CONTENTS

CHAPTER 1  
Cisco Jabber Overview 1  
Purpose of this Guide 1  
About Cisco Jabber 1  
Cisco Jabber Planning Checklist 2

CHAPTER 2  
Deployment Scenarios 3  
On-Premises Deployment 3  
On-Premises Deployment with Cisco Unified Communications Manager 3  
On-Premises Deployments with Cisco Unified Presence 4  
On-Premises Deployment in Phone Mode 5  
Cloud-Based Deployments 6  
Cloud-Based Deployment 6  
Hybrid Cloud-Based Deployment 7  
Deployment with Single Sign-On 8  
Single Sign-On Requirements 9  
Single Sign-On and Remote Access 10  
Enable SAML SSO in the Client 10  
Deployment in a Virtual Environment 11  
Virtual Environment Requirements 11  
Virtual Environment and Roaming Profiles 12

CHAPTER 3  
Requirements 13  
On-Premises Servers for Cisco Jabber for Windows and Cisco Jabber for Mac 13  
On-Premises Servers for Cisco Jabber for Android 14  
On-Premises Servers for Cisco Jabber for iPhone and iPad 16  
Hardware Requirements For Desktop Clients 18  
Supported Operating Systems for Cisco Jabber for Windows 18  
Operating Systems for Cisco Jabber for Mac 19
CTI Supported Devices 19
Hardware Requirements for Cisco Jabber for Android 19
Hardware Requirements for Cisco Jabber for iPhone and iPad 21
Network Requirements 22
  Ports and Protocols for Cisco Jabber for Windows and Cisco Jabber for Mac 22
  Ports and Protocols for Cisco Jabber for Android, iPhone and iPad 24
Supported Codecs for Cisco Jabber for Windows and Cisco Jabber for Mac 26
Supported Codecs for Cisco Jabber for Android, iPhone and iPad 26

CHAPTER 4  Contact Source 29

  On-Premises Contact Source Options 29
    IM Address Scheme 29
  Directory Servers 30
  Contact Photo Formats and Dimensions 30
    Contact Photo Formats 30
    Contact Photo Dimensions 31
    Contact Photo Adjustments 31

CHAPTER 5  Certificates 33

  Certificate Validation 33
  Required Certificates for On-Premises Servers 34
    Certificate Signing Request Formats and Requirements 35
  Revocation Servers 35
  Server Identity in Certificates 35
  Certificate Requirements for Cloud-Based Servers 36

CHAPTER 6  Service Discovery 39

  About Service Discovery 39
  How the Client Locates Services 40
  Cisco UDS SRV Record 42
  CUP Login SRV Record 43
  Collaboration Edge SRV Record 45

CHAPTER 7  Security 47

  Federal Information Processing Standards (FIPS) 47
Compliance and Policy Control for File Transfer and Screen Capture  47

Instant Message Encryption  48
  On-Premises Encryption  48
  Cloud-Based Encryption  49
    Client to Client Encryption  50

Encryption Icons  51
  Lock Icon for Client to Server Encryption  51
  Padlock Icon for Client to Client Encryption  51

Local Chat History  52

CHAPTER 8

Planning Considerations  53

DNS Configuration  53
  How the Client Uses DNS  53
    How the Client Finds a Name Server  53
    How the Client Gets a Services Domain  54
  How the Client Discovers Available Services  55
    Client Issues HTTP Query  56
    Client Queries Name Server  56
    Client Connects to Internal Services  57
    Client Connects through Expressway for Mobile and Remote Access  59

Domain Name System Designs  60
  Separate Domain Design  60
    Deploy SRV Records in a Separate Domain Structure  60
    Use an Internal Zone for a Services Domain  61
  Same Domain Design  61
    Same Domain, Split-Brain  61
    Same Domain, Not Split-Brain  62
  How the Client Connects to Services  62
    Recommended Connection Methods  63
    Sources of Authentication  66
    High Availability for Instant Messaging and Presence  66
    Client Behavior During Failover  68
    Computer Telephony Integration Servitude  69
Cisco Jabber Overview

• Purpose of this Guide, page 1
• About Cisco Jabber, page 1
• Cisco Jabber Planning Checklist, page 2

Purpose of this Guide

The Cisco Jabber Planning Guide includes the following information to assist you in planning the deployment and installation of Cisco Jabber.

