** section of the BOT device page.

Enable Handoff from VoIP to Mobile Network

Set up a directory number that Cisco Unified Communications Manager can use to hand off active calls from VoIP to the mobile network. Match the user's caller ID with the Mobility Identity to ensure that Cisco Unified Communications Manager can recognize the user. Set up the TCT device and mobile device to support handoff from VoIP to the mobile network.

Set up a directory number that Cisco Unified Communications Manager can use to hand off active calls from VoIP to the mobile network. Match the user's caller ID with the Mobility Identity to ensure that Cisco Unified Communications Manager can recognize the user. Set up the BOT device and mobile device to support handoff from VoIP to the mobile network.

Set Up Handoff DN

Before you begin

Determine the required values. The values that you choose depend on the phone number that the gateway passes (for example, seven digits or ten digits).

Procedure

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

Step 2 Select **Call Routing** > **Mobility** > **Handoff Configuration**.

Step 3 Enter the Handoff Number for the Direct Inward Dial (DID) number that the device uses to hand off a VoIP call to the mobile network.

The service provider must deliver the DID digits exactly as configured. Alternately, for Cisco IOS gateways with H.323 or SIP communication to Cisco Unified Communications Manager, you can use Cisco IOS to manipulate the inbound called-party number at the gateway, presenting the digits to Cisco Unified Communications Manager exactly as configured on the handoff number.

Note You cannot use translation patterns or other similar manipulations within Cisco Unified Communications Manager to match the inbound DID digits to the configured Handoff DN.

Step 4 Select the **Route Partition** for the handoff DID.

This partition should be present in the Remote Destination inbound Calling Search Space (CSS), which points to either the Inbound CSS of the Gateway or Trunk, or the Remote Destination CSS.

This feature does not use the remaining options on this page.

Step 5 Select **Save**.

Match Caller ID with Mobility Identity

To ensure that only authorized phones can initiate outbound calls, calls must originate from a phone that is set up in the system. To do this, the system attempts to match the caller ID of the requesting phone number with an existing Mobility Identity. By default, when a device initiates the Handoff feature, the caller ID that is passed from the gateway to Cisco Unified Communications Manager must exactly match the Mobility Identity number that you entered for that device.

However, your system may be set up such that these numbers do not match exactly. For example, Mobility Identity numbers may include a country code while caller ID does not. If so, you must set up the system to recognize a partial match.

Be sure to account for situations in which the same phone number may exist in different area codes or in different countries. Also, be aware that service providers can identify calls with a variable number of digits, which may affect partial matching. For example, local calls may be identified using seven digits (such as 555 0123) while out-of-area calls may be identified using ten digits (such as 408 555 0199).

Before you begin

Set up the Mobility Identity. See the *Add Mobility Identity* topic.

To determine whether you need to complete this procedure, perform the following steps. Dial in to the system from the mobile device and compare the caller ID value with the Destination Number in the Mobility Identity. If the numbers do not match, you must perform this procedure. Repeat this procedure for devices that are issued in all expected locales and area codes.

Procedure

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

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

Step 3 Select the active server.

Step 4 Select the **Cisco CallManager (Active)** service.

Step 5 Scroll down to the **Clusterwide Parameters (System - Mobility)** section.

Step 6 Select **Matching Caller ID with Remote Destination** and read essential information about this value.

Step 7 Select **Partial Match for Matching Caller ID with Remote Destination**.

Step 8 Select **Number of Digits for Caller ID Partial Match** and read the essential requirements for this value.

Step 9 Enter the required number of digits to ensure partial matches.

Step 10 Select **Save**.

Set Up User and Device Settings for Handoff

Before you begin

- Set up the user device on the Cisco Unified Communications Manager.
- Set up the user with a Mobility Identity.

Procedure

Step 1 In the **Cisco Unified CM Administration** interface, go to the TCT Device page, and select **Use Handoff DN Feature** for the **Transfer to Mobile Network** option.

Do not assign this method for iPod Touch devices. Use the Mobility Softkey method instead.

Step 2 In the **Cisco Unified CM Administration** interface, go to the BOT Device page, and select **Use Handoff DN Feature** for the **Transfer to Mobile Network** option.

Step 3 On the iOS device, tap **Settings** > **Phone** > **Show My Caller ID** to verify that Caller ID is on.

Step 4 On some Android device and operating system combinations, you can verify that the Caller ID is on. On the Android device, open the Phone application and tap **Menu** > **Call Settings** > **Additional settings** > **Caller ID** > **Show Number**.

Step 5 Test this feature.

Enable Transfer from VoIP to Mobile Network

Procedure

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

Step 2 For system-level settings, check that the Mobility softkey appears when the phone is in the connected and on-hook call states.

a) Select **Device** > **Device Settings** > **Softkey Template**.
b) Select the same softkey template that you selected when you configured the device for Mobile Connect.
c) In the **Related Links** drop-down list at the upper right, select **Configure Softkey Layout** and select **Go**.
d) In the call state drop-down list, select the On Hook state and verify that the Mobility key is in the list of selected softkeys.
e) In the call state drop-down list, select the Connected state and verify that the Mobility key is in the list of selected softkeys.

Step 3 Navigate to the device that you want to configure as follows:

a) Select **Device** > **Phone**.
b) Search for the device that you want to configure.
c) Select the device name to open the **Phone Configuration** window.

Step 4 For the per-user and per-device settings in Cisco Unified Communications Manager, set the specific device to use the Mobility softkey when the device transfers calls to the mobile voice network. Ensure that you have set up both Mobility Identity and Mobile Connect for the mobile device. After the transfer feature is working, users can enable and disable Mobile Connect at their convenience without affecting the feature.

If the device is an iPod Touch, you can configure a Mobility Identity using an alternate phone number such as the mobile phone of the user.

a) Select the **Owner User ID** on the device page.
b) Select the **Mobility User ID**. The value usually matches that of the Owner User ID.
c) In the Product Specific Configuration Layout section, for the Transfer to Mobile Network option, select **Use Mobility Softkey** or **Use HandoffDN Feature**.

Step 5 In the User Locale field, choose **English, United States**.

Step 6 Select **Save**.

Step 7 Select **Apply Config**.

Step 8 Instruct the user to sign out of the client and then to sign back in again to access the feature.

What to do next

Test your settings by transferring an active call from VoIP to the mobile network.

Dial via Office

Applies to: Cisco Jabber for Android, Cisco Jabber for iOS

Important User-controlled voicemail avoidance, which can be used in conjunction with the DvO feature, is available only on Cisco Unified Communications Manager release 9.0 and later. Timer-controlled voicemail avoidance is available on Cisco Unified Communications Manager release 6.0 and later.

The DvO feature is not supported when users connect to the corporate network using Expressway for Mobile and Remote Access.

The DvO feature allows users to initiate Cisco Jabber outgoing calls with their work number using the mobile voice network for the device.

Cisco Jabber supports DvO-R (DvO-Reverse) calls, which works as follows:

1. User initiates a DvO-R call.
2. The client notifies Cisco Unified Communications Manager to call the mobile phone number.
3. Cisco Unified Communications Manager calls and connects to the mobile phone number.
4. Cisco Unified Communications Manager calls and connects to the number that the user dialed.
5. Cisco Unified Communications Manager connects the two segments.
6. The user and the called party continue as with an ordinary call.

Incoming calls use either Mobile Connect or the Voice over IP, depending on which Calling Options the user sets on the client. Dial via Office does not require Mobile Connect to work. However, we recommend that you enable Mobile Connect to allow the native mobile number to ring when someone calls the work number. From the Cisco Unified Communications Manager user pages, users can enable and disable Mobile Connect, and adjust Mobile Connect behavior using settings (for example, the time of day routing and Delay Before

Ringing Timer settings). For information about setting up Mobile Connect, see the *Set Up Mobile Connect* topic.

The following table describes the calling methods used for incoming and outgoing calls. The calling method (VoIP, Mobile Connect, DvO-R, or native cellular call) varies depending on the selected Calling Options and the network connection.

Table 13: Calling Methods used with Calling Options over Different Network Connections

Connection	Calling Options					
	Voice over IP		**Mobile Voice Network**		**Autoselect**	
Corporate Wi-Fi	Outgoing: VoIP	Incoming: VoIP	Outgoing: DvO-R	Incoming: Mobile Connect	Outgoing: VoIP	Incoming: VoIP
Noncorporate Wi-Fi						
Mobile Network (3G, 4G)					Outgoing: DvO-R	Incoming: Mobile Connect
Phone Services are not registered	Outgoing Native Cellular Call					
	Incoming Mobile Connect					

To set up Dial via Office-Reverse (DvO-R), you must do the following:

1. Set up the Cisco Unified Communications Manager to support DvO-R. See the *Set Up Cisco Unified Communications Manager to Support DvO* topic for more information.
2. Enable DvO on each Cisco Dual Mode for iPhone device. See the *Set Up Dial via Office for Each Device* topic for more information.
3. Enable DvO on each Cisco Dual Mode for Android device. See the *Set Up Dial via Office for Each Device* topic for more information.

Set Up Cisco Unified Communications Manager to Support Dial via Office

To set up Cisco Unified Communications Manager to support Dial via Office-Reverse (DvO-R), perform the following procedures:

1. Complete one or both of the following procedures.
    - *Set Up Enterprise Feature Access Number*
    - *Set Up Mobility Profile*
2. Complete the *Verify Device COP File Version* procedure.

3. If necessary, create application dial rules to allow the system to route calls to the Mobile Identity phone number to the outbound gateway. Ensure that the format of the Mobile Identity phone number matches the application dial rules.

Set Up Enterprise Feature Access Number

Use this procedure to set up an Enterprise Feature Access Number for all Cisco Jabber calls that are made using Dial via Office-Reverse.

The Enterprise Feature Access Number is the number that Cisco Unified Communications Manager uses to call the mobile phone and the dialed number unless a different number is set up in Mobility Profile for this purpose.

Before you begin

- Reserve a Direct Inward Dial (DID) number to use as the Enterprise Feature Access Number (EFAN). This procedure is optional if you already set up a mobility profile.

- Determine the required format for this number. The exact value you choose depends on the phone number that the gateway passes (for example, 7 digits or 10 digits). The Enterprise Feature Access Number must be a routable number.

Procedure

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

Step 2 Select **Call Routing** > **Mobility** > **Enterprise Feature Access Number Configuration**.

Step 3 Select **Add New**.

Step 4 In the **Number** field, enter the Enterprise Feature Access number.

Enter a DID number that is unique in the system.

To support dialing internationally, you can prepend this number with \+.

Step 5 From the **Route Partition** drop-down list, choose the partition of the DID that is required for enterprise feature access.

This partition is set under **System** > **Service Parameters**, in the **Clusterwide Parameters (System - Mobility)** section, in the **Inbound Calling Search Space for Remote Destination** setting. This setting points either to the Inbound Calling Search Space of the Gateway or Trunk, or to the Calling Search Space assigned on the **Phone Configuration** window for the device.

If the user sets up the DvO Callback Number with an alternate number, ensure that you set up the trunk Calling Search Space (CSS) to route to destination of the alternate phone number.

Step 6 In the **Description** field, enter a description of the Mobility Enterprise Feature Access number.

Step 7 (Optional) Check the **Default Enterprise Feature Access Number** check box if you want to make this Enterprise Feature Access number the default for this system.

Step 8 Select **Save**.

Set Up Mobility Profile

Use this procedure to set up a mobility profile for Cisco Jabber devices. This procedure is optional if you already set up an Enterprise Feature Access Number.

Mobility profiles allow you to set up the Dial via Office-Reverse settings for a mobile client. After you set up a mobility profile, you can assign it to a user or to a group of users, such as the users in a region or location.

Procedure

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

Step 2 Select **Call Routing** > **Mobility** > **Mobility Profile**.

Step 3 In the **Mobility Profile Information** section, in the **Name** field, enter a descriptive name for the mobility profile.

Step 4 In the **Dial via Office-Reverse Callback** section, in the **Callback Caller ID** field, enter the caller ID for the callback call that the client receives from Cisco Unified Communications Manager.

Step 5 Click **Save**.

Verify Device COP File Version

Use the following procedure to verify that you are using the correct device COP file for this release of Cisco Jabber.

Procedure

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

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

Step 3 Click **Add New**.

Step 4 From the **Phone Type** drop-down list, choose **Cisco Dual Mode for iPhone**.

Step 5 From the **Phone Type** drop-down list, choose **Cisco Dual Mode for Android**.

Step 6 Click **Next**.

Step 7 Scroll down to the Product Specific Configuration Layout section, and verify that you can see the **Video Capabilities** drop-down list.

If you can see the **Video Capabilities** drop-down list, the COP file is already installed on your system.

If you cannot see the **Video Capabilities** drop-down list, locate and download the correct COP file.

Set Up Dial via Office for Each Device

Use the following procedures to set up Dial via Office - Reverse for each TCT device.

Use the following procedures to set up Dial via Office - Reverse for each BOT device.

1. Add a Mobility Identity for each user.
2. Enable Dial via Office on each device.

3. If you enabled Mobile Connect, verify that Mobile Connect works. Dial the desk phone extension and check that the phone number that is specified in the associated Mobile Identity rings.

Add Mobility Identity

Use this procedure to add a mobility identity to specify the mobile phone number of the mobile device as the destination number. This destination number is used by features such as Dial via Office or mobile connect.

You can specify only one number when you add a mobility identity. If you want to specify an alternate number such as a second mobile phone number for a mobile device, you can set up a remote destination. The mobility identity configuration characteristics are identical to those of the remote destination configuration.

Procedure

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

Step 2 Navigate to the device that you want to configure as follows:

a) Select **Device** > **Phone**.
b) Search for the device that you want to configure.
c) Select the device name to open the **Phone Configuration** window.

Step 3 In the **Associated Mobility Identity** section, select **Add a New Mobility Identity**.

Step 4 Enter the mobile phone number as the destination number.

You must be able to rout this number to an outbound gateway. Generally, the number is the full E.164 number.

Note If you enable the Dial via Office — Reverse feature for a user, you must enter a destination number for the user's mobility identity.

If you enable Dial via Office — Reverse and leave the destination number empty in the mobility identity:

- The phone service cannot connect if the user selects the **Autoselect** calling option while using a mobile data network and VPN.
- The phone service cannot connect if the user selects the **Mobile Voice Network** calling option on any type of network.
- The logs do not indicate why the phone service cannot connect.

Step 5 Enter the initial values for call timers.

These values ensure that calls are not routed to the mobile service provider voicemail before they ring in the client on the mobile device. You can adjust these values to work with the end user's mobile network. For more information, see the online help in Cisco Unified Communications Manager.

The following is an example of mobility Identity timers' information in Cisco Unified Communications Manager 9.x.

Setting	Suggested Initial Value
Answer Too Soon Timer	3000
Answer Too Late Timer	20000

Setting	Suggested Initial Value
Delay Before Ringing Timer	0 **Note** This setting does not apply to DvO-R calls.

The following is an example of mobility Identity timers' information in Cisco Unified Communications Manager 10.x.

Setting	Suggested Initial Value
Wait * before ringing this phone when my business line is dialed.*	0.0 seconds
Prevent this call from going straight to this phone's voicemail by using a time delay of * to detect when calls go straight to voicemail.*	3.0 seconds
Stop ringing this phone after * to avoid connecting to this phone's voicemail.*	20.0 seconds

Step 6 Do one of the following:

- Cisco Unified Communications Manager release 9 or earlier — Check the **Enable Mobile Connect** check box.
- Cisco Unified Communications Manager release 10 — Check the **Enable Single Number Reach** check box.

Step 7 If you are setting up the Dial via Office feature, in the Mobility Profile drop-down list, select one of the following options.

Option	Description
Leave blank	Choose this option if you want users to use the Enterprise Feature Access Number (EFAN).
Mobility Profile	Choose the mobility profile that you just created if you want users to use a mobility profile instead of an EFAN.

Step 8 Set up the schedule for routing calls to the mobile number.

Step 9 Select **Save**.

Enable Dial via Office on Each Device

Use this procedure to enable Dial via Office on each device.

Procedure

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

Step 2 Navigate to the device that you want to configure as follows:

a) Select **Device** > **Phone**.
b) Search for the device that you want to configure.
c) Select the device name to open the **Phone Configuration** window.

Step 3 In the **Device Information** section, check the Enable Cisco Unified Mobile Communicator check box.

Step 4 In the **Protocol Specific Information** section, in the **Rerouting Calling Search Space** drop-down list, select a Calling Search Space (CSS) that can route the call to the DvO callback number.

Step 5 In the **Product Specific Configuration Layout** section, set the **Dial via Office** drop-down list to **Enabled**.

Step 6 Select **Save**.

Step 7 Select **Apply Config**.

Step 8 Instruct the user to sign out of the client and then to sign back in again to access the feature.

Note DVO enabled devices may encounter issues registering with Cisco Unified Communications Manager. Resetting the device from the Cisco Unified Communications Manager administrative interface fixes this issue.

What to do next

Test this feature.

Voicemail Avoidance

Applies to: All clients

Voicemail avoidance is a feature that prevents calls from being answered by the mobile service provider voice mail. This feature is useful if a user receives a Mobile Connect call from the enterprise on the mobile device. It is also useful when an incoming DvO-R call is placed to the mobile device.

You can set up voicemail avoidance in one of two ways:

- **Timer-controlled**—(Default) With this method, you set timers on the Cisco Unified Communications Manager to determine if the call is answered by the mobile user or mobile service provider voicemail.
- **User-controlled**—With this method, you set Cisco Unified Communications Manager to require that a user presses any key on the keypad of the device to generate a DTMF tone before the call can proceed.

If you deploy DvO-R, Cisco recommends that you also set user-controlled voicemail avoidance. If you set user-controlled Voicemail Avoidance, this feature applies to both DvO-R and Mobile Connect calls.

For more information about voicemail avoidance, see the *Confirmed Answer and DvO VM detection* section in the *Cisco Unified Communications Manager Features and Services Guide* for your release.

Set Up Timer-Controlled Voicemail Avoidance

Set up the timer control method by setting the **Answer Too Soon Timer** and **Answer Too Late Timer** on either the Mobility Identity or the Remote Destination. For more information, see the *Add Mobility Identity* or *Add Remote Destination (Optional)* topics.

Before you begin

Timer-controlled voicemail avoidance is supported on Cisco Unified Communications Manager, release 6.0 and later.

Set Up User-Controlled Voicemail Avoidance

Important User-controlled voicemail avoidance is available on Cisco Unified Communications Manager, release 9.0 and later.

Set up User-Controlled Voicemail Avoidance as follows:

1. Set up Cisco Unified Communications Manager using the *Set Up Cisco Unified Communications Manager to Support Voicemail Avoidance* topic.
2. Set up the device using one of the following topics:
    - *Enable Voicemail Avoidance on Mobility Identity*
    - *Enable Voicemail Avoidance on Remote Destination*

Important Cisco does not support user-controlled voicemail avoidance when using DvO-R with alternate numbers that the end user sets up in the client. An alternate number is any phone number that the user enters in the DvO Callback Number field on the client that does not match the phone number that you set up on the user's Mobility Identity.

If you set up this feature with alternate numbers, the Cisco Unified Communications Manager connects the DvO-R calls even if the callback connects to a wrong number or a voicemail system.

Set Up Cisco Unified Communications Manager to Support Voicemail Avoidance

Use this procedure to set up the Cisco Unified Communications Manager to support user-controlled Voicemail Avoidance.

Procedure

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

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

Step 3 In the **Server** drop-down list, select the active Cisco Unified Communications Manager.

Step 4 In the **Service** drop-down list, select the **Cisco Call Manager (Active)** service.

Step 5 Configure the settings in the **Clusterwide Parameters (System - Mobility Single Number Reach Voicemail)** section.

Note The settings in this section are not specific to Cisco Jabber. For information about how to configure these settings, see the *Confirmed Answer and DvO VM detection* section in the *Cisco Unified Communications Manager Administrator Guide* for your release.

Step 6 Click **Save**.

Enable Voicemail Avoidance on Mobility Identity

Use this procedure to enable user-controlled voicemail avoidance for the end user's mobility identity.

Before you begin

- Set up the annunciator on the Cisco Unified Communications Manager. For more information, see the *Annunciator setup* section in the *Cisco Unified Communications Manager Administrator Guide* for your release.
- If you set up a Media Resource Group on the Cisco Unified Communications Manager, set up the annunciator on the Media Resource Group. For more information, see the *Media resource group setup* section in the *Cisco Unified Communications Manager Administrator Guide* for your release.

Procedure

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

Step 2 Navigate to the device that you want to configure as follows:

a) Select **Device** > **Phone**.
b) Search for the device that you want to configure.
c) Select the device name to open the **Phone Configuration** window.

Step 3 In the **Associated Mobility Identity** section, click the link for the Mobility Identity.

Note To ensure that the Voicemail Avoidance feature works correctly, the DvO Callback Number that the end user enters in the Cisco Jabber client must match the Destination Number that you enter on the Mobility Identity Configuration screen.

Step 4 Set the policies as follows:

- Cisco Unified Communications Manager release 9 — In the **Single Number Reach Voicemail Policy** drop-down list, select **User Control**.
- Cisco Unified Communications Manager release 10 without Dial via Office — In the **Single Number Reach Voicemail Policy** drop-down list, select **User Control**.
- Cisco Unified Communications Manager release 10 with Dial via Office
  - In the **Single Number Reach Voicemail Policy** drop-down list, select **Timer Control**.
  - In the **Dial-via-Office Reverse Voicemail Policy** drop-down list, select **User Control**.

Step 5 Click **Save**.

Enable Voicemail Avoidance on Remote Destination

Use this procedure to enable user-controlled voicemail avoidance for the end user's remote destination.

Before you begin

- Set up the annunciator on the Cisco Unified Communications Manager. For more information, see the *Annunciator setup* section in the Cisco Unified Communications Manager Administrator Guide for your release.
- If you set up a Media Resource Group on the Cisco Unified Communications Manager, set up the annunciator on the Media Resource Group. For more information, see the *Media resource group setup* section in the Cisco Unified Communications Manager Administrator Guide for your release.

Procedure

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

Step 2 Navigate to the device that you want to configure as follows:

a) Select **Device** > **Phone**.
b) Search for the device that you want to configure.
c) Select the device name to open the **Phone Configuration** window.

Step 3 In the **Associated Remote Destinations** section, click the link for the associated remote destination.

Step 4 Set the policies as follows:

- Cisco Unified Communications Manager release 9 — In the **Single Number Reach Voicemail Policy** drop-down list, select **User Control**.
- Cisco Unified Communications Manager release 10 without Dial via Office — In the **Single Number Reach Voicemail Policy** drop-down list, select **User Control**.
- Cisco Unified Communications Manager release 10 with Dial via Office
  - In the **Single Number Reach Voicemail Policy** drop-down list, select **Timer Control**.
  - In the **Dial-via-Office Reverse Voicemail Policy** drop-down list, select **User Control**.

Step 5 Click **Save**.

CHAPTER 7

Configure Voicemail

Configure Voicemail for Cloud-Based Deployments

Procedure

	Command or Action	Purpose
Step 1	Configure Voicemail, on page 237	
Step 2	Allow Users to Set Voicemail Server Settings, on page 237	

Configure Voicemail

To configure your voicemail settings, use the Cisco WebEx Administration Tool.

What to do next

Allow Users to Set Voicemail Server Settings, on page 237

Allow Users to Set Voicemail Server Settings

Select an option with the Cisco WebEx Administration Tool so that users can specify voicemail server settings in the client interface.

Before you begin

Configure Voicemail, on page 237

Procedure

Step 1 Open the Cisco WebEx Administration Tool.

Step 2 Select **Configuration** > **Unified Communications**.

Step 3 Select the **Voicemail** tab.

Step 4 Select **Allow user to enter manual settings**.

The user can access advanced voicemail settings in the **Voicemail Accounts** tab on the **Options** window in the client interface.

The user can access advanced voicemail settings in the client interface by tapping **Settings** > **Voicemail**.

Configure Voicemail for an On-Premises Deployment with Cisco Unified Communications Manager Release 9.x and Later

Procedure

	Command or Action	Purpose
Step 1	Configure Cisco Unity Connection for Use with Cisco Jabber, on page 239	Configure Cisco Unity Connection so that Cisco Jabber can access voicemail services.
Step 2	Add a Voicemail Service, on page 240	
Step 3	Add a Mailstore Service, on page 242	
Step 4	Apply Mailstore Service, on page 243	After you add a mailstore service, you must apply it to a service profile so that the client can retrieve the settings.
Step 5	Configure Retrieval and Redirection, on page 244	Configure retrieval so that users can access voice mail messages. Configure redirection so that users can send incoming calls to voicemail.
Step 6	Set a Voicemail Credentials Source, on page 245	
Step 7	Enable Enhanced Message Waiting Indicator, on page 246	This procedure applies only if you want to set up a basic voicemail account that allows users to dial in to their voice mailbox. This procedure is not required if you want to set up visual voicemail.

Configure Cisco Unity Connection for Use with Cisco Jabber

You must complete some specific steps to configure Cisco Unity Connection so that Cisco Jabber can access voicemail services. You should refer to the Cisco Unity Connection documentation for instructions on general tasks such as creating users, passwords, and provisioning users with voicemail access.

Remember Cisco Jabber connects to the voicemail service through a REST interface and supports Cisco Unity Connection release 8.5 or later.

Procedure

Step 1 Ensure the **Connection Jetty** and **Connection REST Service** services are started.

a) Open the **Cisco Unity Connection Serviceability** interface.
b) Select **Tools** > **Service Management**.
c) Locate the following services in the **Optional Services** section:

- **Connection Jetty**
- **Connection REST Service**

d) Start the services if required.

Step 2 Open the **Cisco Unity Connection Administration** interface.

Step 3 Edit user password settings.

a) Select **Users**.
b) Select the appropriate user.
c) Select **Edit** > **Password Settings**.
d) Select **Web Application** from the **Choose Password** menu.
e) Uncheck **User Must Change at Next Sign-In**.
f) Select **Save**.

Step 4 Provide users with access to the web inbox.

a) Select **Class of Service**.

The **Search Class of Service** window opens.

b) Select the appropriate class of service or add a new class of service.
c) Select **Allow Users to Use the Web Inbox and RSS Feeds**.
d) In the **Features** section, select **Allow Users to Use Unified Client to Access Voice Mail**.
e) Select all other options as appropriate.
f) Select **Save**.

Step 5 Select API configuration settings.

a) Select **System Settings** > **Advanced** > **API Settings**.

The **API Configuration** window opens.

b) Select the following options:

- **Allow Access to Secure Message Recordings through CUMI**
- **Display Message Header Information of Secure Messages through CUMI**
- **Allow Message Attachments through CUMI**

c) Select **Save**.

What to do next

If you have Cisco Unified Communications Manager release 9.x and later, Add a Voicemail Service, on page 240.

If you have Cisco Unified Communications Manager release 8.x, Add a Voicemail Server, on page 248.

Add a Voicemail Service

Add a voicemail service, to allow users to receive voice messages.

Before you begin

Configure Cisco Unity Connection for Use with Cisco Jabber, on page 239

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 In the **Find and List UC Services** window, select **Add New**.
UC Service Configuration window opens.