• A product overview describing the features available in the product this release
• Planning considerations for service discovery, encryption, and contact sources (EDI and BDI).
• Information about how you are going to deploy the client, whether it's an on-premises or cloud deployment.
• Requirements for hardware, software, network, and certificates.

To deploy and install Cisco Jabber, use the Deployment and Installation Guide.

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 http://www.cisco.com/go/jabber.
## Cisco Jabber Planning Checklist

Use this checklist to plan your Cisco Jabber Deployment.

<table>
<thead>
<tr>
<th>Task</th>
<th>See</th>
<th>Completed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine how you plan to deploy Cisco Jabber.</td>
<td>Deployment Scenarios, on page 3</td>
<td></td>
</tr>
<tr>
<td>Confirm that your servers, hardware, and network comply with the requirements.</td>
<td>Requirements, on page 13</td>
<td></td>
</tr>
<tr>
<td>Determine how you plan to configure your contact source.</td>
<td>Contact Source, on page 29</td>
<td></td>
</tr>
<tr>
<td>Confirm that you have the required certificates based on the deployment option you select.</td>
<td>Certificates, on page 33</td>
<td></td>
</tr>
<tr>
<td>Review Service Discovery to determine if you plan to configure service discovery and to determine which service discovery records you require.</td>
<td>Service Discovery, on page 39</td>
<td></td>
</tr>
<tr>
<td>Review the security information</td>
<td>Security, on page 47</td>
<td></td>
</tr>
<tr>
<td>Review remaining planning considerations.</td>
<td>Planning Considerations, on page 53</td>
<td></td>
</tr>
</tbody>
</table>
Deployment Scenarios

- On-Premises Deployment, page 3
- Cloud-Based Deployments, page 6
- Deployment with Single Sign-On, page 8
- Deployment in a Virtual Environment, page 11

On-Premises Deployment

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

You can deploy Cisco Jabber 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.

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

On-Premises Deployment with Cisco Unified Communications Manager

The following services are available in an on-premises deployment with Cisco Unified Communications Manager IM and Presence Service:

- **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.
• **File Transfers** — Send and receive files and screenshots through Cisco Unified Communications Manager IM and Presence Service.

• **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 Meeting Server — Provides on-premises meeting capabilities.

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

---

**On-Premises Deployments with Cisco Unified Presence**

The following services are available in an on-premises deployment with Cisco Unified Presence:

• **Presence** — Publish availability and subscribe to other users' availability through Cisco Unified Presence.

• **IM** — 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 Meeting Server** — Provides on-premises meeting capabilities.

**Note**

Cisco Jabber for mobile clients do not support conferencing during Phone mode.

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

---

**On-Premises Deployment in Phone Mode**

The following services are available in a phone mode deployment:

- **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 Meeting Server** — Provides on-premises meeting capabilities.
Note
Cisco Jabber for Android does not support conferencing in phone mode.

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

---

**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 Deployment**

The following services are 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.

The following diagram illustrates the architecture of a cloud-based deployment:
The following services are 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 publish their availability and subscribe to other users' availability.
- **Instant Messaging** — The Cisco WebEx Messenger service lets users send and receive instant messages.
- **Audio** — Place audio calls through desk phone devices or computers through Cisco Unified Communications Manager.
- **Video** — Place video calls through Cisco Unified Communications Manager.
- **Conferencing** — Cisco WebEx Meeting Center provides hosted meeting capabilities.
- **Voicemail** — Send and receive voice messages through Cisco Unity Connection.