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

Step 5 Specify details for the voicemail service as follows:

- **Product Type** — Select **Unity Connection**.
- **Name** — Enter a descriptive name for the server, for example, PrimaryVoicemailServer.
- **Hostname/IP Address** — Enter the IP address or the fully qualified domain name (FQDN) of the voicemail server.
- **Port**—You do not need to specify a port number. By default, the client always uses port 443 to connect to the voicemail server. For this reason, any value you specify does not take effect.
- **Protocol Type**—You do not need to specify a value. By default, the client always uses HTTPS to connect to the voicemail server. For this reason, any value you specify does not take effect.

Step 6 Select **Save**.

What to do next

Apply a Voicemail Service, on page 241

Apply a Voicemail Service

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

Note Cisco Jabber does not read Voicemail UC Service Profile when it is deployed only in the Phone mode.

For Cisco Jabber to retrieve the voicemail server information, update the `jabber-config.xml` file with the voicemail parameters.

```
<Voicemail>

<VoicemailService_UseCredentialsFrom>phone</VoicemailService_UseCredentialsFrom>

<VoicemailPrimaryServer>X.X.X.X</VoicemailPrimaryServer>

</Voicemail>
```

After updating, upload the `jabber-config.xml` file to all the Cisco Unified Communications Manager TFTP servers and restart the TFTP service on TFTP server nodes. Then reset the Jabber client.

Before you begin

Add a Voicemail Service, on page 240

Procedure

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

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

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

Step 3 Find and select your service profile.

The **Service Profile Configuration** window opens.

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

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

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

b) For **Credentials source for voicemail service**, select one of the following:

- **Unified CM - IM and Presence** — Uses the instant messaging and presence credentials to sign in to the voicemail service. As a result, users do not need to enter their credentials for voicemail services in the client.

- **Web conferencing** — This option is not supported, it uses the conferencing credentials to sign in to the voicemail service. You cannot currently synchronize with conferencing credentials.
- **Not set** — This option is selected for Phone mode deployments.

Step 5 Click **Save**.

Step 6 Add users to the service profile.

a) Select **User Management** > **End User**.

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

b) Specify the appropriate filters in the **Find User where** field and then select **Find** to find a user.

c) Click the user in the list.

The **End User Configuration** window opens.

d) Under the **Service Settings** area, check the **Home Cluster** checkbox.

e) For Phone mode deployments, ensure the **Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)** option is not selected.

For all other deployments, check the **Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)** checkbox.

f) Select your service profile from the **UC Service Profile** drop-down list.

g) Click **Save**.

What to do next

Add a Mailstore Service, on page 242

Add a Mailstore Service

The mailstore service provides users with visual voicemail capabilities.

Before you begin

Apply a Voicemail Service, on page 241

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**.

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

Step 5 Provide details for the mailstore service as follows:

- **Name**—Enter a descriptive name for the server, for example, PrimaryMailStoreServer.

- **Hostname/IP Address**—Enter the IP address or the Fully Qualified Domain Name (FQDN) of the mailstore server.
- **Port**—You do not need to specify a port number. By default, the client always uses port 443 to connect to the mailstore server. For this reason, any value you specify does not take effect.
- **Protocol Type**—You do not need to specify a value. By default, the client always uses HTTPS to connect to the mailstore server. For this reason, any value you specify does not take effect.

Step 6 Select **Save**.

What to do next

Apply Mailstore Service, on page 243

Apply Mailstore Service

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

Before you begin

Add a Mailstore Service, on page 242

Procedure

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

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

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

Step 3 Find and select your service profile.

The **Service Profile Configuration** window opens.

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

a) Select up to three services from the following drop-down lists:
   - **Primary**
   - **Secondary**
   - **Tertiary**

b) Specify appropriate values for the following fields:
   - **Inbox Folder**
   - **Trash Folder**
   - **Polling Interval**

Step 5 Select **Save**.

What to do next

Configure Retrieval and Redirection, on page 244

Configure Retrieval and Redirection

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

Procedure

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

Step 2 Configure the voicemail pilot.

a) Select **Advanced Features** > **Voice Mail** > **Voice Mail Pilot**.

   The **Find and List Voice Mail Pilots** window opens.

b) Select **Add New**.

   The **Voice Mail Pilot Configuration** window opens.

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

Step 3 Add the voicemail pilot to the voicemail profile.

a) Select **Advanced Features** > **Voice Mail** > **Voice Mail Profile**.

   The **Find and List Voice Mail Profiles** window opens.

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

   The **Voice Mail Pilot Configuration** window opens.

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

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

a) Select **Device** > **Phone**.

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

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

   The **Phone Configuration** window opens.

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

e) Select the appropriate device number.

   The **Directory Number Configuration** window opens.

f) Locate the **Directory Number Settings** section.
g) Select the voicemail profile from the **Voice Mail Profile** drop-down list.
h) Select **Save**.

What to do next

Set a Voicemail Credentials Source, on page 245

Set a Voicemail Credentials Source

You can specify a voicemail credentials source for users.

Tip In hybrid cloud-based deployments, you can set a voicemail credentials source as part of your configuration file with the VoiceMailService_UseCredentialsForm parameter.

Before you begin

Configure Retrieval and Redirection, on page 244

Procedure

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

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

Step 3 Select the appropriate service profile to open the **Service Profile Configuration** window.

Step 4 In the **Voicemail Profile** section, select **Unified CM - IM and Presence** from the **Credentials source for voicemail service** drop-down list.

Note Do not select **Web Conferencing** from the **Credentials source for voicemail service** drop-down list. You cannot currently use conferencing credentials as a credentials source for voicemail services.

The user's instant messaging and presence credentials match the user's voicemail credentials. As a result, users do not need to specify their voicemail credentials in the client user interface.

What to do next

Important There is no mechanism to synchronize credentials between servers. If you specify a credentials source, you must ensure that those credentials match the user's voicemail credentials.

For example, you specify that a user's instant messaging and presence credentials match the user's Cisco Unity Connection credentials. The user's instant messaging and presence credentials then change. You must update the user's Cisco Unity Connection credentials to reflect that change.

Cloud-Based deployments can use the configuration file parameter VoicemailService_UseCredentialsFrom. Set this parameter to the value `phone` to use the Cisco Unified Communications Manager credentials to sign in to Cisco Unity Connection.

Enable Enhanced Message Waiting Indicator

This procedure applies only if you want to set up a basic voicemail account that allows users to dial in to their voice mailbox. This procedure is not required if you want to set up visual voicemail.

A Message Waiting Indicator (MWI) alerts users to the presence of new voice messages. Enhanced MWI provides a count of new voice messages on systems that support this feature. Users can call the voice messaging system to retrieve the messages.

Note To enable the basic MWI, follow the instructions in the Cisco Unified Communications Manager documentation for your release. There are no unique configurations for this client.

If your deployment supports Enhanced MWI, enable this option in the Cisco Unity Connection Administration portal.

Before you begin

Set a Voicemail Credentials Source, on page 245

Procedure

Step 1 Open the **Cisco Unity Connection Administration** interface.

Step 2 In the left pane, navigate to **Telephony Integrations** > **Phone System**.

Step 3 Select the link for the desired phone system.

Step 4 In the Message Waiting Indicators section, select the **Send Message Counts** check box.

Configure Voicemail for an On-Premises Deployment with Cisco Unified Communications Manager Release 8.6

Procedure

	Command or Action	Purpose
Step 1	Configure Cisco Unity Connection for Use with Cisco Jabber, on page 239	Configure Cisco Unity Connection so that Cisco Jabber can access voicemail services.
Step 2	Add a Voicemail Server, on page 248	
Step 3	Create a Mailstore, on page 249	
Step 4	Create a Voicemail Profile, on page 250	
Step 5	Configure Retrieval and Redirection, on page 244	Configure retrieval so that users can access voice mail messages. Configure redirection so that users can send incoming calls to voicemail.
Step 6	Set a Voicemail Credentials Source, on page 245	

Configure Cisco Unity Connection for Use with Cisco Jabber

You must complete some specific steps to configure Cisco Unity Connection so that Cisco Jabber can access voicemail services. You should refer to the Cisco Unity Connection documentation for instructions on general tasks such as creating users, passwords, and provisioning users with voicemail access.

Remember Cisco Jabber connects to the voicemail service through a REST interface and supports Cisco Unity Connection release 8.5 or later.

Procedure

Step 1 Ensure the **Connection Jetty** and **Connection REST Service** services are started.

a) Open the **Cisco Unity Connection Serviceability** interface.

b) Select **Tools** > **Service Management**.

c) Locate the following services in the **Optional Services** section:

- **Connection Jetty**
- **Connection REST Service**

d) Start the services if required.

Step 2 Open the **Cisco Unity Connection Administration** interface.

Step 3 Edit user password settings.

a) Select **Users**.
b) Select the appropriate user.
c) Select **Edit** > **Password Settings**.
d) Select **Web Application** from the **Choose Password** menu.
e) Uncheck **User Must Change at Next Sign-In**.
f) Select **Save**.

Step 4 Provide users with access to the web inbox.

a) Select **Class of Service**.

   The **Search Class of Service** window opens.

b) Select the appropriate class of service or add a new class of service.
c) Select **Allow Users to Use the Web Inbox and RSS Feeds**.
d) In the **Features** section, select **Allow Users to Use Unified Client to Access Voice Mail**.
e) Select all other options as appropriate.
f) Select **Save**.

Step 5 Select API configuration settings.

a) Select **System Settings** > **Advanced** > **API Settings**.

   The **API Configuration** window opens.

b) Select the following options:

   - **Allow Access to Secure Message Recordings through CUMI**
   - **Display Message Header Information of Secure Messages through CUMI**
   - **Allow Message Attachments through CUMI**

c) Select **Save**.

What to do next

If you have Cisco Unified Communications Manager release 9.x and later, Add a Voicemail Service, on page 240.

If you have Cisco Unified Communications Manager release 8.x, Add a Voicemail Server, on page 248.

Add a Voicemail Server

Complete the steps in this task to add your voicemail server on Cisco Unified Presence.

Before you begin

Configure Cisco Unity Connection for Use with Cisco Jabber, on page 239

Procedure

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

Step 2 Select **Application** > **Cisco Jabber** > **Voicemail Server**.

Note In some versions of Cisco Unified Presence, this path is as follows: **Application** > **Cisco Unified Personal Communicator** > **Voicemail Server**.

The **Find and List Voicemail Servers** window opens.

Step 3 Select **Add New**.

Step 4 Select **Unity Connection** from the **Server Type** drop-down list.

Step 5 Specify details in the **Voicemail Server Configuration** section as follows:

- **Name** — Enter a descriptive name for the server, for example, PrimaryVoicemailServer.
- **Hostname/IP Address** — Enter the IP address or the fully qualified domain name (FQDN) of the voicemail server.
- **Port** — You do not need to specify a port number. By default, the client always uses port 443 to connect to the voicemail server. For this reason, any value you specify does not take effect.
- **Protocol Type** — You do not need to specify a value. By default, the client always uses HTTPS to connect to the voicemail server. For this reason, any value you specify does not take effect.

Step 6 Select **Save**.

What to do next

Create a Mailstore, on page 249

Related Topics

Configuring Voicemail Server Names and Addresses on Cisco Unified Presence

Create a Mailstore

Complete the steps in this task to create a mailstore on Cisco Unified Presence.

Before you begin

Ensure that you have Cisco Unified Communications Manager release 8.x and Cisco Unified Presence.

If you have Cisco Unified Communications Manager release 9.x or later, see Add a Mailstore Service, on page 242.

Procedure

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

Step 2 Depending on your version of Cisco Unified Presence, select one of the following paths:

- **Application** > **Cisco Jabber** > **Mailstore**
- **Application** > **Cisco Unified Personal Communicator** > **Mailstore**

The **Find and List Mailstore Servers** window opens.

Step 3 Select **Add New**.
The **Mailstore Configuration** window opens.

Step 4 Specify details as follows:

- **Name**—Enter a descriptive name for the server, for example, PrimaryMailStoreServer.
- **Hostname/IP Address**—Enter the hostname, IP Address, or Fully Qualified Domain Name (FQDN) of the mailstore server.
- **Port**—You do not need to specify a port number. By default, the client always uses port 443 to connect to the mailstore server. For this reason, any value you specify does not take effect.
- **Protocol Type**—You do not need to specify a value. By default, the client always uses HTTPS to connect to the mailstore server. For this reason, any value you specify does not take effect.

Step 5 Select **Save**.

Create a Voicemail Profile

After you add a voicemail server, you must create a voicemail profile and add that server to the profile.

Before you begin

Create a Mailstore, on page 249

Procedure

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

Step 2 Depending on your version of Cisco Unified Presence, select one of the following:

- **Application** > **Cisco Jabber** > **Voicemail Profile**
- **Application** > **Cisco Unified Personal Communicator** > **Voicemail Profile**

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

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

Step 4 Specify the required details.

Step 5 Add users to the voicemail profile as follows:

a) Select **Add Users to Profile**.
b) To retrieve a list of users, in the **Find User where** field, specify the appropriate filters and then select **Find**.
c) Select the appropriate users from the list.
d) Select **Add Selected**.

The selected users are added to the voicemail profile.

Step 6 Select **Save**.

What to do next

Configure Retrieval and Redirection, on page 244

Configure Retrieval and Redirection

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

Procedure

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

Step 2 Configure the voicemail pilot.

a) Select **Advanced Features** > **Voice Mail** > **Voice Mail Pilot**.

   The **Find and List Voice Mail Pilots** window opens.

b) Select **Add New**.

   The **Voice Mail Pilot Configuration** window opens.

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

Step 3 Add the voicemail pilot to the voicemail profile.

a) Select **Advanced Features** > **Voice Mail** > **Voice Mail Profile**.

   The **Find and List Voice Mail Profiles** window opens.

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

   The **Voice Mail Pilot Configuration** window opens.

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

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

a) Select **Device** > **Phone**.

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

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

   The **Phone Configuration** window opens.

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

e) Select the appropriate device number.

The **Directory Number Configuration** window opens.

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

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

h) Select **Save**.

What to do next

Set a Voicemail Credentials Source, on page 245

Set a Voicemail Credentials Source

You can specify a voicemail credentials source on Cisco Unified Presence.

Tip In hybrid cloud-based deployments, you can set a voicemail credentials source as part of your configuration file with the VoiceMailService_UseCredentialsFrom parameter. See the *Installation and Configuration Guide* for more information.

Procedure

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

Step 2 Select **Application** > **Cisco Jabber** > **Settings**.

In some versions of Cisco Unified Presence this path is as follows: **Application** > **Cisco Unified Personal Communicator** > **Settings**

Step 3 In the **Cisco Jabber Settings** section, select **CUP** from the **Credentials source for voicemail service** drop-down list.

Note Do not select **Web Conferencing** from the **Credentials source for voicemail service** drop-down list. You cannot currently use conferencing credentials as a credentials source for voicemail services.

The user's credentials for Cisco Unified Presence match the user's voicemail credentials. As a result, users do not need to specify their voicemail credentials in the client user interface.

What to do next

Important There is no mechanism to synchronize credentials between servers. If you specify a credentials source, you must ensure that those credentials match the user's voicemail credentials.

For example, you specify that a user's Cisco Unified Presence credentials match the user's Cisco Unity Connection credentials. The user's Cisco Unified Presence credentials then change. You must update the user's Cisco Unity Connection credentials to reflect that change.

Enable Enhanced Message Waiting Indicator

This procedure applies only if you want to set up a basic voicemail account that allows users to dial in to their voice mailbox. This procedure is not required if you want to set up visual voicemail.

A Message Waiting Indicator (MWI) alerts users to the presence of new voice messages. Enhanced MWI provides a count of new voice messages on systems that support this feature. Users can call the voice messaging system to retrieve the messages.

Note To enable the basic MWI, follow the instructions in the Cisco Unified Communications Manager documentation for your release. There are no unique configurations for this client.

If your deployment supports Enhanced MWI, enable this option in the Cisco Unity Connection Administration portal.

Before you begin

Set a Voicemail Credentials Source, on page 245

Procedure

Step 1 Open the **Cisco Unity Connection Administration** interface.

Step 2 In the left pane, navigate to **Telephony Integrations** > **Phone System**.

Step 3 Select the link for the desired phone system.

Step 4 In the Message Waiting Indicators section, select the **Send Message Counts** check box.

CHAPTER 8

Configure Conferencing

Configure Conferencing for an On-Premises Deployment

When you implement an on-premises deployment for Cisco Jabber, you can configure conferencing on-premises with Cisco Webex Meetings Server, or in the cloud in Cisco Webex Meetings Center.

Configure On-Premises Conferencing using WebEx Meetings Server

Procedure

	Command or Action	Purpose
Step 1	Authenticate with Cisco WebEx Meetings Server , on page 255.	
Step 2	Add Cisco Webex Meetings Server on Cisco Unified Communications Manager, on page 256.	Complete this task if you have Cisco Unified Communications Manager release 9.x and later.
Step 3	Add Cisco WebEx Meetings Server on Cisco Unified Presence, on page 258.	Complete this task if you have Cisco Unified Communications Manager Release 8.6 and Cisco Unified Presence.

Cisco WebEx Meetings Server Installation and Configuration

The first step in setting up integration between Cisco WebEx Meetings Server and the client is to install and configure Cisco WebEx Meetings Server. You should refer to the Cisco WebEx Meetings Server product documentation for installation and configuration procedures.

Authenticate with Cisco WebEx Meetings Server

Cisco Jabber supports the following methods of authentication with Cisco WebEx Meetings Server:

Users manually enter credentials in the client

For Cisco Jabber for Windows, each user can enter their credentials in the **Options** window to authenticate directly with Cisco WebEx Meetings Server.

For Cisco Jabber for Mac, each user can enter their credentials in the **Meetings** tab on the **Preferences** window to authenticate directly with Cisco WebEx Meetings Server.

You set a credentials source on Cisco Unified Communications Manager

If the users' credentials for Cisco WebEx Meetings Server match their credentials for Cisco Unified Communications Manager IM and Presence Service or Cisco Unity Connection, you can set a credentials source. The client then automatically authenticates to Cisco WebEx Meetings Server with the users' credential source.

You configure single sign-on (SSO) with Cisco WebEx Meetings Server

If you configure SSO with Cisco WebEx Meetings Server, Cisco Jabber can seamlessly integrate with the SSO environment. In this case, you do not need to specify credentials in order for users to authenticate with Cisco WebEx Meetings Server.

Add Cisco Webex Meetings Server on Cisco Unified Communications Manager

To configure conferencing on Cisco Unified Communications Manager, you must add a Cisco Webex Meetings Server.

Before you begin

Authenticate with Cisco Webex Meetings Server

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface and select **User Management** > **User Settings** > **UC Service**.
The **Find and List UC Services** window opens.

Step 2 Select **Add New**.

Step 3 In the **Add a UC Service** section, from the **UC Service Type** drop-down list, select **Conferencing** and then select **Next**.

Step 4 Complete the following fields:

- **Product Type** — Select Webex **(Conferencing)**.
- **Name** — Enter a name for the configuration. The name you specify is displayed when you add services to profiles. Ensure the name you specify is unique, meaningful, and easy to identify.
- **Hostname/IP Address** — Enter the site URL for Cisco Webex MeetingsServer. This URL is case sensitive and must match the case that was configured for the site URL in Cisco Webex Meetings Server.
- **Port** — Leave the default value.
- **Protocol** — Select **HTTPS**.

Step 5 To use Cisco Webex as the single sign-on (SSO) identity provider, check **User web conference server as SSO identity provider**.

Note This field is available only if you select Webex **(Conferencing)** from the **Product Type** drop-down list.

Step 6 Select **Save**.

What to do next

Add the Cisco Webex Meetings Server to a Service Profile, on page 257

Add the Cisco Webex Meetings Server to a Service Profile

After you add Cisco Webex Meetings Server and add it to a service profile, the client can access conferencing features.

Before you begin

Create a service profile.

Add Cisco Webex Meetings Server on Cisco Unified Communications Manager, on page 256

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface and select **User Management** > **User Settings** > **Service Profile**

Step 2 Find and select your service profile.

Step 3 In the **Conferencing Profile** section, from the **Primary**, **Secondary**, and **Tertiary** drop-down lists, select up to three instances of Cisco Webex Meetings Server.

Step 4 From the **Server Certificate Verification** drop-down list, select the appropriate value.

Step 5 From the **Credentials source for web conference service** drop-down list, select one of the following:

- **Not set**—Select this option if the user does not have a credentials source that matches their Cisco Webex Meetings Server credentials or if you use SSO at the meeting site.
- **Unified CM - IM and Presence**—Select this option if the Cisco Unified Communications Manager IM and Presence Service credentials for the user match their Cisco Webex Meetings Server credentials.
- **Voicemail**—Select this option if the Cisco Unity Connection credentials for the user match their Cisco Webex Meetings Server credentials.

Note You cannot synchronize the credentials you specify in Cisco Unified Communications Manager with credentials you specify in Cisco Webex Meetings Server. For example, if you specify that instant messaging and presence credentials for a user are synchronized with their Cisco Webex Meetings Server credentials, the instant messaging and presence credentials for that user change. You must update the Cisco Webex Meetings Server credentials for that user to match that change.

Step 6 Select **Save**.

Set Up Cisco WebEx Meetings Server on Cisco Unified Presence

The client retrieves Cisco WebEx Meetings Server details from the conferencing profile on Cisco Unified Presence. You must add your details for Cisco WebEx Meetings Server, add Cisco WebEx Meetings Server to a profile, and then add users to the profile.

Add Cisco WebEx Meetings Server on Cisco Unified Presence

Before you begin

Add the Cisco Webex Meetings Server to a Service Profile, on page 257

Procedure

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

Step 2 Depending on your version of Cisco Unified Presence, select one of the following:.

- **Application** > **Cisco Jabber** > **Conferencing Server**
- **Application** > **Cisco Unified Personal Communicator** > **Conferencing Server**

Step 3 Select **Add New**.
The **Conferencing Server Configuration** window opens.

Step 4 Complete the following fields:

- **Name** — Enter a name for the configuration. The name is displayed when you add services to profiles.
- **Hostname/IP Address** — Enter the site URL for Cisco WebEx Meetings Server.
- **Port** — Accept the default value.
- **Protocol** — Select **HTTPS**.
- **Server Type** — Select **WebEx**.
- **Site ID** — You do not need to specify a value for this field.
- **Partner ID** — You do not need to specify a value for this field.

Step 5 Select **Save**.

What to do next

Add Cisco WebEx Meetings Server to a Profile, on page 258

Add Cisco WebEx Meetings Server to a Profile

After you add Cisco WebEx Meetings Server on Cisco Unified Presence and add it to a service profile, the client can access conferencing features.

Before you begin

Add Cisco WebEx Meetings Server on Cisco Unified Presence, on page 258

Procedure

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

Step 2 Depending on your version of Cisco Unified Presence, select one of the following:

- **Application** > **Cisco Jabber** > **Conferencing Profile**
- **Application** > **Cisco Unified Personal Communicator** > **Conferencing Profile**

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

Step 4 Complete the following fields:

- **Name** — Enter a name for the configuration.
- **Description** — Enter an optional description.
- **Primary Conferencing Server** — Select the primary instance of Cisco WebEx Meetings Server.
- **Backup Conferencing Server** — Select the backup instance of Cisco WebEx Meetings Server.

Step 5 From the **Server Certificate Verification** drop-down list, select one of the following:

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

Step 6 To set this profile as the system default, check **Make this the default Conferencing Profile for the system**.

Step 7 In the **Users in Profile** section, select **Add Users to Profile**.

Step 8 In the **Find and List Users** window, select **Find** to retrieve a list of users.

Step 9 Select the appropriate users from the list and then select **Add Selected**.
The selected users are added to the profile.

Step 10 Select **Save**.

Configure Cloud-Based Conferencing Using WebEx Meeting Center

Procedure

	Command or Action	Purpose
Step 1	Integration with Cisco WebEx Meeting Center, on page 260.	
Step 2	Authentication with Cisco WebEx Meeting Center, on page 260.	Authenticate the client with Cisco WebEx Meeting Center using tightly coupled integration.
Step 3	Provide Conferencing Credentials, on page 260.	Provide conferencing credentials to the client.

	Command or Action	Purpose
Step 4	Depending on your version of Cisco Unified Communications Manager, select one of the following: • If you have Cisco Unified Communications Manager release 9.x and later with Cisco Unified Communications Manager IM and Presence Service, Add Cisco WebEx Meeting Center, on page 260. • If you have Cisco Unified Communications Manager Release 8.6 with Cisco Unified Presence, Set Up Cisco WebEx Meeting Center on Cisco Unified Presence , on page 262.	

Integration with Cisco WebEx Meeting Center

To integrate with Cisco WebEx Meeting Center in an on-premises deployment, select one of the following integration options:

- Cloud-based integration — Cisco WebEx Meeting Center provides data, such as participant chat and roster lists, and audio and video capabilities.
- Hybrid cloud-based integration — Cisco WebEx Meeting Center provides data, such as participant chat and roster lists, and a conferencing bridge provides audio and video capabilities.

Authentication with Cisco WebEx Meeting Center

You can authenticate the client with Cisco WebEx Meeting Center using tightly coupled integration. Tightly coupled integration refers to a configuration that you set up between Cisco WebEx Messenger and Cisco WebEx Meeting Center. When users authenticate with Cisco WebEx Messenger, it passes an authentication token back to the client. The client then passes that authentication token to Cisco WebEx Meeting Center. See the *Overview of Tightly Coupled Integration* topic for more information.

Provide Conferencing Credentials

Choose one of the following methods to provide conferencing credentials to the client:

- Users individually specify their credentials in the **Options** window.
- Users individually specify their credentials in the **Meetings** tab on the **Preferences** window.
- You specify a credentials source on Cisco Unified Communications Manager when you apply the conferencing service to the service profile. See the topic in this section that describes how to add the conferencing server to the service profile for instructions.

Add Cisco WebEx Meeting Center

The first step to setting up conferencing on Cisco Unified Communications Manager is to add your details for Cisco WebEx Meeting Center.

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**.

Step 4 In the **Add a UC Service** section, from the **UC Service Type** drop-down list, select **Conferencing** and then select **Next**.

Step 5 Complete the following fields:

- **Product Type** — Select **WebEx (Conferencing)**.
- **Name** — Enter a name for the configuration. The name is displayed when you add services to profiles. Ensure the name you specify is unique, meaningful, and easy to identify.
- **Description** — Enter an optional description.
- **Host Name/IP Address** — Enter the Cisco WebEx Meeting Center site hostname. Do not enter an IP address.
- **Port** — Enter the Cisco WebEx Meeting Center site port number.
- **Protocol** — Select **HTTPS**.

Step 6 To use Cisco WebEx as the single sign-on (SSO) identity provider, check**User web conference server as SSO identity provider**.

Note This field is available only if you select **WebEx (Conferencing)** as the **Product Type**.

Step 7 Select **Save**.

What to do next

Add Cisco WebEx Meeting Center to a service profile.

Add Cisco WebEx Meeting Center to a Profile

After you add Cisco WebEx Meeting Center on Cisco Unified Communications Manager, you add Cisco WebEx Meeting Center to a service profile. The client can then retrieve the details for Cisco WebEx Meeting Center from the profile and access the conferencing features.

Before you begin

Create a service profile.

Procedure

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

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

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

Step 3 Find and select your service profile.

The **Service Profile Configuration** window opens.

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

a) Select your service from the **Primary** drop-down list.

Note The client uses only the service you select from the **Primary** drop-down list. You do not need to select services from the **Secondary** or **Tertiary** drop-down lists.

b) Select the appropriate value from the **Server Certificate Verification** drop-down list.

c) Select one of the following from the **Credentials source for web conference service** drop-down list:

- Not set — The user does not have a credentials source that matches their Cisco WebEx Meeting Center credentials.
- Unified CM - IM and Presence — The user's Cisco Unified Communications Manager IM and Presence Service credentials match their Cisco WebEx Meeting Center credentials.
- Voicemail — The user's Cisco Unity Connection credentials match their Cisco WebEx Meeting Center credentials.

Restriction You cannot specify a credentials source if you use an identity provider for authentication with Cisco WebEx Meeting Center.

Important If you select a credentials source, you must ensure that those credentials match the user's Cisco WebEx Meeting Center credentials.

There is no mechanism to synchronize the credentials you specify in Cisco Unified Communications Manager with credentials you specify in Cisco WebEx Meeting Center. For example, you specify that a user's instant messaging and presence credentials are synchronized with the user's Cisco WebEx Meeting Center credentials. The user's instant messaging and presence credentials then change. You must update the user's Cisco WebEx Meeting Center credentials to match that change.

Step 5 Select **Save**.

Set Up Cisco WebEx Meeting Center on Cisco Unified Presence

The client retrieves Cisco WebEx Meeting Center details from the conferencing profile on Cisco Unified Presence. You must add:

- Details for Cisco WebEx Meeting Center
- A Cisco WebEx Meeting Center profile
- Users to the Cisco WebEx Meeting Center profile

Add Cisco WebEx Meeting Center

The first step to setting up conferencing on Cisco Unified Presence is to add your details for Cisco WebEx Meeting Center.

Procedure

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

Step 2 Select **Application** > **Cisco Jabber** > **Conferencing Server**.

In some versions of Cisco Unified Presence, this path is as follows: **Application** > **Cisco Unified Personal Communicator** > **Conferencing Server**.

Step 3 Select **Add New**.

The **Conferencing Server Configuration** window opens.

Step 4 Specify details for Cisco WebEx Meeting Center in the following fields:

- Name — Enter a name for the configuration. The name you specify displays when you add services to profiles.
- Hostname/IP Address — Specify the hostname of the Cisco WebEx Meeting Center site.

  Note You must specify a hostname, not an IP address.

- Port — Specify a port number for the Cisco WebEx Meeting Center site.
- Protocol — Select **HTTPS** from the drop-down list.
- Server Type — Select **WebEx** from the drop-down list.
- Site ID — Specify the optional primary site ID for Cisco WebEx Meeting Center.
- Partner ID — Specify the optional appropriate partner ID for Cisco WebEx Meeting Center.

Step 5 Select **Save**.

Add Cisco WebEx Meeting Center to a Profile

After you add Cisco WebEx Meeting Center on Cisco Unified Presence, you add Cisco WebEx Meeting Center to a conferencing profile. The client can then retrieve the details for Cisco WebEx Meeting Center from the profile and access the conferencing features.

Procedure

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

Step 2 Select **Application** > **Cisco Jabber** > **Conferencing Profile**.

In some versions of Cisco Unified Presence, this path is as follows: **Application** > **Cisco Unified Personal Communicator** > **Conferencing Profile**.

Step 3 Select **Add New**.

The **Conferencing Profile Configuration** window opens.

Step 4 Specify details for the profile in the following fields:

- **Name** — Enter a name for the configuration.
- **Description** — Enter an optional description.
- **Primary Conferencing Server** — Select the primary Cisco WebEx Meeting Center site from the drop-down list.

  Note The client uses only the site you select from the **Primary Conferencing Server** drop-down list. You do not need to select a site from the **Backup Conferencing Server** drop-down list.

- **Server Certificate Verification** — Select one of the following from the drop-down list:
  - **Any Certificate**
  - **Self Signed or Keystore**
  - **Keystore Only**

Step 5 Select the **Make this the default Conferencing Profile for the system** checkbox to set this profile as the system default.

Step 6 Add users to the conferencing profile as follows:

a) Select **Add Users to Profile** in the **Users in Profile** section.

The **Find and List Users** dialog box opens.

b) Select **Find** to retrieve a list of users.
c) Select the appropriate users from the list.
d) Select **Add Selected**.

The selected users are added to the profile and the **Find and List Users** dialog box closes.

Step 7 Select **Save**.

Configure Conferencing for Cloud-Based Deployments

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.

You can add more Cisco WebEx meeting sites in the Cisco Jabber client. However, you cannot add a meeting site that is configured for SSO, this site must be created in the Cisco WebEx Administration Tool.

Authentication with Cisco WebEx Meeting Center

- Tightly Coupled Integration with the Cisco WebEx Messenger Service — Tightly coupled integration refers to a configuration that you set up between Cisco WebEx Messenger and Cisco WebEx Meeting Center.

  When users authenticate with Cisco WebEx Messenger, it passes an authentication token back to the client. The client then passes that authentication token to Cisco WebEx Meeting Center.

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

- Authentication with an Identity Provider — The client can redirect authentication from Cisco WebEx Meeting Center to an identity provider.

  To enable authentication with an identity provider, complete the following steps:

  1. Set up your identity provider as appropriate.

     When users attempt to authenticate with Cisco WebEx Meeting Center, the client redirects that authentication to your identity provider. Your identity provider then validates the credentials and passes an authentication token back to the client. The client then passes that token to Cisco WebEx Meeting Center to complete the authentication process.

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

  See the *Using SSO with the Cisco WebEx and Cisco WebEx Meeting applications* topic for more information about managing user identities with the Cisco WebEx Messenger service.

You can authenticate the client with Cisco WebEx Meeting Center using tightly coupled integration. Tightly coupled integration refers to a configuration that you set up between Cisco WebEx Messenger and Cisco WebEx Meeting Center. When users authenticate with Cisco WebEx Messenger, it passes an authentication token back to the client. The client then passes that authentication token to Cisco WebEx Meeting Center. See the *Overview of Tightly Coupled Integration* topic for more information.

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**.

Users can specify their credentials in the **Settings**.

On the **Settings** screen, under **Accounts**, tap **WebEx Meeting**.

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

CHAPTER 9

Configure Directory Integration

Client Configuration for Directory Integration

You can configure directory integration through service profiles using Cisco Unified Communications Manager release 9 or later or with the configuration file. Use this section to learn how to configure the client for directory integration.

When both a service profile and a configuration file are present, the following table describes which parameter value takes precedence.

Service Profile	Configuration File	Which Parameter Value Takes Precedence?
Parameter value is set	Parameter value is set	Service profile
Parameter value is set	Parameter value is blank	Service profile
Parameter value is blank	Parameter value is set	Configuration file
Parameter value is blank	Parameter value is blank	Service profile blank (default) value

Note Cisco Unified Presence, Release 8.x profiles cannot be used for directory integration.

When to Configure Directory Integration

Note Install Cisco Jabber for Windows on a workstation that is registered to an Active Directory domain. In this environment, you do not need to configure Cisco Jabber for Windows to connect to the directory. The client automatically discovers the directory and connects to a Global Catalog server in that domain.

Configure Cisco Jabber to connect to a directory services if you plan to use one of the following services as the contact source:

- Domain Controller
- Cisco Unified Communications Manager User Data Service
- OpenLDAP
- Active Directory Lightweight Directory Service
- Active Directory Application Mode

You can optionally configure directory integration to:

- Change the default attribute mappings.
- Adjust directory query settings.
- Specify how the client retrieves contact photos.
- Perform intradomain federation.

Configure Directory Integration in a Service Profile

With Cisco Unified Communications Manager version 9 and higher, you can provision users with service profiles and deploy the `_cisco-uds` SRV record on your internal domain name server.

The client can then automatically discover Cisco Unified Communications Manager and retrieve the service profile to get directory integration configuration.

To set up service discovery to support service profiles, you must:

- Deploy the `_cisco-uds` SRV record on your internal domain name server.
- Ensure that the client can resolve the domain name server address.
- Ensure that the client can resolve the hostname of Cisco Unified Communications Manager.
- Ensure that the client can resolve the fully qualified domain name (FQDN) for the Cisco Unified Communications Manager.

Cisco Jabber now supports Cisco Unified Communications Manager User Data Service (UDS). In addition to being able to deploy Cisco Jabber using LDAP to connect to Active Directory, Jabber can now alternatively be deployed with Cisco Unified Communications Manager User Data Services contact lookup service. Server scaling must be considered when using the UDS server. A Cisco Unified Communication node can support UDS contact service connections for 50% of the maximum device registrations supported by the server.

To configure directory integration in a service profile, do the following:

Procedure

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

Step 2 Add a directory service.

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

b) Select **Add New**.
The **UC Service Configuration** window opens.

c) Select **Directory** from the **UC Service Type** menu and then select **Next**.
d) Set all appropriate values for the directory service and then select **Save**.

Step 3 Apply the directory service to a service profile.

a) Select **User Management** > **User Settings** > **Service Profile**.
The **Find and List Service Profiles** window opens.
b) Select **Add New**.
The **Service Profile Configuration** window opens.
c) Add the directory services to the directory profile.
d) Select **Save**.

When both the directory profile and `jabber-config.xml` file are used at the same time, the configuration in the directory profile have the higher priority and will be used except manual sign-in and service discovery.

To make it work consistently, it is highly recommended that **Username** and **Password** in both directory profile and `jabber-config.xml` are exactly the same.

Directory Profile Parameters

The following table lists the configuration parameters you need to set in the directory profile:

Directory Service Configuration	Description
Primary server	Specifies the address of the primary directory server. This parameter is required for manual connections where the client cannot automatically discover the directory server.
Username	Lets you manually specify a shared username that the client can use to authenticate with the directory server. You should use this parameter only in deployments where you cannot authenticate with the directory server using Microsoft Windows credentials. If you must use this parameter, you should use only a well-known or public set of credentials. The credentials should also be linked to an account that has read-only permissions.
Password	Lets you manually specify a shared password that the client can use to authenticate with the directory server. You should use this parameter only in deployments where you cannot authenticate with the directory server using Microsoft Windows credentials. If you must use this parameter, you should use only a well-known or public set of credentials. The credentials should also be linked to an account that has read-only permissions.

Directory Service Configuration	Description
Search Base 1	Specifies a location in the directory server from which searches begin. In other words, a search base is the root from which the client executes a search. By default, the client searches from the root of the directory tree. You can specify the value of up to three search bases in your OU to override the default behavior. Active Directory does not typically require a search base. You should specify search bases for Active Directory only for specific performance requirements. You must specify a search base for directory servers other than Active Directory to create bindings to specific locations in the directory. **Tip** Specify an OU to restrict searches to certain user groups. For example, a subset of your users have instant messaging capabilities only. Include those users in an OU and then specify that as a search base.

Attribute Mappings

It is not possible to change the default attribute mappings in a service profile. If you plan to change any default attribute mappings, you must define the required mappings in a client configuration file.

Summary of Directory Integration Configuration Parameters

The following tables are a summary of all directory integration parameters.

Attribute Mapping

These parameters are used for attribute mapping with LDAP directory servers.

BDI Parameters	EDI Parameters
• BDICommonName • BDIDisplayName • BDIFirstname • BDILastname • BDIEmailAddress • BDISipUri • BDIPhotoSource • BDIBusinessPhone • BDIMobilePhone • BDIHomePhone • BDIOtherPhone • BDIDirectoryUri • BDITitle • BDICompanyName • BDIUserAccountName • BDIDomainName • BDICountry • BDILocation • BDINickname • BDIPostalCode • BDICity • BDIState • BDIStreetAddress	• CommonName • DisplayName • Firstname • Lastname • EmailAddress • SipUri • PhotoSource • BusinessPhone • MobilePhone • HomePhone • OtherPhone • DirectoryUri • Title • CompanyName • UserAccountName • DomainName • Location • Nickname • PostalCode • City • State • StreetAddress

Directory Server Connection

These parameters are used for connecting to LDAP directory servers.

BDI Parameters	EDI Parameters
• BDILDAPServerType • BDIPresenceDomain • BDIPrimaryServerName • BDIServerPort1 • BDIUseJabberCredentials • BDIConnectionUsername • BDIConnectionPassword • BDIEnableTLS	• DirectoryServerType • ConnectionType • PrimaryServerName • SecondaryServerName • ServerPort1 • ServerPort2 • UseWindowsCredentials • ConnectionUsername • ConnectionPassword • UseSSL • UseSecureConnection

Contact Resolution and Directory Query

These parameters are used for contact resolution and directory queries with LDAP directory servers.

BDI Parameters	EDI Parameters
• BDIBaseFilter • BDIGroupBaseFilter • BDIUseANR • BDIPredictiveSearchFilter • BDISearchBase1 • BDIPhotoUriSubstitutionEnabled • BDIPhotoUriSubstitutionToken • BDIPhotoUriWithToken • BDIUseSIPURIToResolveContacts • BDIUriPrefix • BDIDirectoryUri • BDIDirectoryUriPrefix	• BaseFilter • GroupBaseFilter • PredictiveSearchFilter • DisableSecondaryNumberLookups • PhoneNumberMasks • SearchTimeout • UseWildcards • MinimumCharacterQuery • SearchBase1, SearchBase2, SearchBase3, SearchBase4, and SearchBase5 • PhotoUriSubstitutionEnabled • PhotoUriSubstitutionToken • PhotoUriWithToken • UseSIPURIToResolveContacts • UriPrefix • DirectoryUri • DirectoryUriPrefix

UDS

These parameters are used for interacting with UDS as a contact source.

- DirectoryServerType
- PresenceDomain
- UdsServer
- UdsPhotoUriWithToken

Directory Server Type Parameter

You specify the directory server type with the following parameter in the `jabber-config.xml` file:

Parameter	Value	Description
DirectoryServerType	BDI EDI UDS	Specifies the type of directory server to use. • BDI — Connect to a LDAP server. • EDI — Connect to a LDAP server. • UDS — Connect to UDS.

Directory Integration Parameters

The following sections lists details about the parameters you can configure for LDAP-based directory integration.

Attribute Mapping Parameters

The following table describes the parameters for mapping LDAP directory attributes.

BDI Parameter	EDI Parameter	Directory Attribute	Exists in Global Catalog by Default	Is Indexed by Default	Set for Ambiguous Name Resolution (ANR) by Default
BDICommonName	CommonName	cn	Yes	Yes	No
BDIDisplayName	DisplayName	displayName	Yes	Yes	Yes
BDIFirstname	Firstname	givenName	Yes	Yes	Yes
BDILastname	Lastname	sn	Yes	Yes	Yes
BDIEmailAddress	EmailAddress	mail	Yes	Yes	Yes
BDISipUri **Note** The client uses this parameter for intradomain federation, not URI dialing.	SipUri **Note** The client uses this parameter for intradomain federation, not URI dialing.	msRTCSIP-PrimaryUserAddress	Yes	Yes	Yes
BDIPhotoSource	PhotoSource	thumbnailPhoto	No	No	No
BDIBusinessPhone	BusinessPhone	telephoneNumber	Yes	No	No
BDIMobilePhone	MobilePhone	mobile	Yes	No	No

BDI Parameter	EDI Parameter	Directory Attribute	Exists in Global Catalog by Default	Is Indexed by Default	Set for Ambiguous Name Resolution (ANR) by Default
BDIHomePhone	HomePhone	homePhone	Yes	No	No
BDIOtherPhone	OtherPhone	otherTelephone	Yes	No	No
BDIDirectoryUri **Note** The client uses this parameter for URI dialing.	DirectoryUri **Note** The client uses this parameter for URI dialing.	mail	Yes	No	No
BDITitle	Title	title	Yes	No	No
BDICompanyName	CompanyName	company	Yes	Yes	No
BDIUserAccountName	UserAccountName	sAMAccountName	Yes	Yes	Yes
BDIDomainName	DomainName	EDI - userPrincipalName BDI - dn	Yes	Yes	No
BDICountry		co	Yes	No	No
BDILocation	Location	EDI - co BDI - location	Yes	No	No
BDINickname	Nickname	displayName	Yes	Yes	Yes
BDIPostalCode	PostalCode	postalCode	Yes	No	No
BDICity	City	l	Yes	Yes	No
BDIState	State	st	Yes	Yes	No
BDIStreetAddress	StreetAddress	streetAddress	Yes	No	No

Attributes on the Directory Server

You must index attributes on your LDAP directory server for the clients. This lets clients resolve contacts.

To use the default attribute mappings, you must index the following attributes:

- sAMAccountName
- displayName
- sn

- name
- proxyAddresses
- mail
- department
- givenName
- telephoneNumber

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

  - otherTelephone
  - mobile
  - homePhone

  Note By default secondary number queries are enabled in Cisco Jabber for Windows. You can disable secondary number queries with the DisableSecondaryNumberLookups parameter.

- msRTCSIP-PrimaryUserAddress

  Index msRTCSIP-PrimaryUserAddress for intradomain federation only.

Since Cisco Jabber for Windows connects to a Global Catalog server by default, you must ensure that all attributes reside on your Global Catalog server. You can replicate attributes to a Global Catalog server using an appropriate tool such as the Microsoft Active Directory Schema Snap-in. You can choose either to replicate or not to replicate attributes to your Global Catalog server:

- If you replicate attributes to your Global Catalog server, it generates traffic between Active Directory servers in the domain. For this reason, you should replicate attributes to your Global Catalog server only if the network traffic can handle extra load.
- If you do not want to replicate attributes to a Global Catalog server, configure Cisco Jabber to connect to a Domain Controller. In this case, the client queries single domains only when it connects to a Domain Controller.

Directory Connection Parameters

The following table describes parameters for configuring your LDAP directory connection:

BDI Parameter	EDI Parameter	Value	Description
	ConnectionType	0 1	Specifies if the client connects to a Global Catalog or a Domain Controller. • 0 (default) — Connect to a Global Catalog. • 1 — Connect to a Domain Controller. **Note** Default ports are as follows: • Global Catalog: 3268 • Domain Controller: 389
BDILDAPServerType		AD OpenLDAP	Specifies the type of LDAP directory server to which the client connects. • AD (default) — Connect to Active Directory. • OpenLDAP — Connect to OpenLDAP.
BDIPresenceDomain		Domain of the presence node.	Required parameter. Specifies the domain of the presence node. The client appends this domain to the user ID to create an IM address. For example, a user named Adam McKenzie has the user ID *amckenzie*. You specify *example.com* as the presence node domain. When the user logs in, the client constructs the IM address *amckenzie@example.com* for Adam McKenzie.

BDI Parameter	EDI Parameter	Value	Description
BDIPrimaryServerName	PrimaryServerName	IP address FQDN	Required parameter. Specifies the address of the primary directory server. This parameter is required for manual connections where the client cannot automatically discover the directory server. **Note** Each time the client starts, it attempts to connect to the primary server. The client attempts to connect to the secondary server if: • The primary server is not available. • The primary server fails after the client connects to it. If the connection to the secondary server is successful, the client keeps the connection to the secondary server until the next restart. If the secondary server fails while the client is connected to it, the client attempts to connect to the primary server.
	SecondaryServerName	IP address FQDN	Specifies the address of the backup directory server. This parameter is required for manual connections where the client cannot automatically discover the directory server.

BDI Parameter	EDI Parameter	Value	Description
BDIServerPort1	ServerPort1	Port number	Specifies the port for the primary directory server.
	ServerPort2	Port number	Specifies the port for the backup directory server.
	UseWindowsCredentials	0 1	Specifies if the client uses Microsoft Windows usernames and passwords. • 0 — Do not use Windows credentials. Specify credentials with the ConnectionUsername and ConnectionPassword parameters. • 1 (default) — Use Windows credentials.

BDI Parameter	EDI Parameter	Value	Description
BDIUseJabberCredentials		true false	Specifies whether the client can use the presence server credentials to sign in to the directory server. • true — The client searches for the username and password in this order: 1. Client configuration file (BDIConnectionUsername and BDIConnectionPassword) 2. Presence server If the credentials are not present, the client tries to sign in anonymously. • false (default) — The client tries to sign in using the values of BDIConnectionUsername and BDIConnectionPassword in the client configuration file. If the parameters are not present, the client tries to sign in anonymously.

BDI Parameter	EDI Parameter	Value	Description
BDIConnectionUsername	ConnectionUsername	Username	Lets you manually specify a shared username that the client can use to authenticate with the directory server. **Important** The client transmits and stores this username as plain text. By default, Cisco Jabber for Windows uses Integrated Windows Authentication when connecting to the directory server. This parameter lets you manually specify a username in scenarios where it is not possible to authenticate with the directory server with the user's Microsoft Windows credentials. Use only a well-known or public set of credentials for an account with read-only permissions to the directory.

BDI Parameter	EDI Parameter	Value	Description
BDIConnectionPassword	ConnectionPassword	Password	Lets you manually specify a shared password that the client can use to authenticate with the directory server. **Important** The client transmits and stores this password as plain text. By default, Cisco Jabber for Windows uses Integrated Windows Authentication when connecting to the directory server. This parameter lets you manually specify a password in scenarios where it is not possible to authenticate with the directory server with the user's Microsoft Windows credentials. Use a well-known or public set of credentials for an account with read-only permissions to the directory.
BDIEnableTLS		true false	Use TLS to secure directory connections. • true — Use TLS. • false (default) — Do not use TLS.

BDI Parameter	EDI Parameter	Value	Description
	UseSSL	0 1	Use SSL for secure connections to the directory. • 0 (default) — Do not use SSL. • 1 — Use SSL. The SSL connection certificate must be present: • In the Microsoft Windows certificate store. • On the directory server to which the client connects. To establish an SSL connection, the server presents the client with the certificate. The client then validates the certificate from the server against the certificate in the store on the client computer. Default protocols and ports for SSL connections are as follows: • Global Catalog • Protocol: TCP • Port number: 3269 • Domain Controller • Protocol: TCP • Port number: 636

BDI Parameter	EDI Parameter	Value	Description
	UseSecureConnection	0 1	Specifies the mechanism for authentication with the directory server. • 0 — Use simple authentication. Set this value to connect to the directory server using simple binds. With simple authentication, the client transmits credentials in plain text. You can enable SSL to encrypt credentials with the UseSSL parameter. • 1 (default) — Use Generic Security Service API (GSS-API). GSS-API leverages the system authentication mechanism. In a Microsoft Windows environment, GSS-API lets you connect to the directory server using Kerberos-based Windows authentication.

Directory Query Parameters

The following table describes parameters for configuring how the client queries your LDAP directory:

BDI Parameter	EDI Parameter	Value	Description
BDIBaseFilter	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 the directory. The default value for all clients is `(&(objectCategory=person)(objectClass=user)`. Configuration files can contain only valid XML character entity references. Use `&amp;` instead of `&` if you specify a custom base filter.

BDI Parameter	EDI Parameter	Value	Description
BDIUseANR		true false	Specifies if Cisco Jabber issues a query using Ambiguous Name Resolution (ANR) when it performs a predictive search. • true (default) — Use ANR for predictive search. If you use OpenLDAP, the default value is false. • false — Do not use ANR for predictive search. Set the value to false if you integrate with a directory source other than Active Directory. **Important** Configure your directory server to set attributes for ANR if you want the client to search for those attributes.
BDIPredictiveSearchFilter	PredictiveSearchFilter	Search filter	Defines filters to apply to predictive search queries. You can define multiple, comma-separated values to filter search queries. **Note** This key is only used by Cisco Jabber for iPhone and iPad when BDIUseANR is set to false. And if BDI PredictiveSearchFilter is not set, the default search filter is used. The default EDI value is anr When Cisco Jabber for Windows performs a predictive search, it issues a query using ANR. This query disambiguates the search string and returns results that match the attributes that are set for ANR on your directory server. **Important** Configure your directory server to set attributes for ANR if you want the client to search for those attributes.

BDI Parameter	EDI Parameter	Value	Description
	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 (default) — Users can search for alternative contact numbers. • 1 — Users cannot search for alternative contact numbers.
	SearchTimeout	Number of seconds	Specifies the timeout period for queries in seconds. The default value is 5.
	UseWildcards	0 1	Enables wildcard searches. • 0 (default) — Do not use wildcards. • 1 — Use wildcards. If you use wildcards, it might take longer to search the directory.
	MinimumCharacterQuery	Numerical value	Sets the minimum number of characters in a contact name to query the directory. For example, if you set 2 as the value of this parameter, the client searches the directory when users enter at least two characters in the search field. The default value is 3.

BDI Parameter	EDI Parameter	Value	Description
BDISearchBase1	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 the client executes a search. By default, the client 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. Active Directory does not typically require a search base. Specify search bases for Active Directory only for specific performance requirements. Specify a search base for directory servers other than Active Directory to create bindings to specific locations in the directory. **Tip** Specify an OU to restrict searches to certain user groups. For example, a subset of your users have IM capabilities only. Include those users in an OU and then specify that as a search base.

Base Filter Examples

The following are example base filters you can use to look up specific locations or objects.

Find only specific groups:

```
(&amp;(objectClass=user)(memberOf=cn=group-name,ou=Groups,dc=example,dc=com))
```

Find a nested group within a group:

```
(&amp;(objectClass=user)(memberOf:search-oid:=cn=group-name,ou=Groups,dc=example,dc=com))
```

Find only enabled accounts and non-administrator accounts:

```
(&amp;(objectCategory=person)(objectClass=user)(!(userAccountControl:search-oid:=2))
(!(sAMAccountName=*_dbo))(!(sAMAccountName=*-admin)))
```

Phone Number Masks Parameter

Phone number masks parameter only applies to EDI. The following table describes the parameter to configure masks for phone number resolution:

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: `+1408|+(#) ### ### ####` The length of mask strings cannot exceed the size restriction for registry subkey names.

Phone masks apply to phone numbers before the client 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 Parameters

The following table describes parameters for configuring how the client retrieves contact photos from an LDAP directory.

BDI Parameter	EDI Parameter	Value	Description
BDIPhotoUriSubstitutionEnabled	PhotoUriSubstitutionEnabled	true false	Specifies if photo URI substitution is enabled. • true — Photo URI substitution is enabled. • false (default) — Specifies if photo URI substitution is disabled.

BDI Parameter	EDI Parameter	Value	Description
BDIPhotoUriSubstitutionToken	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

BDI Parameter	EDI Parameter	Value	Description
BDIPhotoUriWithToken	PhotoUriWithToken	URI	Specifies a photo URI with a directory attribute as a variable value. For example: `http://staffphoto.example.com/sAMAccountName.jpg` The parameter applies to LDAP directory integrations. To configure photo URI substitution, you set the directory attribute as the value of BDIPhotoUriSubstitutionToken. **Restriction** The client must be able to retrieve the photos from the web server without credentials.
BDIPhotoSource	PhotoSource	Directory attribute	The name of a directory attribute that stores a contact photo as a binary object or a URI to a contact photo.

Contact Photo Retrieval

Cisco Jabber retrieves and displays 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 Cisco Jabber.