The following diagram illustrates the architecture of a hybrid cloud-based deployment:
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 users start their Cisco Jabber client:

1. The user starts the Jabber client. If you configure your Identity Provider (known as an IdP) to prompt users to sign in using a Web form, the form is displayed within the client.

2. The Cisco Jabber client sends an authorization request to the service it is connecting to, such as Cisco WebEx Messenger Services, Cisco Unified Communications Manager, or Cisco Unity Connection.

3. The service redirects the client to request authentication from the IdP.

4. The IdP requests credentials. Credentials can be supplied in one of the following methods:
   - Form-based authentication that presents a page to the user containing username and password fields.
   - Kerberos for Integrated Windows authentication (IWA) (Windows only)
   - Smart card authentication (Windows only)

5. The IdP provides a cookie to the browser or other authentication method. The IdP authenticates the identity using SAML, which allows the service to provide the client with a token.

6. The client uses the token for authentication to login to the service.

**Authentication Methods**

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

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

Single Sign-On Requirements

Supported Identity Providers

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

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

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

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

Cookies

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

Required Browsers

To share the authentication cookie (issued by IdP) between the browser and the client, you must specify one of the following browsers as your default browser:

<table>
<thead>
<tr>
<th>Product</th>
<th>Required Browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Jabber for Windows</td>
<td>Internet Explorer</td>
</tr>
<tr>
<td>Cisco Jabber for Mac</td>
<td>Safari</td>
</tr>
<tr>
<td>Cisco Jabber for iPhone and iPad</td>
<td>Safari</td>
</tr>
<tr>
<td>Cisco Jabber for Android</td>
<td>Chrome</td>
</tr>
</tbody>
</table>
An embedded browser can not share a cookie with an external browser when using in SSO with Android.

Single Sign-On and Remote Access

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

- Single sign-on (SSO) is available with Cisco Expressway 8.5 and Cisco Unified Communications Manager 10.5.2 or later.
- You cannot use SSO over the Expressway for Mobile and Remote Access on a secure phone.
- The Identity Provider used must have the same internal and external URL. If the URL is different, the user may be prompted to sign in again when changing from inside to outside the corporate firewall and vice versa.

Enable SAML SSO in the Client

Before You Begin

- If you do not use 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 WebEx Messenger, enable SSO on 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 How the Client Locates Services.

Step 3 Define how long a session lasts.
A session is comprised of cookie and token values. A cookie usually lasts longer than a token. The life of the cookie is defined in the Identity Provider, and the duration of the token is defined in the service.

**Step 4** When SSO is enabled, by default all 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 Jabber username and password. To disable SSO for a Jabber user, set the value of the SSO Enabled parameter to FALSE.

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

---

**Deployment in a Virtual Environment**

You can deploy Cisco Jabber for Windows in a virtual environment. The following features are supported in a virtual environment:

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

**Virtual Environment Requirements**

**Software Requirements**

To deploy Cisco Jabber for Windows in a virtual environment, select from the following supported software versions:

<table>
<thead>
<tr>
<th>Software</th>
<th>Supported Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix XenDesktop</td>
<td>7.5, 7.1, 7.0, and 5.6</td>
</tr>
<tr>
<td></td>
<td>6.5 Feature Pack 2 Enterprise Edition for Windows Server 2008 Service Pack 2 64 bit, published desktop</td>
</tr>
<tr>
<td></td>
<td>6.5 Feature Pack 1 Enterprise Edition for Windows Server 2008 R2 Standard Service Pack 1 64 bit, published desktop</td>
</tr>
<tr>
<td></td>
<td>6.5 Enterprise Edition for Windows Server 2008 R2 Standard Service Pack 1 64 bit, published desktop</td>
</tr>
<tr>
<td>VMware Horizon View</td>
<td>6.0, 5.3, and 5.2</td>
</tr>
</tbody>
</table>

---
Softphone Requirements

For softphone calls, use Cisco Virtualization Experience Media Engine (VXME).