URI substitution

Cisco Jabber 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 BDIPhotoUriSubstitutionEnabled or PhotoUriSubstitutionEnabled parameter.
2. Specify a directory attribute to use as a dynamic token as the value of the BDIPhotoUriSubstitutionToken or PhotoUriSubstitutionToken parameter. For example,

   ```
   <BDIPhotoUriSubstitutionToken>sAMAccountName</BDIPhotoUriSubstitutionToken>
   ```

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

3. Specify the URL and the dynamic token as the value of the BDIPhotoUriWithToken or PhotoUriWithToken parameter. Use a direct URL for photo retrieval. Do not use redirected URLs. For example,

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

   ```
   <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 Jabber then takes this value and replaces the token to build the following URL: http://staffphoto.example.com/msmith.jpg.

Binary objects

Cisco Jabber retrieves the binary data for the photo from your database.

If you are using binary objects from Active Directory do not set BDIPhotoUriWithToken or PhotoUriWithToken.

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

```
<BDIPhotoSource>jpegPhoto</BDIPhotoSource>
```

```
<PhotoSource>thumbnailPhoto</PhotoSource>
```

PhotoURL attribute

Cisco Jabber 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 BDIPhotoSource or PhotoSource parameter in the configuration. For example,

```
<BDIPhotoSource>photoUri</BDIPhotoSource>
```

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

UDS Parameters

The following table provides details about the parameters you can use in the configuration file to connect to UDS and perform contact resolution and directory queries.

Parameter	Value	Description
PresenceDomain	Domain of the presence node.	Required parameter. Specifies the domain of the presence server. The client appends this domain to the user ID to create an IM address. For example, a user named Adam McKenzie has the following user ID: amckenzie. You specify example.com as the presence server domain. When the user logs in, the client constructs the following IM address for Adam McKenzie: amckenzie@example.com.
UdsServer	IP address FQDN	Specifies the address of the Cisco Unified Communications Manager User Data Service (UDS) server. This parameter is required for manual connections where the client cannot automatically discover the UDS server.

Parameter	Value	Description
UdsPhotoUriWithToken	URI	Specifies a photo URI with a directory attribute as a variable value; for example, `http://www.photo/url/path/%%uid%%.jpg`. This parameter applies to UDS directory integrations. You must specify this parameter to download contact photos in either of the following cases: • If you configure the DirectoryServerType parameter to use UDS. With this configuration, the client uses UDS for contact resolution when it is inside or outside of the corporate firewall. • If you deploy Expressway for Mobile and Remote Access. With this configuration, the client automatically uses UDS for contact resolution when it is outside of the corporate firewall. **Restriction** The client must be able to retrieve the photos from the web server without credentials.

Contact Photo Retrieval with UDS

Cisco Unified Communications Manager User Data Service (UDS) dynamically builds a URL for contact photos with a directory attribute and a URL template.

To resolve contact photos with UDS, you specify the format of the contact photo URL as the value of the UdsPhotoUriWithToken parameter. You also include a *%%uid%%* token to replace the contact username in the URL, for example,

```
<UdsPhotoUriWithToken>http://server_name/%%uid%%.jpg</UdsPhotoUriWithToken>
```

UDS substitutes the *%%uid%%* token with the value of the `userName` attribute in UDS. For example, a user named Mary Smith exists in your directory. The value of the `userName` attribute for Mary Smith is msmith. To resolve the contact photo for Mary Smith, Cisco Jabber takes the value of the `userName` attribute and replaces the *%%uid%%* token to build the following URL: `http://staffphoto.example.com/msmith.jpg`

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

Important

- If you deploy Expressway for Mobile and Remote Access, the client automatically uses UDS for contact resolution when users connect to services from outside the corporate network. When you set up UDS contact resolution for Expressway for Mobile and Remote Access, you must add the web server on which you host the contact photos to the HTTP server allow list in your Cisco Expressway-C server configuration. The HTTP server allow list enables the client to access web services inside the corporate network.
- All contact photos must follow the format of the URL you specify as the value of UdsPhotoUriWithToken.

Contact Photo Formats and Dimensions

To achieve the best result with Cisco Jabber, your contact photos should have specific formats and dimensions. Review supported formats and optimal dimensions. Learn about adjustments the client makes to contact photos.

Contact Photo Formats

Cisco Jabber supports the following formats for contact photos in your directory:

- JPG
- PNG
- BMP

Important Cisco Jabber does not apply any modifications to enhance rendering for contact photos in GIF format. As a result, contact photos in GIF format might render incorrectly or with less than optimal quality. To obtain the best quality, use PNG format for your contact photos.

Contact Photo Dimensions

Tip The optimum dimensions for contact photos are 128 pixels by 128 pixels with an aspect ratio of 1:1.

128 pixels by 128 pixels are the maximum dimensions for local contact photos in Microsoft Outlook.

The following table lists the different dimensions for contact photos in Cisco Jabber.

Location	Dimensions
Audio call window	128 pixels by 128 pixels
Invitations and reminders, for example: • Incoming call windows • Meeting reminder windows	64 pixels by 64 pixels
Lists of contacts, for example: • Contact lists • Participant rosters • Call history • Voicemail messages	32 pixels by 32 pixels

Contact Photo Adjustments

Cisco Jabber adjusts contact photos as follows:

- Resizing—If contact photos in your directory are smaller or larger than 128 pixels by 128 pixels, the client automatically resizes the photos. For example, contact photos in your directory are 64 pixels by 64 pixels. When Cisco Jabber retrieves the contact photos from your directory, it resizes the photos to 128 pixels by 128 pixels.

  Tip Resizing contact photos can result in less than optimal resolution. For this reason, use contact photos that are 128 pixels by 128 pixels so that the client does not automatically resize them.

- Cropping—Cisco Jabber automatically crops nonsquare contact photos to a square aspect ratio, or an aspect ratio of 1:1 where the width is the same as the height.

- Portrait orientation—If contact photos in your directory have portrait orientation, the client crops 30 percent from the top and 70 percent from the bottom.

  For example, if contact photos in your directory have a width of 100 pixels and a height of 200 pixels, Cisco Jabber needs to crop 100 pixels from the height to achieve an aspect ratio of 1:1. In this case, the client crops 30 pixels from the top of the photos and 70 pixels from the bottom of the photos.

- Landscape orientation—If contact photos in your directory have landscape orientation, the client crops 50 percent from each side.

  For example, if contact photos in your directory have a width of 200 pixels and a height of 100 pixels, Cisco Jabber needs to crop 100 pixels from the width to achieve an aspect ratio of 1:1. In this case, the client crops 50 pixels from the right side of the photos and 50 pixels from the left side of the photos.

Directory Server Configuration Examples

This section describes supported integration scenarios and provides example configurations.

Domain Controller Connection

To connect to a Domain Controller, set the following parameters:

Parameter	Value
DirectoryServerType	EDI
ConnectionType	1

The following is an example configuration:

```
<Directory><DirectoryServerType>EDI</DirectoryServerType>
<ConnectionType>1</ConnectionType></Directory>
```

Manual Server Connections for Cisco Jabber for Windows

To manually connect to a directory server, set the following parameters:

Parameter	Value
DirectoryServerType	EDI
PrimaryServerName	FQDN IP address
ServerPort1	Port number
SecondaryServerName	FQDN IP address
ServerPort2	Port number

The following is an example configuration:

```
<Directory>

<DirectoryServerType>EDI</DirectoryServerType>

<PrimaryServerName>primary-server-name.domain.com</PrimaryServerName>
<ServerPort1>1234</ServerPort1>
<SecondaryServerName>secondary-server-name.domain.com</SecondaryServerName>
<ServerPort2>5678</ServerPort2>
</Directory>
```

UDS Integration

To integrate with UDS, set the following parameters.

Parameter	Value
DirectoryServerType	UDS
UdsServer	IP address of the UDS server
UdsPhotoUriWithToken	Contact photo URL
PresenceDomain **Note** This parameter is only applicable to Phone Mode.	Server address of your presence domain

Note Configure the DirectoryServerType parameter to UDS only if you want to use UDS for all contact resolution (that is, from inside and outside the corporate firewall).

The following is an example configuration:

```
<Directory>
  <DirectoryServerType>UDS</DirectoryServerType>
  <UdsServer>11.22.33.444</UdsServer>
  <UdsPhotoUriWithToken>http://server-name/%%uid%%.jpg</UdsPhotoUriWithToken>
</Directory>
```

LDAP Integration with Expressway for Mobile and Remote Access

When you deploy Expressway for Mobile and Remote Access with an LDAP directory integration, the client uses:

- LDAP when inside the corporate firewall
- UDS when outside the corporate firewall

Note LDAP is the default configuration, so it is not necessary to include the DirectoryServerType parameter in your client configuration file.

To ensure that the client can resolve contact photos from both inside and outside your corporate firewall, set the following parameters.

Parameter	Value
PhotoUriWithToken	Contact photo URL when inside the corporate firewall
BDIPhotoUriWithToken	Contact photo URL when inside the corporate firewall
UdsPhotoUriWithToken	Contact photo URL when outside the corporate firewall

The following is an example configuration:

```
<Directory>
  <PhotoUriWithToken>http://photo.example.com/sAMAccountName.jpg</PhotoUriWithToken>
  <BDIPhotoUriWithToken>http://photo.example.com/sAMAccountName.jpg</BDIPhotoUriWithToken>
  <UdsPhotoUriWithToken>http://server-name/%%uid%%.jpg</UdsPhotoUriWithToken>
</Directory>
```

Simple Authentication for Cisco Jabber for Windows

Simple authentication lets you connect to a directory server using simple binds, as in the following example configuration:

```
<UseWindowsCredentials>0</UseWindowsCredentials>
<UseSSL>0</UseSSL>
<UseSecureConnection>0</UseSecureConnection>
<ConnectionUsername>username</ConnectionUsername>
<ConnectionPassword>password</ConnectionPassword>
```

This configuration specifies that the client:

- Does not use Microsoft Windows credentials.
- Does not use SSL.
- Uses simple authentication.
- Uses custom credentials.

As a result of the simple bind, the client transmits the credentials in the payload of the bind request in plain text.

Simple Authentication for Mobile Clients and Cisco Jabber for Mac

Simple authentication lets you connect to a directory server using simple binds, as in the following example configuration:

```
<BDIEnableTLS>False</BDIEnableTLS>
<BDIConnectionUsername>username</BDIConnectionUsername>
<BDIConnectionPassword>password</BDIConnectionPassword>
<BDIServerPort1>389/3268</BDIServerPort1>
```

This configuration specifies that the client:

- Does not use SSL.
- Uses simple authentication.
- Uses custom credentials.
- Uses port 389/3268 for non-TLS.

As a result of the simple bind, the client transmits the credentials in the payload of the bind request in plain text.

Simple Authentication with SSL for Cisco Jabber for Windows

Enable SSL in directory server connections with the UseSSL parameter. You can use SSL to encrypt credentials when you use simple authentication, as in the following example configuration:

```
<UseWindowsCredentials>0</UseWindowsCredentials>
<UseSSL>1</UseSSL>
<UseSecureConnection>0</UseSecureConnection>
<ConnectionUsername>username</ConnectionUsername>
<ConnectionPassword>password</ConnectionPassword>
```

This configuration specifies that the client:

- Does not use Microsoft Windows credentials.
- Uses SSL.
- Uses simple authentication.
- Uses custom credentials.

As a result, the client uses SSL to encrypt the credentials in the client configuration.

Simple Authentication with SSL for Mobile Clients

Enable SSL in directory server connections with the BDIEnableTLS parameter. You can use SSL to encrypt credentials when you use simple authentication, as in the following example configuration:

```
<BDIEnableTLS>True</BDIEnableTLS>
<BDIConnectionUsername>username</BDIConnectionUsername>
<BDIConnectionPassword>password</BDIConnecitonPassword>
<ServerPort1>636</<ServerPort1>
<ServerPort1>3269</ServerPort1>
```

This configuration specifies that the client:

- Uses SSL.
- Uses simple authentication.

- Uses custom credentials.
- Uses port 636 or 3269 for TLS.

As a result, the client uses SSL to encrypt the credentials in the client configuration.

OpenLDAP Integration

You can integrate with OpenLDAP using anonymous binds or authenticated binds.

Anonymous Binds for Cisco Jabber for Windows

To integrate with OpenLDAP using anonymous binds, set the following parameters:

Parameter	Value
DirectoryServerType	EDI
ConnectionType	1
PrimaryServerName	IP address Hostname
UseWindowsCredentials	0
UseSecureConnection	1
SearchBase1	Root of the directory service or the organizational unit (OU)
UserAccountName	Unique identifier such as UID or CN
BaseFilter	Object class that your directory service uses; for example, inetOrgPerson.
PredictiveSearchFilter	UID or other search filter

The following is an example configuration:

```
<Directory>
 <DirectoryServerType>EDI</DirectoryServerType>
 <ConnectionType>1</ConnectionType>
 <PrimaryServerName>11.22.33.456</PrimaryServerName>
 <UseWindowsCredentials>0</UseWindowsCredentials>
 <UseSecureConnection>1</UseSecureConnection>
 <SearchBase1>ou=people,dc=cisco,dc=com</SearchBase1>
 <UserAccountName>uid</UserAccountName>
  <BaseFilter>(&amp;(objectClass=inetOrgPerson)</BaseFilter>
 <PredictiveSearchFilter>uid</PredictiveSearchFilter>
</Directory>
```

Anonymous Binds for Mobile Clients and Cisco Jabber for Mac

To integrate with OpenLDAP using anonymous binds, set the following parameters:

Parameter	Value
DirectoryServerType	BDI
BDILDAPServerType	OpenLDAP
BDIPrimaryServerName	IP address Hostname
BDIEnableTLS	True
BDISearchBase1	Root of the directory service or the organizational unit (OU)
BDIServerPort1	The port for the primary directory server
BDIUserAccountName	Unique identifier such as uid or cn
BDIBaseFilter	Object class that your directory service uses; for example, inetOrgPerson.
(Optional) BDIPredictiveSearchFilter	uid or other search filter

The following is an example configuration:

```
<Directory>
 <DirectoryServerType>BDI</DirectoryServerType>
 <BDILDAPServerType>OpenLDAP</BDILDAPServerType>
 <BDIPrimaryServerName>11.22.33.456</BDIPrimaryServerName>
 <BDIEnableTLS>True</BDIEnableTLS>
 <BDISearchBase1>ou=people,dc=cisco,dc=com</BDISearchBase1>
 <BDIServerPort1>636</BDIServerPort1>
 <BDIUserAccountName>uid</BDIUserAccountName>
 <BDIBaseFilter>(&amp;(objectClass=inetOrgPerson)</BDIBaseFilter>
 <BDIPredictiveSearchFilter>uid</BDIPredictiveSearchFilter>
</Directory>
```

Authenticated Binds for Cisco Jabber for Windows

To integrate with OpenLDAP using authenticated binds, set the following parameters:

Parameter	Value
DirectoryServerType	EDI
ConnectionType	1
PrimaryServerName	IP address Hostname
UserWindowsCredentials	0
UseSecureConnection	0
SearchBase1	Root of the directory service or the organizational unit (OU)

Parameter	Value
UserAccountName	Unique identifier such as UID or CN
BaseFilter	Object class that your directory service uses; for example, inetOrgPerson.
PredictiveSearchFilter	UID or other search filter
ConnectionUsername	Username
ConnectionPassword	Password

The following is an example configuration:

```
<Directory>
  <DirectoryServerType>EDI</DirectoryServerType>
  <ConnectionType>1</ConnectionType>
  <PrimaryServerName>11.22.33.456</PrimaryServerName>
  <UserWindowsCredentials>0</UserWindowsCredentials>
  <UseSecureConnection>0</UseSecureConnection>
  <SearchBase1>ou=people,dc=cisco,dc=com</SearchBase1>
  <UserAccountName>uid</UserAccountName>
  <BaseFilter>(&amp;(objectClass=inetOrgPerson)</BaseFilter>
  <PredictiveSearchFilter>uid</PredictiveSearchFilter>
  <ConnectionUsername>cn=lds-read-only-user,dc=cisco,dc=com</ConnectionUsername>
  <ConnectionPassword>password</ConnectionPassword>
</Directory>
```

Authenticated Binds for Mobile Clients and Cisco Jabber for Mac

To integrate with OpenLDAP using authenticated binds, set the following parameters:

Parameter	Value
BDILDAPServerType	OpenLDAP
BDIPrimaryServerName	IP address Hostname
BDIEnableTLS	False
BDISearchBase1	Root of the directory service or the organizational unit (OU)
BDIServerPort1	The port for the primary directory server
BDIUserAccountName	Unique identifier such as UID or CN
BDIBaseFilter	Object class that your directory service uses; for example, inetOrgPerson.
BDIPredictiveSearchFilter	(Optional) UID or other search filter
BDIConnectionUsername	Username
BDIConnectionPassword	Password

The following is an example configuration:

```
<Directory>
<BDILDAPServerType>OpenLDAP</BDILDAPServerType>
  <BDIPrimaryServerName>11.22.33.456</BDIPrimaryServerName>
  <BDIEnableTLS>False</BDIEnableTLS>
  <BDISearchBase1>ou=people,dc=cisco,dc=com</BDISearchBase1>

  <BDIServerPort1>636</BDIServerPort1>
  <BDIUserAccountName>uid</BDIUserAccountName>
  <BDIBaseFilter>(&amp;(objectClass=inetOrgPerson)</BDIBaseFilter>

  <BDIPredictiveSearchFilter>uid</BDIPredictiveSearchFilter>
  <BDIConnectionUsername>cn=administrator,dc=cisco,dc=com</BDIConnectionUsername>
  <BDIConnectionPassword>password</BDIConnectionPassword>
</Directory>
```

AD LDS Integration

You can integrate with AD LDS or ADAM using specific configurations.

Anonymous Binds for Cisco Jabber for Windows

To integrate with AD LDS or ADAM using anonymous binds, set the following parameters:

Parameter	Value
DirectoryServerType	EDI
PrimaryServerName	IP address Hostname
ServerPort1	Port number
UseWindowsCredentials	0
UseSecureConnection	1
SearchBase1	Root of the directory service or the organizational unit (OU)

The following is an example configuration:

```
<Directory>

  <DirectoryServerType>EDI</DirectoryServerType>

  <PrimaryServerName>11.22.33.456</PrimaryServerName>
  <ServerPort1>50000</ServerPort1>

  <UseWindowsCredentials>0</UseWindowsCredentials>
  <UseSecureConnection>1</UseSecureConnection>

  <SearchBase1>dc=adam,dc=test</SearchBase1>
</Directory>
```

Anonymous Binds for Mobile Clients and Cisco Jabber for Mac

To integrate with AD LDS or ADAM using anonymous binds, set the following parameters:

Parameter	Value
BDIPrimaryServerName	IP address Hostname
BDIServerPort1	Port number
BDISearchBase1	Root of the directory service or the organizational unit (OU)

The following is an example configuration:

```
<Directory>
  <BDIPrimaryServerName>11.22.33.456</BDIPrimaryServerName>
  <BDIServerPort1>50000</BDIServerPort1>
  <BDISearchBase1>dc=adam,dc=test</BDISearchBase1>
</Directory>
```

Windows Principal User Authentication

To integrate with AD LDS or ADAM using authentication with the Microsoft Windows principal user, set the following parameters:

Parameter	Value
DirectoryServerType	EDI
PrimaryServerName	IP address Hostname
ServerPort1	Port number
UseWindowsCredentials	0
UseSecureConnection	1
ConnectionUsername	Username
ConnectionPassword	Password
UserAccountName	Unique identifier such as UID or CN
SearchBase1	Root of the directory service or the organizational unit (OU)

The following is an example configuration:

```
<Directory>
  <DirectoryServerType>EDI</DirectoryServerType>
  <PrimaryServerName>11.22.33.456</PrimaryServerName>
  <ServerPort1>50000</ServerPort1>
  <UseWindowsCredentials>0</UseWindowsCredentials>
  <UseSecureConnection>1</UseSecureConnection>
  <ConnectionUsername>cn=administrator,dc=cisco,dc=com</ConnectionUsername>
  <ConnectionPassword>password</ConnectionPassword>
  <UserAccountName>cn</UserAccountName>
  <SearchBase1>ou=people,dc=cisco,dc=com</SearchBase1>
</Directory>
```

AD LDS Principal User Authentication for Cisco Jabber for Windows

To integrate with AD LDS or ADAM using authentication with the AD LDS principal user, set the following parameters:

Parameter	Value
DirectoryServerType	EDI
PrimaryServer	IP address Hostname
ServerPort1	Port number
UseWindowsCredentials	0
UseSecureConnection	0
ConnectionUsername	Username
ConnectionPassword	Password
UserAccountName	Unique identifier such as UID or CN
SearchBase1	Root of the directory service or the organizational unit (OU)

The following is an example configuration:

```
<Directory>

<DirectoryServerType>EDI</DirectoryServerType>

<PrimaryServerName>11.22.33.456</PrimaryServerName>
  <ServerPort1>50000</ServerPort1>
  <UseWindowsCredentials>0</UseWindowsCredentials>
  <UseSecureConnection>0</UseSecureConnection>
  <ConnectionUsername>cn=administrator,dc=cisco,dc=com</ConnectionUsername>
  <ConnectionPassword>password</ConnectionPassword>
  <UserAccountName>cn</UserAccountName>
  <SearchBase1>ou=people,dc=cisco,dc=com</SearchBase1>
</Directory>
```

AD LDS Principal User Authentication for Mobile Clients and Cisco Jabber for Mac

To integrate with AD LDS or ADAM using authentication with the AD LDS principal user, set the following parameters:

Parameter	Value
BDIPrimaryServerName	IP address Hostname
BDIServerPort1	Port number

Parameter	Value
BDIConnectionUsername	Username
BDIConnectionPassword	Password
BDIUserAccountName	Unique identifier such as uid or cn
BDISearchBase1	Root of the directory service or the organizational unit (OU)

The following is an example configuration:

```
<Directory>>
  <BDIPrimaryServerName>11.22.33.456</BDIPrimaryServerName>
  <BDIServerPort1>50000</BDIServerPort1>
  <BDIConnectionUsername>cn=administrator,dc=cisco,dc=com</BDIConnectionUsername>
  <BDIConnectionPassword>password</BDIConnectionPassword>
  <BDIUserAccountName>cn</BDIUserAccountName>
  <BDISearchBase1>ou=people,dc=cisco,dc=com</BDISearchBase1>
</Directory>
```

CHAPTER 10

Set Up Certificate Validation

About Certificate Validation

Cisco Jabber uses certificate validation to establish secure connections with servers.

When attempting to establish secure connections, servers present Cisco Jabber with certificates.

Cisco Jabber for Mac validates those certificates against certificates in the Keychain.

If the client cannot validate a certificate, it prompts the user to confirm if they want to accept the certificate.

In Expressway for Mobile and Remote Access deployment, when using an online certificate status protocol (OCSP) or online certificate revocation lists (CRL) to obtain the revocation status of the certificates, the Cisco Jabber client expects a response time of less than 5 seconds. Connections will fail if the response time is greater than the expected 5 seconds.

On-Premises Servers

Review which certificates on-premises servers present to the client and the tasks involved in getting those certificates signed.

Required Certificates for On-Premises Servers

On-premises servers present the following certificates to establish a secure connection with Cisco Jabber:

Server	Certificate
Cisco Unified Communications Manager IM and Presence Service	HTTP (Tomcat) XMPP
Cisco Unified Communications Manager	HTTP (Tomcat) and CallManager certificate (secure SIP call signaling for secure phone)
Cisco Unity Connection	HTTP (Tomcat)
Cisco Webex Meetings Server	HTTP (Tomcat)

Server	Certificate
Cisco VCS Expressway Cisco Expressway-E	Server certificate (used for HTTP, XMPP, and SIP call signaling)

Important Notes

- Security Assertion Markup Language (SAML) single sign-on (SSO) and the Identity Provider (IdP) require an X.509 certificate.
- You should apply the most recent Service Update (SU) for Cisco Unified Communications Manager IM and Presence Service before you begin the certificate signing process.
- The required certificates apply to all server versions.
- Each cluster node, subscriber, and publisher, runs 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.

If the process your company uses means you must wait for the CSRs to be sent back to you before you can apply them, then you may wish to configure your services now while you wait for the CSRs. Then you can apply the certificates after the service configuration is complete, prior to deployment.

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

Certificate Signing Request Formats and Requirements

A public certificate authority (CA) typically requires a certificate signing request (CSR) to conform to specific formats. For example, a public CA might only accept CSRs that have the following requirements:

- 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.

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).

For example, to sign the HTTP and XMPP certificates for a single Cisco Unified Communications Manager IM and Presence Service node, you might need to submit each CSR to different public CAs.

Revocation Servers

Cisco Jabber cannot connect to the Cisco Unified Communications Manager servers if the revocation server is not reachable. Also, if a certificate authority (CA) revokes a certificate, Cisco Jabber does not allow users to connect to that server.

Users are not notified of the following outcomes:

- The certificates do not contain revocation information.
- The revocation server cannot be reached.

To validate certificates, the certificate must contain an HTTP URL in the **CDP** or **AIA** fields for a reachable server that can provide revocation information.

To ensure that your certificates are validated when you get a certificate issued by a CA, you must meet one of the following requirements:

- Ensure that the **CRL Distribution Point** (CDP) field contains an HTTP URL to a certificate revocation list (CRL) on a revocation server.
- Ensure that the **Authority Information Access** (AIA) field contains an HTTP URL for an Online Certificate Status Protocol (OCSP) server.

Server Identity in Certificates

As part of the signing process, the CA specifies the server identity in the certificate. 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:

- XMPP certificates
    - `SubjectAltName\OtherName\xmppAddr`
    - `SubjectAltName\OtherName\srvName`
    - `SubjectAltName\dnsNames`
    - `Subject CN`
- 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 or hostname, 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 in many places on your servers. For more information, see *Prevent Identity Mismatch* section in Troubleshooting TechNotes.

Provide XMPP Domain to Clients

This task is not required if you are using Cisco Unified Communications Manager IM and Presence Service version 10.0 or later.

The client identifies `XMPP` certificates using the XMPP domain, rather than the FQDN. The `XMPP` certificates must contain the XMPP domain in an identifier field.

When the client attempts to connect to the presence server, the presence server provides the XMPP domain to the client. The client can then validate the identity of the presence server against the `XMPP` certificate.

Complete the following steps to ensure the presence server provides the XMPP domain to the client:

Procedure

Step 1 Open the administration interface for your presence server, as follows:

- Cisco Unified Communications Manager IM and Presence Service — Open the **Cisco Unified CM IM and Presence Administration** interface.
- Cisco Unified Presence — Open the **Cisco Unified Presence Administration** interface.

Step 2 Select **System** > **Security** > **Settings**.

Step 3 Locate the **XMPP Certificate Settings** section.

Step 4 Specify the presence server domain in the following field: **Domain name for XMPP Server-to-Server Certificate Subject Alternative Name**.

Step 5 Select the following checkbox: **Use Domain Name for XMPP Certificate Subject Alternative Name**.

Step 6 Click **Save**.

Deploy Certificates on Client Computers

Every server certificate should have an associated certificate in the Keychain on the client computers. Cisco Jabber validates the certificates that the servers present against the certificates in the Keychain.

Important If root certificates are not present in the Keychain, Cisco Jabber prompts users to accept certificates from each server in your environment.

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

- Always trust *server name* — The client saves the certificate to the Keychain.
- Continue — The client will connect, but when the user restarts the client they are prompted to accept the certificate again.
- Cancel — The client:
  - Does not save the certificate.
  - Does not connect to the server.

Prevent the warning dialogs by downloading the certificates from the **Cisco Unified OS Administration** interface. Complete the following steps to deploy self-signed certificates to the user.

Procedure

Step 1 For each Cisco node, download the corresponding "tomcat-trust" certificate from the **Cisco Unified OS Administration** interface. Select **Security** > **Certificate Management**.

Step 2 Concatenate the certificates into a single file with the extension **.pem** (for example, "companyABCcertificates.pem").

Step 3 Send the file to your Cisco Jabber users and ask them to double-click it. Doing so launches the Keychain Access application and imports the certificates.

Note The operating system requires that the user enter the Mac OS X administration password for each certificate that is being imported.

Certificate Requirements for Cloud-Based Servers

Cisco WebEx Messenger and Cisco WebEx Meeting Center present the following certificates to the client:

- Central Authentication Service (CAS)
- WLAN Authentication and Privacy Infrastructure (WAPI)

Important Cisco WebEx certificates are signed by a public certificate authority (CA). Cisco Jabber validates these certificates to establish secure connections with cloud-based services.

As of Cisco Jabber for Windows 9.7.2 and Cisco Jabber for Mac 9.6.1, Cisco Jabber validates the XMPP certificate received from Cisco WebEx Messenger. If your operating system does not contain the following certificates for Cisco WebEx Messenger, you must provide them:

- VeriSign Class 3 Public Primary Certification Authority—G5 (stored in the Trusted Root Certificate Authority)
- VeriSign Class 3 Secure Server CA—G3 (stored in the Intermediate Certificate Authority)

The same set of certificates are applicable for Cisco Jabber for Android, iPhone and iPad.

The certificate that is stored in the Intermediate Certificate Authority validates the Cisco WebEx Messenger server identity.

For Cisco Jabber for Windows 9.7.2 or later, you can find more information and installation instructions for the root certificate at http://www.identrust.co.uk/certificates/trustid/install-nes36.html.

For Cisco Jabber for Mac 9.6.1 or later and iOS, you can find more information for the root certificate on the Apple support website at https://support.apple.com.

Update Profile Photo URLs

In cloud-based deployments, Cisco Webex assigns unique URLs to profile photos when you add or import users. When Cisco Jabber resolves contact information, it retrieves the profile photo from Cisco Webex at the URL where the photo is hosted.

Profile photo URLs use HTTP Secure (`https://server_name/`) and present certificates to the client. If the server name in the URL is:

- A fully qualified domain name (FQDN) that contains the Cisco Webex domain — The client can validate the web server that is hosting the profile photo against the Cisco Webexcertificate.
- An IP address — The client cannot validate the web server that is hosting the profile photo against the Cisco Webex certificate. In this case, the client prompts users to accept certificates whenever they look up contacts with an IP address in their profile photo URLs.

Important

- We recommend that you update all profile photo URLs that contain an IP address as the server name. Replace the IP address with the FQDN that contains the Cisco Webex domain to ensure that the client does not prompt users to accept certificates.
- When you update a photo, the photo can take up to 24 hours to refresh in the client.

The following steps describe how to update profile photo URLs. Refer to the appropriate Cisco Webex documentation for detailed instructions.

Procedure

Step 1 Export user contact data in CSV file format with the Cisco WebexAdministration Tool.

Step 2 In the **userProfilePhotoURL** field, replace IP addresses with the Cisco Webex domain.

Step 3 Save the CSV file.

Step 4 Import the CSV file with the Cisco Webex Administration Tool.

PART III

Client Configuration

CHAPTER 11

Configure the Clients

Introduction to Client Configuration

Cisco Jabber can retrieve configuration settings from the following sources:

- Service Profiles — You can configure some client settings in UC service profiles on Cisco Unified Communications Manager release 9 and later. When users launch the client, it discovers the Cisco Unified Communications Manager home cluster using a DNS SRV record and automatically retrieves the configuration from the UC service profile.

  Applies to on-premises deployments only.

- Phone Configuration — You can set some client settings in the phone configuration on Cisco Unified Communications Manager release 9 and later. The client retrieves the settings from the phone configuration in addition to the configuration in the UC service profile.

Applies to on-premises deployments only.

- Cisco Unified Communications Manager IM and Presence Service — You can enable instant messaging and presence capabilities and configure certain settings such as presence subscription requests.

  In the **Advanced settings** window, if you select either **Cisco IM & Presence** or **Cisco Communications Manager 8.x**, the client retrieves UC services from Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service. The client does not use service profiles or SSO discovery.

  Applies to on-premises deployments only.

- Client Configuration Files — You can create XML files that contain configuration parameters. You then host the XML files on a TFTP server. When users sign in, the client retrieves the XML file from the TFTP server and applies the configuration.

  Applies to on-premises and cloud-based deployments.

- Cisco Webex Administration Tool — You can configure some client settings with the Cisco Webex Administration Tool.

  Applies to cloud-based deployments only.

Configure Service Profiles

You can configure some client settings in UC service profiles on Cisco Unified Communications Manager version 9 and later.

Important

- Cisco Jabber only retrieves configuration from service profiles on Cisco Unified Communications Manager if the client gets the `_cisco-uds` SRV record from a DNS query.

  In a hybrid environment, if the CAS URL lookup is successful Cisco Jabber retrieves the configurations from Cisco WebEx Messenger service and the `_cisco-uds` SRV record is ignored.

- 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, then you must manually configure remote cluster information, similar to the EMCC remote cluster set up. For more information on Remote Cluster Configuration, see the *Cisco Unified Communications Manager Features and Services Guide*.

Related Topics

Remote Cluster Configuration on Cisco Unified Communications Manager 10.0

Set Parameters on Service Profile

The client can retrieve UC service configuration and other settings from service profiles.

Parameters in Service Profiles

Learn which configuration parameters you can set in service profiles. Review the corresponding parameters in the client configuration file.

IM and Presence Service Profile

The following table lists the configuration parameters you can set in the IM and Presence Service profile:

Parameter	Description
Product type	Provides the source of authentication to Cisco Jabber and has the following values: • Unified CM (IM and Presence Service) — Cisco Unified Communications Manager IM and Presence Service is the authenticator. • WebEx (IM and Presence Service) — The Cisco WebEx Messenger service is the authenticator. **Note** As of this release, the client issues an HTTP query in addition to the query for SRV records. The HTTP query allows the client to determine if it should authenticate to the Cisco WebEx Messenger service. As a result of the HTTP query, the client connects to the Cisco WebEx Messenger service in cloud-based deployments before getting the `_cisco-uds` SRV record. Setting the value of the **Product type** field to **WebEx** may have no practical effect if the WebEx service has already been discovered by a CAS lookup. • Not set — If the service profile does not contain an IM and presence service configuration, the authenticator is Cisco Unified Communications Manager.

Parameter	Description
Primary server	Specifies the address of your primary presence server. • On-Premises Deployments — You should specify the fully qualified domain name (FQDN) of Cisco Unified Communications Manager IM and Presence Service. • Cloud-Based Deployments — The client uses the following URL as default when you select **WebEx** as the value for the **Product type** parameter: `https://loginp.webexconnect.com/cas/auth.do` This default URL overrides any value that you set.

Voicemail Profile

The following table lists the configuration parameters you can set in the voicemail profile:

Parameter	Description
Voicemail server	Specifies connection settings for the voicemail server.
Credentials source for voicemail service	Specifies that the client uses the credentials for the instant messaging and presence or conferencing service to authenticate with the voicemail service. Ensure that the credentials source that you set match the user's voicemail credentials. If you set a value for this parameter, users cannot specify their voicemail service credentials in the client user interface.

Conferencing Profile

The following table lists the configuration parameters you can set in the conferencing profile:

Conferencing Service Configuration	Description
Conferencing server	Specifies connection settings for the conferencing server.
Credentials source for web conference service	Specifies that the client uses the credentials for the instant messaging and presence or voicemail service to authenticate with the conferencing service. Ensure that the credentials source that you set match the user's conferencing credentials.

Directory Profile

See the *Client Configuration for Directory Integration* chapter for information about configuring directory integration in a service profile.

CTI Profile

The following table lists the configuration parameters you can set in the CTI profile:

CTI Service Configuration	Description
CTI server	Specifies connection settings for the CTI server.

Add Cisco Unified Communications Manager Services

Add Cisco Unified Communications Manager services to specify the address, ports, protocols, and other settings for services such as IM and Presence Service, voicemail, conferencing, and directory.

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 Select the UC service type you want to add and then select **Next**.

Step 5 Configure the UC service as appropriate and then select **Save**.

What to do next

Add your UC services to service profiles.

Create Service Profiles

After you add and configure Cisco Unified Communications Manager services, you add them to a service profile. You can apply additional configuration in the service profile.

Procedure

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

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

The **Find and List UC Services** window opens.

Step 3 Select **Add New**.

The **Service Profile Configuration** window opens.

Step 4 Enter a name for the service profile in the **Name** field.

Step 5 Select **Make this the default service profile for the system** if you want the service profile to be the default for the cluster.

Note On Cisco Unified Communications Manager release 9.x only, users who have only instant messaging capabilities (IM only) must use the default service profile. For this reason, you should set the service profile as the default if you plan to apply the service profile to IM only users.

Step 6 Add your UC services, apply any additional configuration, and then select **Save**.

What to do next

Apply service profiles to end user configuration.

Apply Service Profiles

After you add UC services and create a service profile, you apply the service profile to users. When users sign in to Cisco Jabber, the client can then retrieve the service profile for that user from Cisco Unified Communications Manager.

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 Enter the appropriate search criteria to find existing users and then select a user from the list.

The **End User Configuration** window opens.

Step 4 Locate the **Service Settings** section.

Step 5 Select a service profile to apply to the user from the **UC Service Profile** drop-down list.

Important **Cisco Unified Communications Manager release 9.x only:** If the user has only IIM and Presence Service capabilities (IM only), you must select **Use Default**. For IM only users, Cisco Unified Communications Manager release 9.x always applies the default service profile regardless of what you select from the **UC Service Profile** drop-down list.

Step 6 Apply any other configuration as appropriate and then select **Save**.

Associate Users with Devices

On Cisco Unified Communications Manager version 9.x only, when the client attempts to retrieve the service profile for the user, it first gets the device configuration file from Cisco Unified Communications Manager. The client can then use the device configuration to get the service profile that you applied to the user.

For example, you provision Adam McKenzie with a CSF device named `CSFAKenzi`. The client retrieves `CSFAKenzi.cnf.xml` from Cisco Unified Communications Manager when Adam signs in. The client then looks for the following in `CSFAKenzi.cnf.xml`:

```
<userId  serviceProfileFile="identifier.cnf.xml">amckenzi</userId>
```

For this reason, if you are using Cisco Unified Communications Manager version 9.x, you should do the following to ensure that the client can successfully retrieve the service profiles that you apply to users:

- Associate users with devices.
- Set the **User Owner ID** field in the device configuration to the appropriate user. The client will retrieve the Default Service Profile if this value is not set.

Note A CSF should not be associated to multiple users if you intend to use different service profiles for these users.

Procedure

Step 1 Associate users with devices.

a) Open the **Unified CM Administration** interface.
b) Select **User Management** > **End User**.
c) Find and select the appropriate user.
   The **End User Configuration** window opens.
d) Select **Device Association** in the **Device Information** section.
e) Associate the user with devices as appropriate.
f) Return to the **End User Configuration** window and then select **Save**.

Step 2 Set the **User Owner ID** field in the device configuration.

a) Select **Device** > **Phone**.
b) Find and select the appropriate device.
   The **Phone Configuration** window opens.
c) Locate the **Device Information** section.
d) Select **User** as the value for the **Owner** field.
e) Select the appropriate user ID from the **Owner User ID** field.
f) Select **Save**.

Set Parameters on Phone Configuration for Desktop Clients

The client can retrieve configuration settings in the phone configuration from the following locations on Cisco Unified Communications Manager:

Enterprise Phone Configuration

Applies to the entire cluster.

Note For users with only IM and Presence Service capabilities (IM only), you must set phone configuration parameters in the **Enterprise Phone Configuration** window.

Common Phone Profile Configuration

Applies to groups of devices and takes priority over the cluster configuration.

Cisco Unified Client Services Framework (CSF) Phone Configuration

Applies to individual CSF devices and takes priority over the group configuration.

Parameters in Phone Configuration

The following table lists the configuration parameters you can set in the **Product Specific Configuration Layout** section of the phone configuration and maps corresponding parameters from the client configuration file:

Desktop Client Settings Configuration	Description
Video Calling	Enables or disables video capabilities. **Enabled (default)** Users can send and receive video calls. **Disabled** Users cannot send or receive video calls. **Restriction** This parameter is available only on the CSF device configuration.
File Types to Block in File Transfer	Restricts users from transferring specific file types. Set a file extension as the value, for example, `.exe`. Use a semicolon to delimit multiple values, for example, `.exe;.msi;.rar;.zip`
Automatically Start in Phone Control	Sets the phone type for users when the client starts for the first time. Users can change their phone type after the initial start. The client then saves the user preference and uses it for subsequent starts. **Enabled** Use the desk phone device for calls. **Disabled (default)** Use the software phone (CSF) device for calls.
Jabber For Windows Software Update Server URL	Specifies the URL to the XML file that holds client update information. The client uses this URL to retrieve the XML file from your web server. In hybrid cloud-based deployments, you should use the Cisco WebexAdministration Tool to configure automatic updates.
Problem Report Server URL	Specifies the URL for the custom script that allows users to submit problem reports.

Set Parameters on Phone Configuration for Mobile Clients

The client can retrieve configuration settings in the phone configuration from the following locations on Cisco Unified Communications Manager:

- Cisco Dual Mode for iPhone (TCT) Configuration — Applies to individual TCT devices and takes priority over the group configuration.
- Cisco Jabber for Tablet (TAB) Configuration — Applies to individual TAB devices and takes priority over the group configuration.

Parameters in Phone Configuration

The following table lists the configuration parameters you can set in the **Product Specific Configuration Layout** section of the phone configuration and maps corresponding parameters from the client configuration file:

Parameter	Description
On-Demand VPN URL	URL for initiating on-demand VPN. **Note** Applicable for iOS only.
Preset Wi-fi Networks	Enter the SSIDs for Wi-Fi networks (SSIDs) approved by your organization. Separate SSIDs with a forward slash (/). Devices do not connect to secure connect if connected to one of the entered Wi-Fi networks.
Default Ringtone	Sets the default ringtone to **Normal** or **Loud**.
Video Capabilities	Enables or disables video capabilities. • Enabled (default) — Users can send and receive video calls. • Disabled — Users cannot send or receive video calls.
Dial via Office **Note** TCT and BOT devices only.	Enables or disables Dial via Office. • Enabled — Users can dial via office. • Disabled (default) — Users cannot dial via office.

Create and Host Client Configuration Files

In on-premises and hybrid cloud-based deployments you can create client configuration files and host them on the Cisco Unified Communications Manager TFTP service.

In cloud-based deployments, you should configure the client with the Cisco WebEx Administration Tool. However, you can optionally set up a TFTP server to configure the client with settings that are not available in Cisco WebEx Administration Tool.

Important In most environments, the client does not require any configuration to connect to services. You should create a configuration file only if you require custom content such as:

- Automatic updates
- Problem reporting
- User policies and options

Important You must create a global configuration file to set up:

- Directory integration for on-premises deployments.
- Voicemail service credentials for hybrid-cloud deployments.

Client Configuration Files

Before you deploy configuration files, review the differences between global and group configuration files. To successfully deploy configuration files you should also review the requirements for configuration files such as supported encoding.

Review details about configuration files and understand requirements such as supported encoding.

Global Configuration Files

Global configuration files apply to all users. The client downloads the global configuration file from your TFTP server during the login sequence.

The default name for the global configuration file is `jabber-config.xml`.

Group Configuration Files

Note

- Group configuration files are supported on Cisco Jabber for Windows and on Cisco Jabber for mobile devices.
- Group configuration files apply to subsets of users. Group configuration files take priority over global configuration files.

Group Configuration File Names

You specify the name of the group configuration files in the **Cisco Support Field** on the CSF, BOT, TCT, or TAB 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, the client 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, BOT, TCT, or TAB device configuration by deleting the entire `configurationFile=`*`group_configuration_file_name.xml`* string or by deleting the group configuration filename from the string.

Configuration File Requirements

- Configuration filenames are case sensitive. Use lowercase letters in the filename to prevent errors and to ensure the client can retrieve the file from the TFTP server.
- You must use utf-8 encoding for the configuration files.
- The client 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.
- Your XML can contain only valid XML character entity references. For example, use `&amp;` instead of `&`. If your XML contains invalid characters, the client cannot parse the configuration file.

Tip Open your configuration file in Microsoft Internet Explorer to see 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.

Specify Your TFTP Server Address

The client gets configuration files from a TFTP server. The first step in configuring the client is to specify your TFTP server address so the client can access your configuration file.

Attention If Cisco Jabber 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.

Specify Your TFTP Server on Cisco Unified Presence

If you are using Cisco Unified Communications Manager release 8.x, complete the steps to specify the address of your TFTP server on Cisco Unified Presence. If you are using Cisco Unified Communications Manager release 9.x, then you do not need to follow the steps below.

Procedure

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

Step 2 Select **Application** > **Cisco Jabber** > **Settings**.

Note In some versions of Cisco Unified Presence, this path is as follows: **Application** > **Cisco Unified Personal Communicator** > **Settings**.

The **Cisco Jabber Settings** window opens.

Step 3 Locate the fields to specify TFTP servers in one of the following sections, depending on your version of Cisco Unified Presence:

- **Cisco Jabber Security Settings**
- **CUPC Global Settings**

Step 4 Specify the IP address of your primary and backup TFTP servers in the following fields:

- **Primary TFTP Server**
- **Backup TFTP Server**
- **Backup TFTP Server**

Note Ensure that you enter the fully qualified domain name (FQDN) or IP address for the TFTP servers rather than a host name.

Step 5 Select **Save**.

Specify Your TFTP Server on Cisco Unified Communications Manager IM and Presence Service

If you are using Cisco Unified Communications Manager release 9.x, then you do not need to follow the steps below.

Procedure

Step 1 Open the **Cisco Unified CM IM and Presence Administration** interface.

Step 2 Select **Application** > **Legacy Clients** > **Settings**.

The **Legacy Client Settings** window opens.

Step 3 Locate the **Legacy Client Security Settings** section.

Step 4 Specify the IP address of your primary and backup TFTP servers in the following fields:

- **Primary TFTP Server**
- **Backup TFTP Server**
- **Backup TFTP Server**

Step 5 Select **Save**.

Specify TFTP Servers in Phone Mode

If you deploy the client in phone mode you can provide the address of the TFTP server as follows:

- 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.

Specify TFTP Servers with the Cisco WebEx Administration Tool

If the client connects to the Cisco WebEx Messenger service, you specify your TFTP server address with the Cisco WebEx Administrator Tool.

Procedure

Step 1 Open the Cisco WebEx Administrator Tool.

Step 2 Select the **Configuration** tab.

Step 3 Select **Unified Communications** in the **Additional Services** section.
The **Unified Communications** window opens.

Step 4 Select the **Clusters** tab.

Step 5 Select the appropriate cluster from the list.
The **Edit Cluster** window opens.

Step 6 Select **Advanced Server Settings** in the **Cisco Unified Communications Manager Server Settings** section.

Step 7 Specify the IP address of your primary TFTP server in the **TFTP Server** field.

Step 8 Specify the IP address of your backup TFTP servers in the **Backup Server #1** and **Backup Server #2** fields.

Step 9 Select **Save**.
The **Edit Cluster** window closes.

Step 10 Select **Save** in the **Unified Communications** window.

Create Global Configurations

The client downloads the global configuration file from your TFTP server during the login sequence. Configure the client for all users in your deployment.

Before you begin

If the structure of your configuration file is not valid, the client cannot read the values you set. Review the XML samples in this chapter for more information.

Procedure

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

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

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

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

If your environment has multiple TFTP servers, ensure that the configuration file is the same on all TFTP servers.

Create Group Configurations

Group configuration files apply to subsets of users and are supported on Cisco Jabber for desktop (CSF devices) and on Cisco Jabber for mobile devices. Group configuration files take priority over global configuration files.

If you provision users with CSF devices, specify the group configuration filenames in the **Cisco Support Field** field on the device configuration. If users do not have CSF devices, set a unique configuration filename for each group during installation with the TFTP_FILE_NAME argument.

Before you begin

- If you have Cisco Unified Communications Manager 8.6, the **Cisco Support Field** field does not exist. Download the ciscocm.addcsfsupportfield.cop COP file from the Cisco Jabber administration package to your file system and deploy to Cisco Unified Communications Manager. For more information about deploying COP files, see the Cisco Unified Communications Manager documentation.

  The COP file adds the **Cisco Support Field** field to CSF devices in the **Desktop Client Settings** section on the **Phone Configuration** window.

- If the structure of your configuration file is not valid, the client cannot read the values you set. Review the XML samples in this chapter for more information.

Procedure

Step 1 Create an XML group configuration file with any text editor.

The group configuration file can have any appropriate name; for example, `jabber-groupa-config.xml`.

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

Step 3 Add the group configuration file to applicable CSF devices.

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) In the **Phone Configuration** window, navigate to **Product Specific Configuration Layout** > **Desktop Client Settings**.
e) In the **Cisco Support Field** field, enter `configurationfile=`*`group_configuration_file_name.xml`*. For example, enter `configurationfile=groupa-config.xml`.

Note 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; for example, `configurationfile=/customFolder/groupa-config.xml`.

Do not add more than one group configuration file. The client uses only the first group configuration in the **Cisco Support Field** field.

f) Select **Save**.

Step 4 Host the group configuration file on your TFTP server.

Host Configuration Files

You can host configuration files on any TFTP server. However, Cisco recommends hosting configuration files on the Cisco Unified Communications Manager TFTP server, which is the same as that where the device configuration file resides.

Procedure

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

Step 2 Select **Software Upgrades** > **TFTP File Management**.

Step 3 Select **Upload File**.

Step 4 Select **Browse** in the **Upload File** section.

Step 5 Select the configuration file on the file system.

Step 6 Do not specify a value in the **Directory** text box in the **Upload File** section.

You should leave an empty value in the **Directory** text box so that the configuration file resides in the default directory of the TFTP server.

Step 7 Select **Upload File**.

Restart Your TFTP Server

You must restart your TFTP server before the client 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

You create client configuration files in an XML format that contains the following elements

XML Declaration

The configuration file must conform to XML standards and contain the following declaration:

```
<?xml version="1.0" encoding="utf-8"?>
```

Root Element

The root element config, contains all group elements. You must also add the version attribute to the root element as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
</config>
```

Group Elements

Group elements contain configuration parameters and values. You must nest group elements within the root element.

Group Elements and Parameters

The following table describes the group elements you can specify in a client configuration file:

Element	Description
Client	Contains configuration parameters for the client.
Directory	Contains configuration parameters for directory integration.
Options	Contains configuration parameters for user options.
Phone	Contains configuration parameters for phone services.
Policies	Contains configuration parameters for policies.
Presence	Contains configuration parameters for presence options.
Voicemail	Contains configuration parameters for the voicemail service.

XML Structure

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

```
<Client>
  <parameter>value</parameter>
</Client>
<Directory>
  <parameter>value</parameter>
</Directory>
<Options>
  <parameter>value</parameter>
</Options>
<Phone>
  <parameter>value</parameter>
</Phone>
<Policies>
  <parameter>value</parameter>
</Policies>
<Presence>
  <parameter>value</parameter>
</Presence>
<Voicemail>
  <parameter>value</parameter>
</Voicemail>
```

Summary of Configuration Parameters

The following table lists all the parameters you can include in the client configuration:

Parameter	Group Element
PrtLogServerUrl	Client
UpdateUrl	Client
jabber-plugin-config	Client
Forgot_Password_URL	Client
Persistent_Chat_Enabled	Client
Mention_P2Pchat	Client
Mention_GroupChat	Client
Mention_PersistentChat	Client
spell_check_enabled	Client
Disable_IM_History	Client
Set_Status_Away_On_Inactive	Options
Set_Status_Inactive_Timeout	Options
Set_Status_Away_On_Lock_OS	Options
StartCallWithVideo	Options
Start_Client_On_Start_OS	Options
AllowUserCustomTabs	Options
ShowContactPictures	Options

Parameter	Group Element
ShowOfflineContacts	Options
DockedWindowVisible	Options
DockedWindowPosition	Options
Callhistory_Expire_Days	Options
DeviceAuthenticationPrimaryServer	Phone
DeviceAuthenticationBackupServer	Phone
TftpServer1	Phone
TftpServer2	Phone
CtiServer1	Phone
CtiServer2	Phone
useCUCMGroupForCti	Phone
CcmcipServer1	Phone
CcmcipServer2	Phone
Meeting_Server_Address	Phone
Meeting_Server_Address_Backup	Phone
Meeting_Server_Address_Backup2	Phone
EnableDSCPPacketMarking	Phone
EnableVideo	Policies
InitialPhoneSelection	Policies
UserDefinedRemoteDestinations	Policies
enableLocalAddressBookSearch	Policies
EnableAccessoriesManager	Policies
BlockAccessoriesManagerPlugins	Policies
ForceFontSmoothing	Policies
Screen_Capture_Enabled	Policies
File_Transfer_Enabled	Policies
Disallowed_File_Transfer_Types	Policies
EnableBFCPVideoDesktopShare	Policies
Meetings_Enabled	Policies
Telephony_Enabled	Policies
Voicemail_Enabled	Policies
EnableTelProtocolHandler	Policies

Parameter	Group Element
EnableIMProtocolHandler	Policies
EnableSIPProtocolHandler	Policies
EnableSaveChatToFile	Policies
EnableSIPURIDialling	Policies
DirectoryURI BDIDirectoryURI	Policies
ForceC2XDirectoryResolution	Policies
ServiceDiscoveryExcludedServices	Policies
VoiceServicesDomain	Policies
ctiwindowbehaviour	Policies
EnableCallPickup	Policies
EnableGroupCallPickup	Policies
EnableOtherGroupPickup	Policies
EnableHuntGroup	Policies
PreventDeclineOnHuntCall	Policies
TelemetryEnabled	Policies
TelemetryCustomerID	Policies
TelemetryEnabledOverCellularData	Policies
EnableTelProtocolPopupWindow CiscoTelProtocolPermissionEnabled	Policies
EnableP2PDesktopShare	Policies
Customize_Phone_Server	Policies
Customize_Voicemail_Server	Policies
ServicesDomainSsoEmailPrompt	Policies
EnableForensicsContactData	Policies
LoginResource	Presence
PresenceServerAddress	Presence
PresenceServerURL	Presence
VoiceMailService_UseCredentialsFrom	Voicemail
VoicemailPrimaryServer	Voicemail

Related Topics

Group Elements and Parameters, on page 332

Client Parameters, on page 336

Options Parameters, on page 339
Phone Parameters, on page 342
Policies Parameters, on page 345
Presence Parameters, on page 357
Service Credentials Parameters, on page 358
Voicemail Parameters, on page 359
Integrate with Directory Sources

Example Configuration

The following is an example of a configuration file used in an on-premises deployment for all clients:

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
 <Client>
  <PrtLogServerUrl>http://server_name:port/path/prt_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>
  <Options>
    <Set_Status_Inactive_Timeout>20</Set_Status_Inactive_Timeout>
    <StartCallWithVideo>false</StartCallWithVideo>
  </Options>
  <Policies>
    <Disallowed_File_Transfer_Types>.exe;.msi</Disallowed_File_Transfer_Types>
  </Policies>
  <Directory>
  <BDIPresenceDomain>example.com</BDIPresenceDomain>
    <BDIPrimaryServerName>dir.example.com</BDIPrimaryServerName>
    <BDISearchBase1>ou=staff,dc=example,dc=com</BDISearchBase1>
    <BDIConnectionUsername>ad_jabber_access@example.com</BDIConnectionUsername>
    <BDIConnectionPassword>jabber</BDIConnectionPassword>
    <BDIPhotoUriSubstitutionEnabled>True</BDIPhotoUriSubstitutionEnabled>
    <BDIPhotoUriSubstitutionToken>sAMAccountName</BDIPhotoUriSubstitutionToken>
    <BDIPhotoUriWithToken>http://example.com/photo/sAMAccountName.jpg
    </BDIPhotoUriWithToken>
  </Directory>
</config>
```

Client Parameters

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

Parameter	Value	Description
PrtLogServerUrl	URL	Specifies the custom script for submitting problem reports.

Parameter	Value	Description
UpdateUrl	URL	Specifies the URL to the automatic updates XML definition file on your HTTP server. The client uses this URL to retrieve the update XML file. In hybrid cloud-based deployments, you should use the Cisco WebEx Administration Tool to configure automatic updates.
jabber-plugin-config	Plug-in definition	Contains plug-in definitions such as custom embedded tabs that display HTML content.
Forgot_Password_URL	URL	Specifies the URL of your web page for users to reset or retrieve forgotten passwords. In hybrid cloud-based deployments, you should use the Cisco WebEx Administration Tool to direct users to the web page to reset or retrieve forgotten passwords.
Persistent_Chat_Enabled	true false	Specifies whether the Persistent Chat feature is available in the client. **true** If the value is set to true, the Persistent Chat interface is shown in the client. **false (default)** The default value is assumed if the setting is not present in the configuration file.
Mention_P2Pchat	true false	Specifies whether mentions are enabled in person to person chat. **true (default)** Enables mentions in person to person chat. **false** Disables mentions in person to person chat.
Mention_GroupChat	true false	Specifies whether mentions are enabled in group chat. **true (default)** Enables mentions in group chat. **false** Disables mentions in group chat.
Mention_PersistentChat	true false	Specifies whether mentions are enabled in persistent chat. **true (default)** Enables mentions in persistent chat. **false** Disables mentions in persistent chat.

Parameter	Value	Description
spell_check_enabled	true false	Specifies whether spell check is enabled in the client. Spell check supports autocorrect, allows users to select the correct word from a list of suggestions, and add the word to a dictionary. Spell check has the following limitations: • Cisco Jabber for Windows supports spell check in Windows 8. • Spell check uses the built-in functionality of the operating system language. If the Cisco Jabber for Windows client language is different to the operating system language then spell check uses the operating system language • The shortcut keys for undo and redo (Ctrl-Z and Ctrl-Y) do not work when spell check is enabled. **true** Spell check is enabled. **false (default)** Spell check is disabled.
Disable_IM_History	true false	Specifies whether to retain chat history after participants close the chat window. **Note** This parameter is not available for IM-only deployments. **true** Do not retain chat history after participants close the chat window. **false (default)** Retain chat history: • After participants close the chat window. • Until the participants sign out. If the participants re-open the chat window, the last 99 messages show. Message archiving should be disabled on the server.

Parameter	Value	Description
CachePasswordMobile	true false	Specifies whether the password is remembered or not on the client side. **true (default)** The password is prefilled and **Automatic sign-in** is shown. Users can allow the client to cache their password. This option allows users to automatically sign in when the client starts. **false** After the client successfully registers to the Cisco Unified Communications Manager, the password field is empty and **Automatic sign-in** is not shown. Users cannot allow the client to cache their password. Users must enter their password each time the client starts. **Note** The client displays **Automatic sign-in** on first sign-in, or if the user clears the application data.

Options Parameters

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

Parameter	Value	Description
Set_Status_Away_On_Inactive	true false	Specifies if the availability status changes to **Away** when users are inactive. **true (default)** Availability status changes to **Away** when users are inactive. **false** Availability status does not change to **Away** when users are inactive.
Set_Status_Inactive_Timeout	Number of minutes	Sets the amount of time, in minutes, before the availability status changes to **Away** if users are inactive. The default value is 15.

Parameter	Value	Description
Set_Status_Away_On_Lock_OS	true false	Specifies if the availability status changes to **Away** when users lock their operating systems. **true (default)** Availability status changes to **Away** when users lock their operating systems. **false** Availability status does not change to **Away** when users lock their operating systems.
StartCallWithVideo	true false	Specifies how calls start when users place calls. Calls can start with audio only or audio and video. **true (default)** Calls always start with audio and video. **false** Calls always start with audio only. **Important** Server settings take priority over this parameter in the client configuration file. However, if users change the default option in the client user interface, that setting takes priority over both the server and client configurations. Configure this setting on the server as follows: **Cisco Unified Presence** 1. Open the **Cisco Unified Presence Administration** interface. 2. Select **Application** > **Cisco Jabber** > **Settings**. 3. Select or clear the **Always begin calls with video muted** parameter and then select **Save**. **Cisco Unified Communications Manager version 9.x and higher** 1. Open the **Cisco Unified CM Administration** interface. 2. Select **System** > **Enterprise Parameters**. 3. Set a value for the **Never Start Call with Video** parameter and then select **Save**.

Parameter	Value	Description
Start_Client_On_Start_OS	true false	Specifies if the client starts automatically when the operating system starts. **true** The client starts automatically. **false (default)** The client does not start automatically.
AllowUserCustomTabs	true false	Specifies if users can create their own custom embedded tabs. **true (default)** Users can create custom embedded tabs. **false** Users cannot create custom embedded tabs. **Note** This parameter affects only custom embedded tabs that users create. • If you allow users to create custom embedded tabs, they cannot modify or remove the tabs that you define in the client configuration. • If you do not allow users to create custom embedded tabs, the tabs that you define are still available to users.
ShowContactPictures	true false	Specifies if contact pictures display in the contact list. **true (default)** Contact pictures display in the contact list. **false** Contact pictures do not display in the contact list.
ShowOfflineContacts	true false	Specifies if offline contacts display in the contact list. **true (default)** Offline contacts display in the contact list. **false** Offline contacts do not display in the contact list.

Parameter	Value	Description
DockedWindowVisible	TRUE FALSE	Specifies if the docked window displays when the client starts. **true (default)** The docked window displays when the client starts. **false** The docked window does not display when the client starts.
DockedWindowPosition	TopCenter TopLeft TopRight	Sets the position of the docked window on the user's screen. **TopCenter (default)** The position of the docked window is at the top center of the screen. **TopLeft** The position of the docked window is at the top left of the screen. **TopRight** The position of the docked window is at the top right of the screen.
Callhistory_Expire_Days	Number of days	Sets the number of days before the call history is deleted. If the value is 0 or not specified in the configuration file the call history is not deleted until the count exceeds the maximum number of stored calls.

Phone Parameters

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

Parameter	Value	Description
DeviceAuthenticationPrimaryServer	Hostname IP address FQDN	Specifies the address of the primary instance of Cisco Unified Communications Manager to which users authenticate in phone mode deployments. Set one of the following as the value: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*hostname.domain.com*) This parameter can only be used in Cisco Jabber 9.6 and 9.7.

Parameter	Value	Description
DeviceAuthenticationBackupServer	Hostname IP address FQDN	Specifies the address of the backup instance of Cisco Unified Communications Manager to which users authenticate in phone mode deployments. Set one of the following as the value: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*hostname.domain.com*) This parameter can only be used in Cisco Jabber 9.6 and 9.7
TftpServer1	Hostname IP address 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*) You should set this parameter in the client configuration only if: • You deploy the client in phone mode. • The TFTP server address for the device configuration is different to the TFTP server address for the client configuration. During installation, you should set the address of the TFTP server where the client configuration file resides with the following argument: TFTP.
TftpServer2	Hostname IP address FQDN	Specifies the address of the secondary Cisco Unified Communications Manager TFTP service. This parameter is optional.
CtiServer1	Hostname IP address FQDN	Specifies the address of the primary CTI server. You should specify a CTI server address in the client configuration if users have desk phone devices.
CtiServer2	Hostname IP address FQDN	Specifies the address of the secondary CTI server. This parameter is optional.

Parameter	Value	Description
useCUCMGroupForCti	true false	Specifies if the Cisco Unified CM Group handles load balancing for CTI servers. Set one of the following values: **true** The Cisco Unified CM 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 CM Group does not handle CTI load balancing.
CcmcipServer1	Hostname IP address 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 TFTP server address. If the address of the CCMCIP server is the same as the TFTP server address, the client can use the TFTP server address to connect to the CCMCIP server. • In deployments with Cisco Unified Communications Manager version 8. In deployments with Cisco Unified Communications Manager version 9 and higher, the client can discover the CCMCIP server if you provision the `_cisco-uds` SRV record. Cisco Unified Communications Manager release 9.x and earlier—If you enable Cisco Extension Mobility, the `Cisco Extension Mobility` service must be activated on the Cisco Unified Communications Manager nodes that are used for CCMCIP. For information about Cisco Extension Mobility, see the *Feature and Services* guide for your Cisco Unified Communications Manager release.
CcmcipServer2	Hostname IP address FQDN	Specifies the address of the secondary CCMCIP server. This parameter is optional.

Parameter	Value	Description
Meeting_Server_Address	Cisco WebEx meetings site URL	Specifies the primary Cisco WebEx meeting site URL for users. The client populates this meeting site in the user's host account on the **Options** window. Users can enter their credentials to set up the host account and access their Cisco WebEx meetings, if the meeting site requires credentials. The client populates the meeting site in the user's host account on the **Preferences** > **Meetings** window. Users can enter their credentials to set up the host account and access their meetings site, if the Cisco WebEx meeting site requires credentials. **Important** If you specify an invalid meeting site, users cannot add, or edit, any meetings sites in the client user interface. This parameter is optional.
Meeting_Server_Address_Backup	Cisco WebEx meetings site URL	Specifies the secondary Cisco WebEx meeting site URL for users. This parameter is optional.
Meeting_Server_Address_Backup2	Cisco WebEx meetings site URL	Specifies the tertiary Cisco WebEx meeting site URL for users. This parameter is optional.
EnableDSCPPacketMarking	true false	Specifies if DSCP marking is applied to the packets: **true (default)** DSCP marking is enabled and the checkbox in the client is not shown. **false** DSCP marking is not made to packets and the checkbox in the client is not shown.

Related Topics

TFTP Server Address, on page 400

Policies Parameters

Policies parameters let you control specific client functionality.

On-Premises Policies

The following table describes the parameters you can specify within the Policies element in on-premises deployments:

Parameter	Value	Description
Screen_Capture_Enabled	true false	Specifies if users can take screen captures. **true (default)** Users can take screen captures. **false** Users cannot take screen captures.
File_Transfer_Enabled	true false	Specifies if users can transfer files to each other. **true (default)** Users can transfer files to each other. **false** Users cannot transfer files to each other.
Disallowed_File_Transfer_Types	File extension	Restricts users from transferring specific file types. Set file extensions as the value, for example, `.exe`. Use a semicolon to delimit multiple file extensions, for example, `.exe;.msi;.rar;.zip`.
Customize_Phone_Server	true false	Allows users to change their phone server settings in the client in on-premises deployments. Do not set this parameter to true if you are deploying SAML SSO, as changing phone server settings could interfere with SSO working properly. **true** Users can change their phone server settings. **false (default)** Users cannot change their phone server settings.
Customize_Voicemail_Server	true false	Allows users to change their voicemail server settings in the client in on-premises deployments. Do not set this parameter to true if you are deploying SAML SSO, as changing voicemail server settings could interfere with SSO working properly. **true** Users can change their voicemail server settings. **false (default)** Users cannot change their voicemail server settings.

Related Topics

Common Policies, on page 347

Cisco WebEx Policies, on page 357

Common Policies

The following table describes the parameters you can specify within the Policies element in both on-premises deployments and hybrid cloud-based deployments:

Parameter	Value	Description
EnableVideo	true false	Enables or disables video capabilities. **true (default)** Users can make and receive video calls. **false** Users cannot make or receive video calls.
InitialPhoneSelection	deskphone softphone	Sets the phone type for users when the client starts for the first time. Users can change their phone type after the initial start. The client then saves the user preference and uses it for subsequent starts. **deskphone** Use the desk phone device for calls. **softphone (default)** Use the software phone (CSF) device for calls. The client selects devices in the following order: **1.** Software phone devices **2.** Desk phone devices If you do not provision users with software phone devices, the client automatically selects desk phone devices.
UserDefinedRemoteDestinations	true false	Lets users add, edit, and delete remote destinations through the client interface. Use this parameter to change the default behavior when you provision Extend and Connect capabilities. By default, if a user's device list contains only a CTI remote device, the client does not let that user add, edit, or delete remote destinations. This occurs to prevent users from modifying dedicated remote devices that you assign. However, if the user's device list contains a software device or a desk phone device, the client lets users add, edit, and delete remote destinations. **true** Users can add, edit, and delete remote destinations. **false (default)** Users cannot add, edit, and delete remote destinations.

Parameter	Value	Description
enableLocalAddressBookSearch	true false	Lets users search for and add local Microsoft Outlook contacts to their contact lists. **true (default)** Users can search for and add local contacts to their contact lists. **false** Users cannot search for or add local contacts to their contact lists.
EnableAccessoriesManager	true false	Enables the accessories API in the client. This API lets accessory vendors create plugins to enable call management functionality for devices such as headsets. **true (default)** Enable the accessories API. **false** Disable the accessories API.

BlockAccessoriesManagerPlugins	Plugin library	Disables specific Accessories Manager plugins from third party vendors such as Jabra or Logitech. You should set the name of the plugin DLL file as the value. Use a comma to separate multiple values, for example, on Microsoft Windows:
		`<BlockAccessoriesManagerPlugins>`
		`JabraJabberPlugin.dll,lucpcisco.dll`
		`</BlockAccessoriesManagerPlugins>`
		There is no default value.

ForceFontSmoothing	true false	Specifies if the client applies anti-aliasing to smooth text. **true (default)** The client applies anti-aliasing to text. **false** The operating system applies anti-aliasing to text.

Parameter	Value	Description
EnableBFCPVideoDesktopShare	true false	Enables BFCP video desktop sharing capabilities. **true (default)** Enables BFCP video desktop sharing on the client. **false** Disables BFCP video desktop sharing. **Note** BFCP video desktop sharing is enabled on the server as follows: • On Cisco Unified Communications Manager version 8.x and lower, you must select the **Allow Presentation Sharing using BFCP** checkbox. • On Cisco Unified Communications Manager version 9.x and higher, BFCP video desktop sharing is enabled by default.
Meetings_Enabled	true false	Enables meetings capabilities in the client. Works in conjunction with the CalendarIntegrationType parameter. **true (default)** Enables meetings capabilities, allowing you to create meetings and get reminders to join meetings. **false** Disables meetings capabilities and user interface.
CalendarIntegrationType	0 1	This parameter works in conjunction with the Meetings_Enabled parameter. **0** Disables calendar integration in the Meetings tab of the client user interface. If you disable this parameter, the Meetings tab in the client is empty, but the Meetings tab remains on the hub window. **1** Enables calendar integration in the Meetings tab of the client user interface.

Parameter	Value	Description
Telephony_Enabled	true false	Enables audio and video capabilities and user interface in the client. **true (default)** Enables audio and video capabilities and user interface. **false** Disables audio and video capabilities and user interface. If you are upgrading to this release, and your client is enabled for IM-only mode, then you must set this parameter to false. If you do not set this parameter in IM-only mode deployments, then users may see disabled telephony capabilities on their user interface.
Voicemail_Enabled	true false	Enables voicemail capabilities and user interface in the client. **true (default)** Enables voicemail capabilities and user interface. **false** Disables voicemail capabilities and user interface.
EnableTelProtocolHandler	true false	Specifies if the client registers as the protocol handler for the `tel:` URI. **true (default)** The client registers as the protocol handler for the `tel:` URI. **false** The client does not register as the protocol handler for the `tel:` URI.
EnableIMProtocolHandler	true false	Specifies if the client registers as the protocol handler for the `IM:` URI or `XMPP`: URI. **true (default)** The client registers as the protocol handler for the `IM:` URI or `XMPP`: URI. **false** The client does not register as the protocol handler for the `IM:` URI or `XMPP`: URI.

Parameter	Value	Description
EnableSIPProtocolHandler	true false	Specifies if the client registers as the protocol handler for the `SIP:` URI. **true (default)** The client registers as the protocol handler for the `SIP:` URI. **false** The client does not register as the protocol handler for the `SIP:` URI.
EnableSaveChatToFile	true false	Allows users to save their chats to the file system as HTML. **true (default)** Users can save their chats to file. **false** Users cannot save their chats to file.
EnableSIPURIDialling	true false	Enables URI dialing with Cisco Jabber and allows users to make calls with URIs. **true** Users can make calls with URIs. **false (default)** Users cannot make calls with URIs.

Parameter	Value	Description
DirectoryURI BDIDirectoryURI	Directory attribute	Specifies the directory attribute that holds the SIP URI for users. **On-Premises Deployments** Set one of the following as the value: • mail • msRTCSIP-PrimaryUserAddress **Cloud-Based Deployments** Set one of the following as the value: • mail • imaddress • workphone • homephone • mobilephone The mail attribute is used by default. **Important** The value you specify must match the directory URI setting for users in Cisco Unified Communications Manager or the Cisco WebEx Administration Tool.
ForceC2XDirectoryResolution	true false	Specifies if the client queries the directory to resolve contact information when users perform click-to-x actions. **true (default)** The client queries the directory when users perform click-to-x actions. **false** The client does not query the directory for click-to-x actions. **Note** This parameter does not take effect when users connect to the corporate network through Expressway for Mobile and Remote Access. In this case, UDS provides contact resolution and the client cannot query the directory.

Parameter	Value	Description

ServiceDiscoveryExcludedServices	WEBEX
	CUCM
	CUP
		Specifies whether to exclude certain services from Service Discovery.
		WEBEX
		When you set this value, the client:
		- Does not perform CAS lookup
		- Looks for `_cisco-uds`, `_cuplogin`, and `_collab-edge`
		CUCM
		When you set this value, the client:
		- Does not look for `_cisco_uds`
		- Looks for `_cuplogin` and `_collab-edge`
		CUP
		When you set this value, the client:
		- Does not look for `_cuplogin`
		- Looks for `_cisco-uds_collab-edge`
		You can specify multiple, comma-separated values to exclude multiple services. For example:
		`<ServiceDiscoveryExcludedServices>`
		`WEBEX,CUCM`
		`</ServiceDiscoveryExcludedServices>`

VoiceServicesDomain	FQDN	Specifies the Fully Qualified Domain Name that represents the DNS domain where the DNS SRV records for *_collab-edge* and *_cisco-uds* are configured. **Example:** Given the following DNS SRV records: - *_collab-edge.*_tls.voice.example.com - *_cisco-uds.*_tcp.voice.example.com The *VoiceServicesDomain* value would be *voice.example.com*.

Parameter	Value	Description
ctiwindowbehaviour	OnVideo OnCall Never	Specifies the behavior of the conversation window when the user has answered a call in deskphone control mode (CTI mode). **OnVideo** Conversation window is only displayed for video calls. This option is not supported on Cisco Jabber for Mac. **OnCall (default)** Conversation window is always displayed when a call is answered. **Never** Conversation window is never displayed when a call is answered.
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.
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.
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
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.

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.
TelemetryEnabled	true false	Specifies whether analytics data will be gathered. **true (default)** Analytics data will be gathered. **false** Analytics data will not be gathered.
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.

Parameter	Value	Description
TelemetryEnabledOverCellularData	true false	Specifies whether analytics data will be sent over Wi-Fi only. **true (default)** Analytics data will be sent over Wi-Fi and mobile data connections. **false** Analytics data will be sent over Wi-Fi connections only. This parameter is optional.
EnableTelProtocolPopupWindow CiscoTelProtocolPermissionEnabled	true false	Specifies whether the pop-up window is enabled or disabled which asks users to confirm if they want to make a call after they click on a ciscotel:uri enabled number. **true (default)** Pop-up window is enabled and users are asked to confirm that they want to place the call. **false** Pop-up window is disabled and the call is made without requesting confirmation first. This may cause accidental or unwanted calls. **Note** The CiscoTelProtocolPermissionEnabled parameter replaces the EnableTelProtocolPopupWindow parameter. Both parameters are supported in the client, however the pop-up window is disabled if either parameter is set to false.
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.
EnableP2PDesktopShare	true false	Allows users to share their screen if not on a call. **true (Default)** Allows users to share their screens. **false** Users cannot do peer to peer screen sharing.

Parameter	Value	Description
EnableForensicsContactData	true false	Specifies whether users' Contacts folder is collected by the Problem Reporting Tool (PRT) when reporting a problem that is related to their contacts. **true (default)** Contacts folder is collected by the PRT tool. **false** Contacts folder is not collected by the PRT tool.

Related Topics

On-Premises Policies, on page 346
Cisco WebEx Policies, on page 357

Cisco WebEx Policies

If you use the Cisco WebEx Messenger service for instant messaging and presence capabilities, you can set policies for the client through the Cisco WebEx Administration Tool. See *Using policy actions available in Cisco WebEx* for a list of available policies and descriptions.

Related Topics

On-Premises Policies, on page 346
Common Policies, on page 347
Using policy actions available in Cisco WebEx

Presence Parameters

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

Parameter	Value	Description
LoginResource	multiResource wbxconnect	Controls user log in to multiple client instances. **multiResource (default)** Users can log in to multiple instances of the client at the same time. **wbxconnect** Users can log in to one instance of the client at a time. The client appends the `wbxconnect` suffix to the user's JID. Users cannot log in to any other Cisco Jabber client that uses the `wbxconnect` suffix.

Parameter	Value	Description
PresenceServerAddress	Hostname IP address FQDN	Specifies the address of a presence server for on-premises deployments. Set one of the following as the value: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*hostname.domain.com*)
PresenceServerURL	CAS URL	Specifies the Central Authentication Service (CAS) URL for the Cisco WebEx Messenger service. The following is an example of a URL you can set as the value: `https://loginp.webexconnect.com/cas/sso/ex_org/orgadmin.app`
CalendarWebExMeetingPresence	true false	Enables users' presence to change to "In a WebEx meeting" even if they do not join the WebEx session link but the meeting is in their Microsoft Outlook calendar. **true** Users' presence changes to "In a WebEx meeting" even if they do not join the WebEx session link. **false (default)** Users must join the WebEx session link for their presence to change to "In a WebEx meeting". Otherwise, their presence remains "Available", even if the meeting is in their Microsoft Outlook calendar.

Service Credentials Parameters

You can specify service credentials parameters so that users do not need to authenticate with certain services.

Voicemail Service Credentials

You can specify the following parameter to configure voicemail service credentials within the Voicemail element:

Parameter	Value	Description
VoiceMailService_UseCredentialsFrom	phone	Specifies that the client uses the phone service credentials to access voicemail services. Ensure the user's phone service credentials match their voicemail service credentials. If you set this configuration, users cannot specify voicemail service credentials in the client interface. This parameter is not set by default. You should set this parameter in the following deployments only: • Hybrid cloud-based deployments. • Phone mode deployments. In on-premises deployments, you should set the credentials source for voicemail services on the presence server.

The following is an example of the voicemail service credentials parameter:

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
  <Voicemail>
    <VoicemailService_UseCredentialsFrom>phone</VoicemailService_UseCredentialsFrom>
  </Voicemail>
</config>
```

Voicemail Parameters

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

Key	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*)

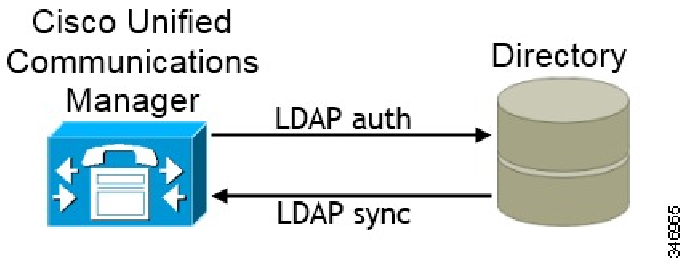
Related Topics

Service Credentials Parameters, on page 358

Set Up Directory Synchronization and Authentication

When you set up an on-premises deployment, you should configure Cisco Unified Communications Manager to do both of the following:

- Synchronize with the directory server.
- Authenticate with the directory server.



Synchronizing with the directory server replicates contact data from your directory to Cisco Unified Communications Manager.

Enabling authentication with the directory server lets Cisco Unified Communications Manager proxy authentication from the client to the directory server. In this way, users authenticate with the directory server, not with Cisco Unified Communications Manager or a presence server.

Related Topics

Configuring Cisco Unified Communications Manager Directory Integration

Synchronize with the Directory Server

Directory server synchronization ensures that contact data in your directory server is replicated to Cisco Unified Communications Manager.

Enable Synchronization

To ensure that contact data in your directory server is replicated to Cisco Unified Communications Manager, you must synchronize with the directory server. Before you can synchronize with the directory server, you must enable synchronization.

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 type of directory server from which you are synchronizing data from the **LDAP Server Type** drop-down list.

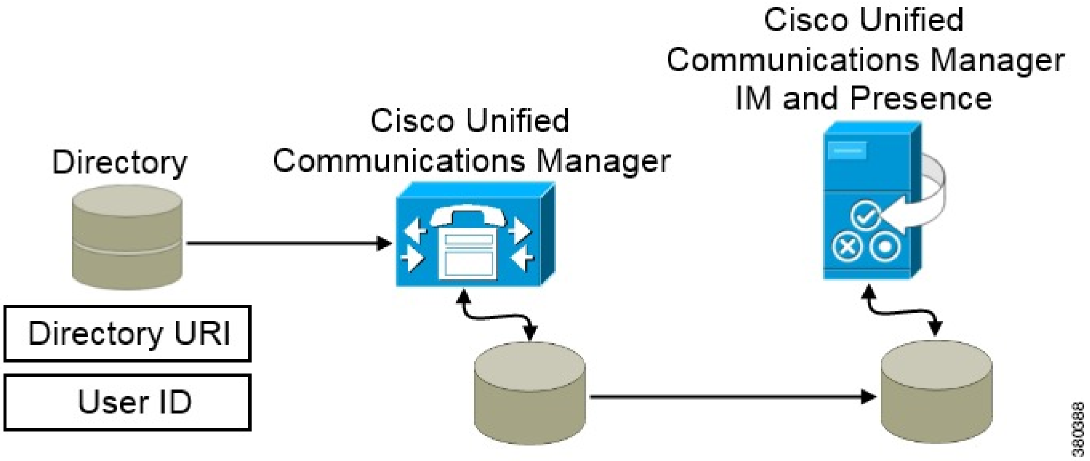
What to do next

Specify an LDAP attribute for the user ID.

Populate User ID and Directory URI

When you synchronize your LDAP directory server with Cisco Unified Communications Manager, you can populate the end user configuration tables in both the Cisco Unified Communications Manager and the Cisco Unified Communications Manager IM and Presence Service databases with attributes that contain values for the following:

- User ID — You must specify a value for the user ID on Cisco Unified Communications Manager. This value is required for the default IM address scheme and for users to sign in. The default value is `sAMAccountName`.
- Directory URI — You should specify a value for the directory URI if you plan to:
    - Enable URI dialing in Cisco Jabber.