Virtual Environment and Roaming Profiles

In a virtual environment, users do not always access the same virtual desktop. To guarantee a consistent user experience, these files must be accessible every time the client is launched. Cisco Jabber stores user data in the following locations:

- **C:\Users\username\AppData\Local\Cisco\Unified Communications\Jabber\CSF**
  - **Contacts** — Contact cache files
  - **History** — Call and chat history
  - **Photo cache** — Caches the directory photos locally

- **C:\Users\username\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF**
  - **Config** — Maintains user configuration files and stores configuration store cache
  - **Credentials** — Stores encrypted username and password file

If required, you can exclude files and folders from synchronization by adding them to an exclusion list. To synchronize a subfolder that is in an excluded folder, add the subfolder to an inclusion list.

To preserve personal user settings

- Do not exclude the following directories:
  - **AppData\Local\Cisco**
  - **AppData\Local\JabberWerxCPP**
  - **AppData\Roaming\Cisco**
  - **AppData\Roaming\JabberWerxCPP**

- Use the following dedicated profile management solutions:
  - **Citrix Profile Management** — This 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** — This 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.
Requirements

- On-Premises Servers for Cisco Jabber for Windows and Cisco Jabber for Mac, page 13
- On-Premises Servers for Cisco Jabber for Android, page 14
- On-Premises Servers for Cisco Jabber for iPhone and iPad, page 16
- Hardware Requirements For Desktop Clients, page 18
- Hardware Requirements for Cisco Jabber for Android, page 19
- Hardware Requirements for Cisco Jabber for iPhone and iPad, page 21
- Network Requirements, page 22

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

Cisco Jabber supports the following on-premises servers:

- Cisco Unified Communications Manager version 8.6(2) or later
- Cisco Unified Presence version 8.6(2) or later
- Cisco Unity Connection version 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 Communication 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

**Restriction**
Cisco Jabber requires an active connection to the presence server to successfully fall back to Cisco Unified Survivable Remote Site Telephony.


### On-Premises Servers for Cisco Jabber for Android

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

**Cisco Unified Communications Manager**

- Cisco Unified Communications Manager Release 8.6(1)
- Cisco Unified Communications Manager Release 8.6(2)
- Cisco Unified Communications Manager Release 9.1(1)
- 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 Presence**

- Cisco Unified Presence Release 8.6(1)
- 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)

**Video Conferencing Bridge**

- Cisco TelePresence MCU 5310
- Cisco TelePresence Server 7010
- Cisco TelePresence Server MSE 8710
- Cisco Integrated Services Router (with 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 8.5
- 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 2.0
- Cisco WebEx Meetings Server Version 2.5
- Cisco WebEx Meetings client Version 4.5 to 6.5

**Cisco Expressway Series for Cisco Unified Communications Manager (Optional)**

Use the following servers to set up mobile and remote access for the client. Note that 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 8.2
Cisco Expressway 8.2.1


Cisco Adaptive Security Appliance (Optional)

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 using AnyConnect with Samsung the supported version is 4.0.01128.

- Cisco ASA (Adaptive Security Appliance) 5500 Series, 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

On-Premises Servers for Cisco Jabber for iPhone and iPad

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

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

  Important The DVO-R feature is only available on iPhone. It requires Cisco Jabber for iPhone and iPad client, Release 9.6 and later.

Cisco Unified Presence

  - Cisco Unified Presence Release 8.6
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
- Cisco Unified Communications Manager IM and Presence Service Release 10.0

Cisco Unity Connection
- Cisco Unity Connection Release 8.5 or later

Cisco WebEx Meetings Server
Cisco WebEx Meetings Server version 1.5 or later

Cisco Adaptive Security Appliance (Optional)

VPN On Demand (Optional)
The Apple iOS On-Demand VPN feature requires certificate-only authentication. If you set up the ASA (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

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


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.