Cisco Unified Communications Manager IM and Presence
Cisco Unified Communications Manager
Directory
Directory URI
User ID
380388

When Cisco Unified Communications Manager synchronizes with the directory source, it retrieves the values for the directory URI and user ID and populates them in the end user configuration table in the Cisco Unified Communications Manager database.

The Cisco Unified Communications Manager database then synchronizes with the Cisco Unified Communications Manager IM and Presence Service database. As a result, the values for the directory URI and user ID are populated in the end user configuration table in the Cisco Unified Communications Manager IM and Presence Service database.

Specify an LDAP Attribute for the User ID

When you synchronize from your directory source to Cisco Unified Communications Manager, you can populate the user ID from an attribute in the directory. The default attribute that holds the user ID is `sAMAccountName`.

Procedure

Step 1 Locate the **LDAP Attribute for User ID** drop-down list on the **LDAP System Configuration** window.

Step 2 Specify an attribute for the user ID as appropriate and then select **Save**.

Important If the attribute for the user ID is other than `sAMAccountName` and you are using the default IM address scheme in Cisco Unified Communications Manager IM and Presence Service, you must specify the attribute as the value for the parameter in your client configuration file as follows:

The EDI parameter is `UserAccountName`.

```
<UserAccountName>attribute-name</UserAccountName>
```

The BDI parameter is `BDIUserAccountName`.

```
<BDIUserAccountName>attribute-name</BDIUserAccountName>
```

If you do not specify the attribute in your configuration, and the attribute is other than `sAMAccountName`, the client cannot resolve contacts in your directory. As a result, users do not get presence and cannot send or receive instant messages.

Related Topics

Specify an LDAP Attribute for the Directory URI, on page 362

Specify an LDAP Attribute for the Directory URI

On Cisco Unified Communications Manager release 9.0(1) and later, you can populate the directory URI from an attribute in the directory.

Before you begin

Enable Synchronization.

Procedure

Step 1 Select **System** > **LDAP** > **LDAP Directory**.

Step 2 Select the appropriate LDAP directory or select **Add New** to add an LDAP directory.

Step 3 Locate the **Standard User Fields To Be Synchronized** section.

Step 4 Select one of the following LDAP attributes from the **Directory URI** drop-down list:

- **msRTCSIP-primaryuseraddress**—This attribute is populated in the AD when Microsoft Lync or Microsoft OCS are used. This is the default attribute.
- **mail**

Step 5 Select **Save**.

Related Topics

Specify an LDAP Attribute for the User ID, on page 361

Perform Synchronization

After you add a directory server and specify the required parameters, you can synchronize Cisco Unified Communications Manager with the directory server.

Before you begin

If your environment includes a presence server, you should ensure the following feature service is activated and started before you synchronize with the directory server:

- Cisco Unified Presence — **Cisco UP Sync Agent**
- Cisco Unified Communications Manager IM and Presence Service — **Cisco Sync Agent**

This service keeps data synchronized between the presence server and Cisco Unified Communications Manager. When you perform the synchronization with your directory server, Cisco Unified Communications Manager then synchronizes the data with the presence server. However, the **Cisco Sync Agent** service must be activated and started.

Procedure

Step 1 Select **System** > **LDAP** > **LDAP Directory**.

Step 2 Select **Add New**.

The **LDAP Directory** window opens.

Step 3 Specify the required details on the **LDAP Directory** window.

See the Cisco Unified Communications Manager Administration Guide for more information about the values and formats you can specify.

Step 4 Create an LDAP Directory Synchronization Schedule to ensure that your information is synchronized regularly.

Step 5 Select **Save**.

Step 6 Select **Perform 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 presence server database.

Authenticate with the LDAP Server

Perform this procedure if you want to enable LDAP authentication so that end user passwords are authenticated against the password that is assigned in the company LDAP directory. LDAP authentication gives system administrators the ability to assign an end user a single password for all company applications. This configuration applies to end user passwords only and does not apply to end user PINs or application user passwords. When users sign in to the client, the presence service routes that authentication to Cisco Unified

Communications Manager. Cisco Unified Communications Manager then sends that authentication to the directory server.

Procedure

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

Step 2 Select **System** > **LDAP** > **LDAP Authentication**.

Step 3 Select **Use LDAP Authentication for End Users**.

Step 4 Specify LDAP credentials and a user search base as appropriate.

See the *Cisco Unified Communications Manager Administration Guide* for information about the fields on the **LDAP Authentication** window.

Step 5 Select **Save**.

Federation

Federation lets Cisco Jabber users communicate with users who are provisioned on different systems and who are using client applications other than Cisco Jabber.

Interdomain Federation

Interdomain federation enables Cisco Jabber users in an enterprise domain to share availability and send instant messages with users in another domain.

- Cisco Jabber users must manually enter contacts from another domain.
- Cisco Jabber supports federation with the following:
  - Microsoft Office Communications Server
  - Microsoft Lync
  - IBM Sametime
  - XMPP standard-based environments such as Google Talk

    Note Expressway for Mobile and Remote Access doesn’t enable XMPP Interdomain federation itself. Cisco Jabber clients connecting over Expressway for Mobile and Remote Access can use XMPP Interdomain federation if it has been enabled on Cisco Unified Communications Manager IM and Presence.

  - AOL Instant Messenger

You configure interdomain federation for Cisco Jabber on Cisco Unified Communications Manager IM and Presence Service. See the appropriate server documentation for more information.

Related Topics

Integration Guide for Configuring Cisco Unified Presence Release 8.6 for Interdomain Federation

Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager

Intradomain Federation

Intradomain federation enables users within the same domain to share availability and send instant messages between Cisco Unified Communications Manager IM and Presence Service and Microsoft Office Communications Server, Microsoft Live Communications Server, or another presence server.

Intradomain federation allows you to migrate users to Cisco Unified Communications Manager IM and Presence Service from a different presence server. For this reason, you configure intradomain federation for Cisco Jabber on the presence server. See the following for more information:

- Cisco Unified Presence: *Integration Guide for Configuring Partitioned Intradomain Federation for Cisco Unified Presence Release 8.6 and Microsoft LCS/OCS*
- Cisco Unified Communications Manager IM and Presence Service: *Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager*

Configure Intradomain Federation for BDI or EDI

In addition to configuring intradomain federation on the presence server, you might need to specify some configuration settings in the Cisco Jabber configuration files.

To resolve contacts during contact search or retrieve contact information from your directory, Cisco Jabber requires the contact ID for each user. Cisco Unified Communications Manager IM & Presence server uses a specific format for resolving contact information that does not always match the format on other presence servers such as Microsoft Office Communications Server or Microsoft Live Communications Server.

The parameters that you use to configure intradomain federation depend on whether you use *Enhanced Directory Integration* (EDI) or *Basic Directory Integration* (BDI). EDI uses native Microsoft Windows APIs to retrieve contact data from the directory service and is only used by Cisco Jabber for Windows. For BDI, the client retrieves contact data from the directory service and is used by Cisco Jabber for Mac, Cisco Jabber for Android, and Cisco Jabber for iPhone and iPad.

Procedure

Step 1 Set the value of the relevant parameter to true:

- For BDI: BDIUseSipUriToResolveContacts
- For EDI: UseSIPURIToResolveContacts

Step 2 Specify an attribute that contains the Cisco Jabber contact ID that the client uses to retrieve contact information. The default value is `msRTCSIP-PrimaryUserAddress`, or you can specify another attribute in the relevant parameter:

- For BDI: BDISipUri
- For EDI: SipUri

Note When you deploy intradomain federation and the client connects with Expressway for Mobile and Remote Access from outside the firewall, contact search is supported only when the contact ID uses one of the following formats:

- sAMAccountName@domain
- UserPrincipleName (UPN)@domain
- EmailAddress@domain
- employeeNumber@domain
- phoneNumber@domain

Step 3 In the UriPrefix parameter, specify any prefix text that precedes each contact ID in the relevant SipUri parameter.

Example:

For example, you specify `msRTCSIP-PrimaryUserAddress` as the value of SipUri. In your directory the value of `msRTCSIP-PrimaryUserAddress` for each user has the following format: `sip:`*`username@domain`*.

- For BDI: BDIUriPrefix
- For EDI: UriPrefix

Example

The following XML snippet provides an example of the resulting configuration for BDI:

```
<Directory>
  <BDIUseSIPURIToResolveContacts>true</BDIUseSIPURIToResolveContacts>
  <BDISipUri>non-default-attribute</BDISipUri>
  <BDIUriPrefix>sip:</BDIUriPrefix>
</Directory>
```

The following XML snippet provides an example of the resulting configuration for EDI:

```
<Directory>
  <UseSIPURIToResolveContacts>true</UseSIPURIToResolveContacts>
  <SipUri>non-default-attribute</SipUri>
  <UriPrefix>sip:</UriPrefix>
</Directory>
```

Related Topics

Example of Intradomain Federation, on page 366

Example of Intradomain Federation

The following example shows how to create intradomain federation contacts using the following BDI or EDI parameters and example values:

For BDI: BDISipUri
For EDI: SipURI

Value: msRTCSIP-PrimaryUserAddress

For BDI: BDIUseSIPURIToResolveContacts
For EDI: UseSIPURIToResolveContacts

Value: true

For BDI: BDIUriPrefix
For EDI: UriPrefix

Value: sip

For the user Mary Smith, the directory contains **`sip:msmith@domain.com`** as the value of the msRTCSIP-PrimaryUserAddress attribute.

The following workflow describes how the client connects to your directory to resolve contact information for Mary Smith:

1. Your presence server passes `msmith@domain.com` to the client.
2. The client adds sip: to `msmith@domain.com` and then queries your directory.
3. `sip:msmith@domain.com` matches the value of the `msRTCSIP-PrimaryUserAddress` attribute.
4. The client retrieves contact information for Mary Smith.

When Cisco Jabber users search for Mary Smith, the client removes the sip: prefix from `sip:msmith@domain.com` to get her contact ID.

Related Topics

Configure Intradomain Federation for BDI or EDI, on page 365

Administer and Moderate Persistent Chat Rooms

Note

- Persistent Chat Rooms and their administration is for on-premises deployments only.
- Persistent Chat Rooms are not available for mobile clients.

You administer persistent chat rooms from the Jabber client by creating rooms, delegating their moderators, and specifying members. The node on which the room is created is created automatically, although you can override it and specify a specific node. Administrators and moderators are privileged users in Persistent Chat rooms. You can administer Persistent Chat rooms on any service node that you are an administrator for on Cisco Unified Communications Manager IM and Presence servers.

Administrator Capabilities

Administrators can perform the following tasks from the **All Rooms** tab of Persistent Chat in the client hub window:

- Create rooms. When you create a room, you automatically become the room administrator.

- Define and change up to 30 moderators for a chat room (who become *room owners*).
- Specify and change the room name.
- Define the maximum number of participants in a room. This number cannot be less than the number of participants already in a room.
- Add and remove room members.
- Block, remove, and revoke participants.
- Destroy rooms (which removes it from the server, but the history is not deleted).

Moderator Capabilities

Up to 30 moderators can be defined by an administrator for one Persistent Chat room. Moderators can perform the following tasks:

- Change the subject of a room.
- Edit members (which includes adding, removing, and banning them).

Room Creation

When creating a room, you can provide the following types of information:

- Room name (required, maximum 200 characters)
- Description
- Room type (public or restricted)

  After the room type has been defined, it cannot be changed by anyone.
- Specify whether to add the room to your **My Rooms** tab (off by default)
- Add up to 30 moderators (who must have a valid Jabber ID to moderate a room).
- Room password

After you create the room, you have the option to add members to the room immediately or at a later time. Refresh the **All Rooms** list in order to see your new room in the list of available rooms.

Problem Reporting

Applies to: Cisco Jabber for Windows

Setting up problem reporting enables users to send a summary of issues that they encounter with the client. There are two methods for submitting problem reports as follows:

- Users submit the problem report directly through the client interface.
- Users save the problem report locally and then upload it at a later time.

The client 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 that enables 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.

Configure Automatic Updates

Applies to: Cisco Jabber for Windows, Cisco Jabber for Mac

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. The client retrieves the XML file when users sign in, resume their computer from sleep mode, or perform a manual update request from the **Help** menu.

Note If you use the Cisco WebEx Messenger service for instant messaging and presence capabilities, you should use the Cisco WebEx Administration Tool to configure automatic updates.

XML File Structure

XML files for automatic updates have the following structure:

```
<JabberUpdate>
          <App name=”JabberWin”>
               <LatestBuildNum>12345</LatestBuildNum>
               <LatestVersion>10.5.x</LatestVersion>
               <Mandatory>true</Mandatory>
               <Message>
                  <![CDATA[<b>This new version of Cisco Jabber 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/jabber">here</a>.]]>
                 </Message>
                 <DownloadURL>http://http_server_name/CiscoJabberSetup.msi</DownloadURL>

            </App>
          </JabberUpdate>
```

Example XML File 1

The following is example XML file for automatic updates:

```
<JabberUpdate>
<App name="JabberWin">
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.x</LatestVersion>
  <Message><![CDATA[<b>This new version of Cisco Jabber 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/jabber">here</a>.]]></Message>
  <DownloadURL>http://http_server_name/CiscoJabberSetup.msi</DownloadURL>
</App>
</JabberUpdate>
```

Example XML File 2

The following is an example XML file for automatic updates for both Cisco Jabber for Windows and Cisco Jabber for Mac:

```
<JabberUpdate>
 <App name="JabberMac">
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.6.1</LatestVersion>
  <Message><![CDATA[<b>This new version of Cisco Jabber 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/jabber">here</a>.]]>
  </Message>

<DownloadURL>http://http_server_name/Cisco-Jabber-Mac-9.6.1-12345-MrbCdd.zip</DownloadURL>

 </App>
 <App name="JabberWin">
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.0</LatestVersion>
  <Message><![CDATA[<b>This new version of Cisco Jabber 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/jabber">here</a>.]]>
  </Message>
  <DownloadURL>http://http_server_name/CiscoJabberSetup.msi
  </DownloadURL>
</App>
</JabberUpdate>
```

Before you begin

- Install and configure an HTTP server to host the XML file and installation package.
- Ensure users have permission to install software updates on their workstations.

  Microsoft Windows stops update installations if users do not have administrative rights on their workstations. You must be logged in with administrative rights to complete installation.

Procedure

Step 1 Host the update installation program on your HTTP server.

Step 2 Create an update XML file with any text editor.

Step 3 Specify values in the XML as follows:

- `name`—Specify the following ID as the value of the `name` attribute for the `App` element:
  - JabberWin—The update applies to Cisco Jabber for Windows.
  - JabberMac—The update applies to Cisco Jabber for Mac.
- `LatestBuildNum`—Build number of the update.
- `LatestVersion`—Version number of the update.
- `Mandatory`—(Windows clients only) True or False. Determines whether users must upgrade their client version when prompted.
- `Message`—HTML in the following format:

  `<![CDATA[`*`your_html`*`]]>`
- `DownloadURL`—URL of the installation package on your HTTP server.

  For Cisco Jabber for Mac the URL file must be in the following format:

  `Cisco-Jabber-Mac-`*`version-size-dsaSignature`*`.zip`

Step 4 Save and close your update XML file.

Step 5 Host your update XML file on your HTTP server.

Step 6 Specify the URL of your update XML file as the value of the UpdateUrl 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 Jabber.

Note The Jabber embedded browser does not support cookie sharing with pop-ups from SSO enabled webpages. The content on the pop-up window may fail to load.

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>
```

Cisco 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.

Parameter	Description
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

Chats and Calls from Custom Tabs

You can use protocol handlers to start chats and calls from custom embedded tabs. Make sure the custom embedded tab is an HTML page.

Use the `XMPP:` or `IM:` protocol handler to start chats.
Use the `TEL:` protocol handler to start audio and video calls.

Related Topics

Protocol Handlers, on page 81

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

- onHubResized() — The client invokes this method when users resize or move the client hub window.
- onHubActivated() — The client invokes this method when the client hub windows is activated.
- onHubDeActivated() — The client invokes this method when the client hub window is deactivated.

Subscribe to Presence in Custom Tabs

You can use the following JavaScript functions to subscribe to the presence of a contact and receive presence updates from the client:

- SubscribePresence() — Specify a string value using the IM address of a user for this method.
- OnPresenceStateChanged — This method enables users to receive updates from the client on the presence of a contact. You can specify one of the following values as the string:
    - IM address
    - Basic presence (Available, Away, Offline, Do Not Disturb)
    - Rich presence (In a meeting, On a call, or a custom presence state)

Note

- If you subscribe to the presence of a person who is not on your contact list (also called *temporary presence subscription*), the subscription expires after 68 minutes. After the subscription expires, you must re-subscribe to the person's presence in order to continue to receive presence updates.
- Jabber for iPad and iPhone only supports OnPresenceStateChanged.

Get Locale Information in Custom Tabs

You can use the following JavaScript functions to retrieve the current locale information of a contact from the client:

- GetUserLocale() — This method enables users to request locale information from the client.
- OnLocaleInfoAvailable — This method enables users to receive locale information from client. You can use a string value that contains the client locale information.

Note Jabber for iPad and iPhone only supports OnLocaleInfoAvailable.

Example JavaScript

The following code is an example of an HTML page that uses JavaScript to display a form into which you can input a number from 1 to 999:

```
<html>
        <head>
                <script type="text/javascript">
                                 function OnPresenceStateChanged(jid, basicPresence,
localizedPresence)
                                 {
                                          var cell = document.getElementById(jid);
                                          cell.innerText = basicPresence.concat(",
",localizedPresence);
                                 }

                                 function GetUserLocale()
                                 {
```

```
                                          window.external.GetUserLocale();
                                 }

                                 function SubscribePresence()
                                 {

window.external.SubscribePresence('johndoe@example.com');
                                 }

                                 function OnLocaleInfoAvailable(currentLocale)
                                 {
                                       var cell = document.getElementById("JabberLocale");

                                          cell.innerText = currentLocale;
                                 }

                                 function onHubActivated()
                                 {
                                          var cell = document.getElementById("hubActive");
                                          cell.innerText = "TRUE";
                                 }

                                 function onHubDeActivated()
                                 {
                                          var cell = document.getElementById("hubActive");
                                          cell.innerText = "FALSE";
                                 }

                                 function onHubResized()
                                 {
                                          alert("Hub Resized or Moved");
                                 }

                                 function OnLoadMethods()
                                 {
                                          SubscribePresence();
                                          GetUserLocale();
                                 }
                     </script>
               </head>

               <body onload="OnLoadMethods()">
                     <table>
                                 <tr>
                                             <td>John Doe</td>
                                             <td id="johndoe@example.com">unknown</td>
                                 </tr>
                    </table>
                    <table>
                                 <tr>
                                             <td>Jabber Locale: </td>
                                             <td id="JabberLocale">Null</td>
                                 </tr>
                                 <tr>
                                             <td>Hub Activated: </td>
                                             <td id="hubActive">---</td>
                                 </tr>
                   </table>
               </body>
```

```
</html>
```

To test this example JavaScript form, copy the preceding example into an HTML page and then specify that page as a custom embedded tab.

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>
```

Custom Emoticons

Applies to: Cisco Jabber for Windows

You can add custom emoticons to Cisco Jabber for Windows by creating emoticon definitions in an XML file and saving it to the file system.

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

- Dimensions: 17 x 17 pixels
- Transparent background
- PNG file format
- RGB colors

Procedure

Step 1 Create a file named `emoticonDefs.xml` with any text editor.

Step 2 Specify the emoticon definitions as appropriate in `emoticonDefs.xml`.

See *Emoticon Definitions* for more information on the structure and available parameters for `emoticonDefs.xml`.

Step 3 Save and close `emoticonDefs.xml`.

Step 4 Save `emoticonDefs.xml` in the appropriate directory on the file system.

Cisco Jabber for Windows loads emoticon definitions from the following directories on the file system.

- The directory can differ depending on your operating system
  - For 32-bit operating systems:
    - `Program Files\Cisco Systems\Cisco Jabber\Emoticons`
    - `Program Files\Cisco Systems\Cisco Jabber\CustomEmoticons`
  - For 64-bit operating systems:
    - `Program Files(x86)\Cisco Systems\Cisco Jabber\Emoticons`
    - `Program Files(x86)\Cisco Systems\Cisco Jabber\CustomEmoticons`

  The `Emoticons` folder contains the default emoticons for Cisco Jabber for Windows and the default `emoticonDefs.xml`.

  The `CustomEmoticons` folder does not exist by default. Administrators can create this folder to contain custom emoticon definitions to include in organizational deployments.

  Emoticons that you define in the `CustomEmoticons` folder take precedence over emoticon definitions in the default `Emoticons` folder.

- *%USERPROFILE%*`\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF\CustomEmoticons`

  This folder contains custom emoticon definitions for individual instances of Cisco Jabber for Windows.

  Emoticons that you define in this directory take precedence over emoticon definitions in the `CustomEmoticons` folder in the installation directory.

Step 5 Restart Cisco Jabber for Windows.

Cisco Jabber for Windows loads the custom emoticon definitions in `emoticonDefs.xml`.

Remember Custom emoticon definitions are available to users only if they are defined locally in `emoticonDefs.xml`. If you send custom emoticons to users who do not have the same emoticon definitions, those users receive the default keys, not the icons; for example:

1. User A defines a custom emoticon in `emoticonDefs.xml`.

   The custom emoticon definition exists only on User A's local file system.

2. User A sends that custom emoticon to User B.
3. User B receives only the default key for the custom emoticon. User B does not receive the icon.

Emoticon Definitions

Cisco Jabber for Windows loads emoticon definitions from `emoticonDefs.xml`.

The following XML snippet shows the basic structure for the emoticon definitions file:

```
<emoticons>
 <emoticon defaultKey="" image="" text="" order="" hidden="">
  <alt></alt>
 </emoticon>
</emoticons>
```

The following table describes the elements and attributes for defining custom emoticons:

Element or attribute	Description
emoticons	This element contains all emoticon definitions.
emoticon	This element contains the definition of an emoticon.
defaultKey	This attribute defines the default key combination that renders the emoticon. Specify any key combination as the value. This attribute is required. defaultKey is an attribute of the emoticon element.
image	This attribute specifies the filename of the emoticon image. Specify the filename of the emoticon as the value. The emoticon image must exist in the same directory as `emoticonDefs.xml`. This attribute is required. Cisco Jabber for Windows supports any icon that Internet Explorer can render, including `.jpeg`, `.png`, and `.gif`. image is an attribute of the emoticon element.

Element or attribute	Description
text	This attribute defines the descriptive text that displays in the **Insert emoticon** dialog box. Specify any string of unicode characters. This attribute is optional. text is an attribute of the emoticon element.
order	This attribute defines the order in which emoticons display in the **Insert emoticon** dialog box. Specify an ordinal number beginning from 1 as the value. order is an attribute of the emoticon element. This attribute is required. However, if the value of hidden is `true` this parameter does not take effect.
hidden	This attribute specifies whether the emoticon displays in the **Insert emoticon** dialog box. Specify one of the following as the value: **true** Specifies the emoticon does not display in the **Insert emoticon** dialog box. Users must enter the key combination to render the emoticon. **false** Specifies the emoticon displays in the **Insert emoticon** dialog box. Users can select the emoticon from the **Insert emoticon** dialog box or enter the key combination to render the emoticon. This is the default value. This attribute is optional. hidden is an attribute of the emoticon element.
alt	This element enables you to map key combinations to emoticons. Specify any key combination as the value. For example, if the value of defaultKey is `:)`, you can specify `:-)` as the value of alt so that both key combinations render the same emoticon. This element is optional.

Remember The default emoticons definitions file contains the following key combinations that enable users to request calls from other users:

- :callme
- :telephone

These key combinations send the callme emoticon, or communicon. Users who receive this emoticon can click the icon to initiate an audio call. You should include these key combinations in any custom emoticons definition file to enable the callme emoticon.

Emoticon Definition Example

```
<emoticons>
 <emoticon defaultKey=":)" image="Emoticons_Smiling.png" text="Smile" order="1">
  <alt>:-)</alt>
  <alt>^_^</alt>
 </emoticon>
 <emoticon defaultKey=":(" image="Emoticons_Frowning.png" text="Frown" order="2">
  <alt>:-(</alt>
 </emoticon>
</emoticons>
```

CHAPTER 12

Install the Clients

Install Cisco Jabber for Windows

Cisco Jabber for Windows provides an MSI installation package that you can use in the following ways:

Install Option	Description
Use the Command Line, on page 386	You can specify arguments in a command line window to set installation properties. Choose this option if you plan to install multiple instances.
Run the MSI Manually, on page 388	Run the MSI manually on the file system of the client workstation and then specify connection properties when you start the client. Choose this option if you plan to install a single instance for testing or evaluation purposes.
Create a Custom Installer, on page 388	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.
Deploy with Group Policy, on page 391	Install the client on multiple computers in the same domain.

Before you begin

You must be logged in with local administrative rights.

Administrative Rights

You must be logged in with local administrative rights to complete installation of Cisco Jabber for Windows.

Add Local Contacts from Microsoft Outlook

Cisco Jabber for Windows lets users search for and add local contacts in Microsoft Outlook. To enable this integration with Microsoft Outlook, you must enable Cached Exchange Mode on the Microsoft Exchange server.

To search for local contacts in Microsoft Outlook with the client, users must have profiles set in Microsoft Outlook. In addition, users must do the following:

1. Select **File** > **Options**.
2. Select the **Integration** tab (**Calendar** tab from release 11.0).
3. Select either **None** or **Microsoft Outlook**.

To add local Microsoft Outlook contacts to contact lists in the client, local contacts must have instant message addresses in Microsoft Outlook.

To show contact photos in the client interface, local contacts in Microsoft Outlook must have instant message addresses.

To communicate with local contacts in Microsoft Outlook using the client, local contacts must have the relevant details. To send instant messages to contacts, local contacts must have an instant message address. To call contacts in Microsoft Outlook, local contacts must have phone numbers.

Microsoft Outlook Calendar Events

Applies to: Cisco Jabber for Windows

You must apply a setting in Microsoft Outlook so that calendar events display in Cisco Jabber for Windows.

Procedure

Step 1 Open the email account settings in Microsoft Outlook, as in the following example:

a) Select **File** > **Account Settings**.
b) Select the **Email** tab on the **Account Settings** window.

Step 2 Double-click the server name.

In most cases, the server name is **Microsoft Exchange**.

Step 3 Select the **Use Cached Exchange Mode** checkbox.

Step 4 Apply the setting and then restart Microsoft Outlook.

When users create calendar events in Microsoft Outlook, those events display in the **Meetings** tab.

Microsoft Outlook Presence Integration

Applies to: Cisco Jabber for Windows

To enable integration with Microsoft Outlook, you must specify `SIP:user@cupdomain` as the value of the `proxyAddresses` attribute in Microsoft Active Directory. Users can then share availability in Microsoft Outlook.

Use one of the following methods to modify the `proxyAddresses` attribute:

- **An Active Directory administrative tool such as Active Directory User and Computers**

  The Active Directory User and Computers administrative tool allows you to edit attributes on Microsoft Windows Server 2008 or later.

- **ADSchemaWizard.exe utility**

  The ADSchemaWizard.exe utility is available in the Cisco Jabber administration package. This utility generates an LDIF file that modifies your directory to add the `proxyAddresses` attribute to each user with the following value: `SIP:user@cupdomain`.

  You should use the ADSchemaWizard.exe utility on servers that do not support the edit attribute feature in the Active Directory User and Computers administrative tool. You can use a tool such as ADSI Edit to verify the changes that you apply with the ADSchemaWizard.exe utility.