Hardware Requirements For Desktop Clients

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Cisco Jabber for Windows</th>
<th>Cisco Jabber for Mac</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed RAM</td>
<td>2 GB RAM on Microsoft Windows 7 and Windows 8</td>
<td>2 GB RAM</td>
</tr>
<tr>
<td>Free Physical Memory</td>
<td>128 MB</td>
<td>1 GB</td>
</tr>
<tr>
<td>Free Disk Space</td>
<td>256 MB</td>
<td>300 MB</td>
</tr>
<tr>
<td>CPU Speed and Type</td>
<td>Mobile AMD Sempron Processor 3600+ 2 GHz</td>
<td>Intel Core 2 Duo or later processors in any of the following Apple hardware:</td>
</tr>
<tr>
<td></td>
<td>Intel Core2 CPU T7400 @ 2.16 GHz</td>
<td>• Mac Pro</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MacBook Pro (including Retina Display model)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MacBook</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MacBook Air</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• iMac</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Mac Mini</td>
</tr>
<tr>
<td>GPU</td>
<td>DirectX11 on Microsoft Windows 7</td>
<td>N/A</td>
</tr>
<tr>
<td>I/O Ports</td>
<td>USB 2.0 for USB camera and audio devices.</td>
<td>USB 2.0 for USB camera and audio devices</td>
</tr>
</tbody>
</table>

Supported 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 and 64 bit—supported in desktop mode only

• Microsoft Windows 8 32 bit and 64 bit—supported in desktop mode only

• Microsoft Windows 7 32 bit and 64 bit

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

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

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

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

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.

Hardware Requirements for Cisco Jabber for Android

The following devices are supported for Cisco Jabber for Android:

<table>
<thead>
<tr>
<th>Device</th>
<th>Device Model</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco DX</td>
<td>70</td>
<td>10.2.x version</td>
</tr>
<tr>
<td></td>
<td>80</td>
<td>10.2.x version</td>
</tr>
<tr>
<td></td>
<td>650</td>
<td>10.2.x version</td>
</tr>
<tr>
<td>HTC</td>
<td>One M7</td>
<td>Android OS 4.4.x</td>
</tr>
<tr>
<td></td>
<td>One M8</td>
<td>Android OS 4.4.x</td>
</tr>
<tr>
<td></td>
<td>One Max</td>
<td>Android OS 4.4.x</td>
</tr>
<tr>
<td>Google Nexus</td>
<td>5</td>
<td>Android OS 4.4.x and Android OS 5.0</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>Android OS 4.4.x and Android OS 5.0</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>Android OS 4.4.x and Android OS 5.1</td>
</tr>
<tr>
<td>LG</td>
<td>G2</td>
<td>Android OS 4.2.2 to Android OS 4.4.x</td>
</tr>
<tr>
<td></td>
<td>G3</td>
<td>Android OS 4.4.x</td>
</tr>
<tr>
<td>Motorola</td>
<td>Moto G</td>
<td>Android OS 4.4.x</td>
</tr>
<tr>
<td>Device</td>
<td>Device Model</td>
<td>Operating System</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Samsung Galaxy</td>
<td>Note II</td>
<td>Android OS 4.2 to Android OS 4.4.x</td>
</tr>
<tr>
<td></td>
<td>Note III</td>
<td>Android OS 4.3 to Android OS 4.4.x</td>
</tr>
<tr>
<td></td>
<td>Note IV</td>
<td>Android OS 4.4.x</td>
</tr>
<tr>
<td></td>
<td>Note Pro 12.2</td>
<td>Android OS 4.4.x</td>
</tr>
<tr>
<td></td>
<td>Rugby Pro</td>
<td>Android OS 4.2.2 to Android OS 4.4 x</td>
</tr>
<tr>
<td></td>
<td>SII</td>
<td>Android OS 4.1.2 to Android OS 4.4 x</td>
</tr>
<tr>
<td></td>
<td>SIII</td>
<td>Android OS 4.2 to Android OS 4.4 x</td>
</tr>
<tr>
<td></td>
<td>S4</td>
<td>Android OS 4.2.2 to Android OS 4.4 x</td>
</tr>
<tr>
<td></td>
<td>S4 mini</td>
<td>Android OS 4.2.2 to Android OS 4.4 x</td>
</tr>
<tr>
<td></td>
<td>S5</td>
<td>Android OS 4.4.x</td>
</tr>
<tr>
<td></td>
<td>S5 mini</td>
<td>Android OS 4.4.x</td>
</tr>
<tr>
<td></td>
<td>Tab 3 8-inch</td>
<td>Android OS 4.4.x</td>
</tr>
<tr>
<td></td>
<td>Tab 4 7-inch, 8-inch, and 10.1-inch</td>
<td>Android OS 4.4.x</td>
</tr>
<tr>
<td></td>
<td>Tab PRO 8.4-inch and 10.1-inch</td>
<td>Android OS 4.4.x</td>
</tr>
<tr>
<td></td>
<td>Tab S 8.4-inch &amp; 10.5-inch</td>
<td>Android OS 4.4.x</td>
</tr>
<tr>
<td>Sony Xperia</td>
<td>M2</td>
<td>Android OS 4.3</td>
</tr>
<tr>
<td></td>
<td>Z1</td>
<td>Android OS 4.2 to Android OS 4.4 x</td>
</tr>
<tr>
<td></td>
<td>Z2</td>
<td>Android OS 4.4.x</td>
</tr>
<tr>
<td></td>
<td>Z2 tablet</td>
<td>Android OS 4.4.x</td>
</tr>
<tr>
<td></td>
<td>Z3</td>
<td>Android OS 4.4.x</td>
</tr>
<tr>
<td></td>
<td>ZR/A</td>
<td>Android OS 4.1.2 to Android OS 4.4 x</td>
</tr>
</tbody>
</table>