  The ADSchemaWizard.exe utility requires Microsoft .NET Framework version 3.5 or later.

- **Create a script with Microsoft Windows PowerShell**

  Refer to the appropriate Microsoft documentation for creating a script to enable presence in Microsoft Outlook.

Enable Presence with the Active Directory User and Computers Tool

Complete the following steps to enable presence in Microsoft Outlook for individual users with the Active Directory User and Computers administrative tool:

Procedure

Step 1 Start the Active Directory User and Computers administrative tool.

You must have administrator permissions to run the Active Directory User and Computers administrative tool.

Step 2 Select **View** in the menu bar and then select the **Advanced Features** option from the drop-down list.

Step 3 Navigate to the appropriate user in the Active Directory User and Computers administrative tool.

Step 4 Double click the user to open the **Properties** dialog box.

Step 5 Select the **Attribute Editor** tab.

Step 6 Locate and select the `proxyAddresses` attribute in the **Attributes** list box.

Step 7 Select **Edit** to open the **Multi-valued String Editor** dialog box.

Step 8 In the **Value to add** text box, specify the following value: `SIP:user@cupdomain`.

For example, `SIP:msmith@cisco.com`.

Where the `user@cupdomain` value is the user's instant messaging address. `cupdomain` corresponds to the domain for Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.

Methods of Installation

Cisco Jabber for Windows provides an MSI installation package. You must be logged in as an administrator to complete installation. You can use this installation package in the following ways:

Use the Command Line

Specify arguments in a command line window to set installation properties.

Choose this option if you plan to install multiple instances.

Run the MSI Manually

Run the MSI manually on the file system of the client workstation and then specify connection properties when you start the client.

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

Create a Custom Installer

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.

Deploy with Group Policy

Install the client on multiple computers in the same domain.

Use the Command Line

Specify installation arguments in a command line window.

Procedure

Step 1 Open a command line window.

Step 2 Enter the following command:

```
msiexec.exe /i CiscoJabberSetup.msi
```

Step 3 Specify command line arguments as parameter=value pairs.

```
msiexec.exe /i CiscoJabberSetup.msi argument=value
```

Step 4 Run the command to install Cisco Jabber for Windows.

Example Installation Commands

Review examples of commands to install Cisco Jabber for Windows.

Cisco Unified Communications Manager, Release 9.x

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1
```

Where:

CLEAR=1 — Deletes any existing bootstrap file.
`/quiet` — Specifies a silent installation.

Cisco Unified Communications Manager, Release 8.x in Default Mode

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=CUP CUP_ADDRESS=1.2.3.4
```

Where:

CLEAR=1 — Deletes any existing bootstrap file.
AUTHENTICATOR=CUP — Sets Cisco Unified Presence as the authenticator.
CUP_ADDRESS=1.2.3.4 — Sets 1.2.3.4 as the IP address of the presence server.
`/quiet` — Specifies a silent installation.

Cisco Unified Communications Manager, Release 8.x in Phone Mode

If you are integrating with UDS when you are installing in phone mode, you must first define the <PresenceDomain>*Domain address of your Presence server*</PresenceDomain> parameter.

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 PRODUCT_MODE=Phone_Mode AUTHENTICATOR=CUCM
 TFTP=1.2.3.4 CTI=5.6.7.8
```

Where:

CLEAR=1 — Deletes any existing bootstrap file.
PRODUCT_MODE=Phone_Mode — Sets the client to phone mode.
AUTHENTICATOR=CUCM — Sets Cisco Unified Communications Manager as the authenticator.
TFTP=1.2.3.4 — Sets 1.2.3.4 as the IP address of the TFTP server that hosts the client configuration.
CTI=5.6.7.8 — Sets 5.6.7.8 as the IP address of the CTI server.
`/quiet` — Specifies a silent installation.

Cisco WebEx Messenger Service

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=WEBEX
```

Where:

CLEAR=1 — Deletes any existing bootstrap file.
AUTHENTICATOR=WEBEX — Sets the Cisco WebEx Messenger service as the authenticator.
`/quiet` — Specifies a silent installation.

Cisco WebEx Messenger Service with SSO

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=WEBEX
 SSO_ORG_DOMAIN=example.com
```

Where:

CLEAR=1 — Deletes any existing bootstrap file.
AUTHENTICATOR=WEBEX — Sets the Cisco WebEx Messenger service as the authenticator.
SSO_ORG_DOMAIN=example.com — Sets `example.com` as the single sign-on (SSO) domain.
`/quiet` — Specifies a silent installation.

Run the MSI Manually

You can run the installation program manually to install a single instance of the client and specify connection settings in the Advanced settings window.

Procedure

Step 1 Launch `CiscoJabberSetup.msi`.

The installation program opens a window to guide you through the installation process.

Step 2 Follow the steps to complete the installation process.

Step 3 Start Cisco Jabber for Windows.

Step 4 Select **Manual setup and sign in**.

The Advanced settings window opens.

Step 5 Specify values for the connection settings properties.

Step 6 Select **Save**.

Create a Custom Installer

You can transform the default installation package to create a custom installer.

Note You use Microsoft Orca to create custom installers. Microsoft Orca is available as part of the Microsoft Windows SDK for Windows 7 and .NET Framework 4.

Download and install Microsoft Windows SDK for Windows 7 and .NET Framework 4 from the Microsoft website.

Procedure

	Command or Action	Purpose
Step 1	Get the Default Transform File, on page 389	You must have the default transform file to modify the installation package with Microsoft Orca.
Step 2	Create Custom Transform Files, on page 389	Transform files contain installation properties that you apply to the installer.
Step 3	Transform the Installer, on page 390	Apply a transform file to customize the installer.

Related Topics

Microsoft Windows SDK for Windows 7 and .NET Framework 4

Get the Default Transform File

You must have the default transform file to modify the installation package with Microsoft Orca.

Procedure

Step 1 Download the Cisco Jabber administration package from Software Download page.

Step 2 Copy `CiscoJabberProperties.msi` from the Cisco Jabber administration package to your file system.

What to do next

Create Custom Transform Files, on page 389

Related Topics

Software Downloads

Create Custom Transform Files

To create a custom installer, you use a transform file. Transform files contain installation properties that you apply to the installer.

The default transform file lets you specify values for properties when you transform the installer. You should use the default transform file if you are creating one custom installer.

You can optionally create custom transform files. You specify values for properties in a custom transform file and then apply it to the installer.

Create custom transform files if you require more than one custom installer with different property values. For example, create one transform file that sets the default language to French and another transform file that sets the default language to Spanish. You can then apply each transform file to the installation package separately. The result is that you create two installers, one for each language.

Before you begin

Get the Default Transform File, on page 389

Procedure

Step 1 Start Microsoft Orca.

Step 2 Open `CiscoJabberSetup.msi` and then apply `CiscoJabberProperties.msi`.

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 `CiscoJabberSetup.msi`.

What to do next

Transform the Installer, on page 390

Transform the Installer

Apply a transform file to customize the installer.

Note Applying transform files will alter the digital signature of `CiscoJabberSetup.msi`. Attempts to modify or rename `CiscoJabberSetup.msi` will remove the signature entirely.

Before you begin

Create Custom Transform Files, on page 389

Procedure

Step 1 Start Microsoft Orca.

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

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

The installation package 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).

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.

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 a transform file.

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

Step 5 Select **Property** from the list of tables in the **Tables** pane.

The list of properties for `CiscoJabberSetup.msi` opens in the right panel of the application window.

Step 6 Specify values for the properties you require.

Step 7 Remove any properties that you do not require.

It is essential to remove any properties that are not being set, otherwise the properties being set will not take effect. Remove each property that is not needed one at a time.

a) Right-click the property you want to remove.
b) Select **Drop Row**.
c) Select **OK** when Microsoft Orca prompts you to continue.

Step 8 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 9 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**.

Related Topics

Installer Properties, on page 405

Deploy with Group Policy

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

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

Procedure

	Command or Action	Purpose
Step 1	Set a Language Code, on page 392	You must use this procedure and set the Language field to 1033 only if the MSI is to be modified by Orca in any way.
Step 2	Deploy the Client with Group Policy, on page 392	Deploy Cisco Jabber for Windows with Group Policy.

Set a Language Code

Altering the installation language is not necessary in Group Policy deployment scenarios where the exact MSI file provided by Cisco will be used. The installation language will be determined from the Windows User Locale (Format) in these situations. You must use this procedure and set the Language field to 1033 only if the MSI is to be modified by Orca in any way.

Procedure

Step 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.

Step 2 Open `CiscoJabberSetup.msi`.

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

Step 3 Select **View** > **Summary Information**.

Step 4 Locate the **Languages** field.

Step 5 Set the **Languages** field to 1033.

Step 6 Select **OK**.

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

Deploy the Client with Group Policy, on page 392

Related Topics

Supported Languages, on page 405

Deploy the Client with Group Policy

Complete the steps in this task to deploy Cisco Jabber for Windows with Group Policy.

Before you begin

Set a Language Code, on page 392

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 Jabber for Windows 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 Jabber for Windows.

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 Jabber for Windows.

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 Jabber for Windows on each computer the next time each computer starts.

Command Line Arguments

Review the command line arguments you can specify when you install Cisco Jabber for Windows.

Override Argument

The following table describes the parameter you must specify to override any existing bootstrap files from previous installations:

Argument	Value	Description
CLEAR	1	Specifies if the client overrides any existing bootstrap file from previous installations. The client saves the arguments and values you set during installation to a bootstrap file. The client then loads settings from the bootstrap file at startup.

If you specify CLEAR, the following occurs during installation:

1. The client deletes any existing bootstrap file.
2. The client creates a new bootstrap file.

If you do not specify CLEAR, the client checks for existing bootstrap files during installation.

- If no bootstrap file exists, the client creates a bootstrap file during installation.
- If a bootstrap file exists, the client does not override that bootstrap file and preserves the existing settings.

Note If you are reinstalling Cisco Jabber for Windows, you should consider the following:

- The client does not preserve settings from existing bootstrap files. If you specify CLEAR, you must also specify all other installation arguments as appropriate.
- The client 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 CiscoJabberSetup.msi CLEAR=1
```

Mode Type Argument

The following table describes the command line argument with which you specify the product mode:

Argument	Value	Description
PRODUCT_MODE	Phone_Mode	Specifies the product mode for the client. You can set the following value: • Phone_Mode — Cisco Unified Communications Manager is the authenticator. Choose this value to provision users with audio devices as base functionality.

When to Set the Product Mode

In phone mode deployments Cisco Unified Communications Manager is the authenticator. When the client gets the authenticator, it determines the product mode is phone mode. However, because the client always starts in the default product mode on the initial launch, users must restart the client to enter phone mode after sign in.

- Cisco Unified Communications Manager, Release 9.x and Later — You should not set PRODUCT_MODE during installation. The client gets the authenticator from the service profile. After the user signs in, the client requires a restart to enter phone mode.
- Cisco Unified Communications Manager, Release 8.x — You can specify phone mode during installation if you set Cisco Unified Communications Manager as the authenticator. The client reads the bootstrap file on the initial launch and determines it should start in phone mode. The client then gets Cisco Unified Communications Manager as the authenticator from the bootstrap file or manual settings. After the user signs in, the client does not require a restart.

Change Product Modes

To change the product mode, you must change the authenticator for the client. The client can then determine the product mode from the authenticator.

The method for changing from one product mode to another after installation, depends on your deployment.

Note In all deployments, the user can manually set the authenticator in the Advanced settings window.

In this case, you must instruct the user to change the authenticator in the Advanced settings window to change the product mode. You cannot override the manual settings, even if you uninstall and then reinstall the client.

Change Product Modes with Cisco Unified Communications Manager Version 9.x and Later

To change product modes with Cisco Unified Communications Manager version 9.x and later, you change the authenticator in the service profile.

Procedure

Step 1 Change the authenticator in the service profiles for the appropriate users.

Change Default Mode > Phone Mode

Do not provision users with an IM and Presence service.

If the service profile does not contain an IM and presence service configuration, the authenticator is Cisco Unified Communications Manager.

Change Phone Mode > Default Mode

Provision users with an IM and Presence service.

If you set the value of the **Product type** field in the IM and Presence profile to:

- **Unified CM (IM and Presence)** the authenticator is Cisco Unified Communications Manager IM and Presence Service.
- Webex **(IM and Presence)** the authenticator is the Cisco Webex Messenger service.

Step 2 Instruct users to sign out and then sign in again.

When users sign in to the client, it retrieves the changes in the service profile and signs the user in to the authenticator. The client then determines the product mode and prompts the user to restart the client.

After the user restarts the client, the product mode change is complete.

Change Product Modes with Cisco Unified Communications Manager Version 8.x

To change product modes with Cisco Unified Communications Manager version 8.x, you must reinstall Cisco Jabber for Windows to change the authenticator.

Change Default Mode > Phone Mode

Set the following arguments, at a minimum:

- CLEAR=1 to delete any existing bootstrap file.
- AUTHENTICATOR=CUCM to set the authenticator to Cisco Unified Communications Manager.
- PRODUCT_MODE=Phone_Mode to set phone mode as the product mode.

Change Phone Mode > Default Mode

Set the following arguments, at a minimum:

- CLEAR=1 to delete any existing bootstrap file.
- AUTHENTICATOR= one of the following:
  - CUP to set the authenticator to Cisco Unified Presence or Cisco Unified Communications Manager.
  - WEBEX to set the authenticator to the Cisco WebEx Messenger service.

Authentication Arguments

The following table describe the command line arguments you can set to specify the source of authentication:

Argument	Value	Description
AUTHENTICATOR	CUP CUCM Webex	Specifies the source of authentication for the client. This value is used if Service Discovery fails. Set one of the following as the value: • CUP—Cisco Unified Communications Manager IM and Presence Service. On-premises deployments in the default product mode. The default product mode can be either full UC or IM only. • CUCM—Cisco Unified Communications Manager. On-premises deployments in phone mode. • Webex—Cisco Webex Messenger Service. Cloud-based or hybrid cloud-based deployments. In on-premises deployments with Cisco Unified Communications Manager version 9.x and later, you should deploy the `_cisco-uds` SRV record. The client can then automatically determine the authenticator.
CUP_ADDRESS	IP address Hostname FQDN	Specifies the address of Cisco Unified Communications Manager IM and Presence Service. Set one of the following as the value: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*hostname.domain.com*)
TFTP	IP address Hostname FQDN	Specifies the address of your TFTP server. Set one of the following as the value: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*hostname.domain.com*) You should specify this argument if you set Cisco Unified Communications Manager as the authenticator. If you deploy: • In phone mode—you should specify the address of the TFTP server that hosts the client configuration. • In default mode—you can specify the address of the Cisco Unified Communications Manager TFTP service that hosts the device configuration.

Argument	Value	Description
CTI	IP address Hostname FQDN	Sets the address of your CTI server. Specify this argument if: • You set Cisco Unified Communications Manager as the authenticator. • Users have desk phone devices and require a CTI server.
CCMCIP	IP address Hostname FQDN	Sets the address of your CCMCIP server. Specify this argument if: • You set Cisco Unified Communications Manager as the authenticator. • The address of your CCMCIP server is not the same as the TFTP server address. The client can locate the CCMCIP server with the TFTP server address if both addresses are the same. Cisco Unified Communications Manager release 9.x and earlier—If you enable Cisco Extension Mobility, the `Cisco Extension Mobility` service must be activated on the Cisco Unified Communications Manager nodes that are used for CCMCIP. For information about Cisco Extension Mobility, see the *Feature and Services* guide for your Cisco Unified Communications Manager release.
SERVICES_DOMAIN	Domain	Sets the value of the domain where the DNS SRV records for Service Discovery reside. This argument can be set to a domain where no DNS SRV records reside if you want the client to use installer settings or manual configuration for this information. If this argument is not specified and Service Discovery fails, the user will be prompted for services domain information.

Argument	Value	Description
VOICE_SERVICES_DOMAIN	Domain	In Hybrid Deployments the domain required to discover Webex via CAS lookup may be a different domain than where the DNS records are deployed. If this is the case then set the SERVICES_DOMAIN to be the domain used for Webex discovery (or let the user enter an email address) and set the VOICE_SERVICES_DOMAIN to be the domain where DNS records are deployed. If this setting is specified, the client will use the value of VOICE_SERVICES_DOMAIN to lookup the following DNS records for the purposes of Service Discovery and Edge Detection: • `_cisco-uds` • `_cuplogin` • `_collab-edge` This setting is optional and if not specified, the DNS records are queried on the Services Domain which is obtained from the SERVICES_DOMAIN, email address input by the user, or cached user configuration.
EXCLUDED_SERVICES	One or more of: • CUP • Webex • CUCM	Lists the services that you want Jabber to exclude from Service Discovery. For example, you may have done a trial with Webex which means that your company domain is registered on Webex, but you do not want Jabber users to authenticate using Webex. You want Jabber to authenticate with an on-premises CUP CUCM server. In this case set: • EXCLUDED_SERVICES=WEBEX Possible values are CUP, CUCM, Webex To exclude more than one service, use comma separated values. For example, to exclude CUP and CUCM, specify: **`EXCLUDED_SERVICEs=CUP,CUCM`**. To exclude all services, specify: **`EXCLUDED_SERVICES=CUP,CUCM,WEBEX`** If you exclude all services, you need to use manual configuration or bootstrap configuration to configure the Jabber client.

Argument	Value	Description
UPN_DISCOVERY_ENABLED	true false	Allows you to define whether the client uses the User Principal Name (UPN) of a Windows session to get the User ID and domain for a user when discovering services. • true (default)—The UPN is used to find the User ID and the domain of the user, which is used during service discovery. Only the user discovered from UPN can log in to the client. • false—The UPN is not used to find the User ID and domain of the user. The user is prompted to enter credentials to find the domain for service discovery. Example installation command: `msiexec.exe /i CiscoJabberSetup.msi /quiet UPN_DISCOVERY_ENABLED=false`

TFTP Server Address

Cisco Jabber for Windows retrieves two different configuration files from the TFTP server:

- Client configuration files that you create.
- Device configuration files that reside on the Cisco Unified Communications Manager TFTP service when you provision users with devices.

To minimize effort, you should host your client configuration files on the Cisco Unified Communications Manager TFTP service. You then have only one TFTP server address for all configuration files and can specify that address as required.

You can, however, host your client configuration on a different TFTP server to the one that contains the device configuration. In this case, you have two different TFTP server addresses, one address for the TFTP server that hosts device configuration and another address for the TFTP server that hosts client configuration files.

Default Deployments

This section describes how you should handle two different TFTP server addresses in deployments that have a presence server.

You should do the following:

1. Specify the address of the TFTP server that hosts the client configuration on the presence server.
2. During installation, specify the address of the Cisco Unified Communications Manager TFTP service with the TFTP argument.

When the client starts for the first time, it:

1. Retrieves the address of the Cisco Unified Communications Manager TFTP service from the bootstrap file.
2. Gets device configuration from the Cisco Unified Communications Manager TFTP service.

3. Connects to the presence server.
4. Retrieves the address of the TFTP service that hosts the client configuration from the presence server.
5. Gets client configuration from the TFTP server.

Phone Mode Deployments

This section describes how you should handle two different TFTP server addresses in phone mode deployments.

You should do the following:

1. During installation, specify the address of the TFTP server that hosts the client configuration with the TFTP argument.
2. Specify the address of the TFTP server that hosts the device configuration in your client configuration file with the following parameter: TftpServer1.
3. Host the client configuration file on the TFTP server.

When the client starts for the first time, it:

1. Retrieves the address of the TFTP server from the bootstrap file.
2. Gets client configuration from the TFTP server.
3. Retrieves the address of the Cisco Unified Communications Manager TFTP service from the client configuration.
4. Gets device configuration from the Cisco Unified Communications Manager TFTP service.

Common Installation Arguments

The following table describes command line arguments that are common to all deployments:

Argument	Value	Description
LANGUAGE	LCID in decimal	Defines the Locale ID (LCID), in decimal, of the language that Cisco Jabber for Windows 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 Jabber for Windows uses the regional language for the current user as the default. From Release 11.1(1) onwards, if you do not specify a value, Cisco Jabber for Windows checks the value for the UseSystemLanguage parameter. If the UseSystemLanguage parameter is set to true, the same language is used as for the operating system. If the UseSystemLanguage parameter is to set to false or not defined, then the client uses the regional language for the current user 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**.
FORGOT_PASSWORD_URL	URL	Specifies the URL where users can reset lost or forgotten passwords. This argument is optional but recommended. **Note** In cloud-based deployments, you can specify a forgot password URL using the Cisco WebEx Administration Tool. However, the client cannot retrieve that forgot password URL until users sign in.
AUTOMATIC_SIGN_IN	true false	Applies to Release 11.1(1) onwards. Specifies whether the **Sign me in when Cisco Jabber starts** check box is checked when the user installs the client. • true—The **Sign me in when Cisco Jabber starts** check box is checked when the user installs the client. • false (default)—The **Sign me in when Cisco Jabber starts** check box is not checked when the user installs the client.

Argument	Value	Description
TFTP_FILE_NAME	Filename	Specifies the unique name of a group configuration file. You can specify either an unqualified or fully qualified filename as the value. The filename you specify as the value for this argument takes priority over any other configuration file on your TFTP server. This argument is optional. **Remember** You can specify group configuration files in the **Cisco Support Field** on the CSF device configuration on Cisco Unified Communications Manager.
LOGIN_RESOURCE	WBX MUT	Controls user sign in to multiple client instances. By default, users can sign in to multiple instances of Cisco Jabber at the same time. Set one of the following values to change the default behavior: • WBX—Users can sign in to one instance of Cisco Jabber for Windows at a time. Cisco Jabber for Windows appends the `wbxconnect` suffix to the user's JID. Users cannot sign in to any other Cisco Jabber client that uses the `wbxconnect` suffix. • MUT—Users can sign in to one instance of Cisco Jabber for Windows at a time, but can sign in to other Cisco Jabber clients at the same time. Each instance of Cisco Jabber for Windows appends the user's JID with a unique suffix.
LOG_DIRECTORY	Absolute path on the local filesystem	Defines the directory where the client writes log files. Use quotation marks to escape space characters in the path, as in the following example: `"C:\my_directory\Log Directory"` The path you specify must not contain Windows invalid characters. The default value is `%USER_PROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\Logs`

Argument	Value	Description
CLICK2X	DISABLE	Disables click-to-x functionality with Cisco Jabber. If you specify this argument during installation, the client does not register as a handler for click-to-x functionality with the operating system. This argument prevents the client from writing to the Microsoft Windows registry during installation. You must re-install the client and omit this argument to enable click-to-x functionality with the client after installation.
Telemetry_Enabled	true false	Specifies whether analytics data is gathered. The default value is true. To improve your experience and product performance, Cisco Jabber may collect and send non-personally identifiable usage and performance data to Cisco. The aggregated data is used by Cisco to understand trends in how Jabber clients are being used and how they are performing. Full details on what analytics data Cisco Jabber does and does not collect can be found in the Cisco Jabber Supplement to Cisco's On-Line Privacy Policy at http://www.cisco.com/web/siteassets/legal/privacy_02Jun10.html.

SSO Arguments

This section describes the command line arguments you can use to deploy Cisco Jabber for Windows with single sign on (SSO) capabilities.

Cloud-Based SSO Arguments

The arguments in the following table apply to cloud-based deployments only:

Argument	Value	Description
SSO_ORG_DOMAIN	Domain name	Specifies the domain name for the Cisco WebEx Org that contains the URL for the SSO service. Cisco Jabber for Windows uses this argument to retrieve the URL of the SSO service from the Org. When Cisco Jabber for Windows gets the SSO service URL, it can request login tokens to authenticate with Cisco WebEx Messenger. **Note** You specify the URL for the SSO service as the value of the Customer SSO Service Login URL in the Cisco WebEx Administration Tool.

Installer Properties

The following are the properties you can modify in a custom installer:

- CLEAR
- PRODUCT_MODE
- AUTHENTICATOR
- CUP_ADDRESS
- TFTP
- CTI
- CCMCIP
- LANGUAGE
- TFTP_FILE_NAME
- FORGOT_PASSWORD_URL
- SSO_ORG_DOMAIN
- LOGIN_RESOURCE
- LOG_DIRECTORY
- CLICK2X
- SERVICES_DOMAIN

These properties correspond to the installation arguments and have the same values.

Supported Languages

Cisco Jabber for Windows uses the regional language for the current user 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**.

The following table lists the languages that Cisco Jabber for Windows supports.

Arabic Bulgarian Catalan Croatian Czech Danish German Greek English Spanish Finnish	French Hebrew Hungarian Italian Japanese Korean Norwegian Dutch Polish Portuguese - Brazil Portuguese - Portugal	Romanian Russian Serbian Slovak Slovenian Swedish Thai Turkish Chinese - China Chinese - Taiwan

Note Cisco Jabber for Windows does not support Locale IDs for all sub-languages. For example, if you specify French - Canada, Cisco Jabber for Windows uses French - France.

See the following documentation for more information about Locale IDs:

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

Related Topics

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

Cisco Media Services Interface

Cisco Jabber for Windows supports Cisco Media Services Interface version 4.1.2 for Microsoft Windows 7 and later.

Desk Phone Video Capabilities

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

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

Install Cisco Media Services Interface

Procedure

Step 1 Download the Cisco Media Services Interface installation program from the download site on cisco.com.

Step 2 Install Cisco Media Services Interface on each computer on which you install Cisco Jabber.

See the appropriate Cisco Medianet documentation for installing Cisco Media Services Interface.

Related Topics

Download software
Medianet Knowledge Base Portal

Uninstall Cisco Jabber for Windows

You can uninstall Cisco Jabber for Windows using either the command line or the Microsoft Windows control panel. This document describes how to uninstall Cisco Jabber for Windows using the command line.

Use the Installer

If the installer is available on the file system, use it to remove Cisco Jabber for Windows.

Procedure

Step 1 Open a command line window.

Step 2 Enter the following command:

```
msiexec.exe /x path_to_CiscoJabberSetup.msi
```

For example,

```
msiexec.exe /x C:\Windows\Installer\CiscoJabberSetup.msi /quiet
```

Where `/quiet` specifies a silent uninstall.

The command removes Cisco Jabber for Windows from the computer.

Use the Product Code

If the installer is not available on the file system, use the product code to remove Cisco Jabber for Windows.

Procedure

Step 1 Find the product code.

a) Open the Microsoft Windows registry editor.
b) Locate the following registry key: `HKEY_CLASSES_ROOT\Installer\Products`
c) Select **Edit** > **Find**.
d) Enter Cisco Jabber in the **Find what** text box in the **Find** window and select **Find Next**.
e) Find the value of the **ProductIcon** key.

The product code is the value of the **ProductIcon** key, for example, `C:\Windows\Installer\{product_code}\ARPPRODUCTICON.exe`.

Note The product code changes with each version of Cisco Jabber for Windows.

Step 2 Open a command line window.

Step 3 Enter the following command:

```
msiexec.exe /x product_code
```

For example,

```
msiexec.exe /x 45992224-D2DE-49BB-B085-6524845321C7 /quiet
```

Where `/quiet` specifies a silent uninstall.

The command removes Cisco Jabber for Windows from the computer.

Install Cisco Jabber for Mac

Distribute the Cisco Jabber for Mac client

Visit the Cisco Software Center to download the Cisco Jabber for Mac client.

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