Each Android device must meet the following minimum CPU and display requirements:

- **Chipset** — Android devices that are based on an Intel chipset are not supported.
- **CPU** — 1.5 GHz dual-core or higher (quad-core recommended).
• Display — 320 x 480 or higher. For two-way video, the minimum display resolution requirement is 480 x 800 or higher.

**Supported Bluetooth Devices**

• Jabra Motion
• Jawbone ICON for Cisco Bluetooth Headset
  If you use a Samsung Galaxy S4, you can experience problems due to compatibility issues between these devices.
• Plantronics BackBeat 903+
  If you use a Samsung Galaxy S4, you can experience problems due to compatibility issues between these devices.
• Jabra Wave+
• Jabra Easygo

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

**Hardware Requirements for Cisco Jabber for iPhone and iPad**

The following Apple devices are supported for Cisco Jabber for iPhone and iPad on iOS 8 and later:

<table>
<thead>
<tr>
<th>Apple Device</th>
<th>Generation</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>iTouch</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>iPhone</td>
<td>4S, 5, 5C, 5S, 6 and 6 Plus</td>
<td></td>
</tr>
<tr>
<td>iPad</td>
<td>second, third and fourth</td>
<td></td>
</tr>
<tr>
<td>iPad Mini</td>
<td>mini 1, mini 2 and mini 3</td>
<td></td>
</tr>
<tr>
<td>iPad Air</td>
<td>Air1 and Air 2</td>
<td></td>
</tr>
</tbody>
</table>

Bluetooth headsets are supported on all of the above Apple devices:

• Jabra EASYGO
• Jabra EXTREME 2
• Jabra SPEAK 450 for Cisco
• Jabra SUPREME UC
• Jabra WAVE
Network Requirements

If you deploy Phone Services, the mobile device must be able to connect to the corporate network.

For optimal user experience when using Cisco Jabber over your corporate Wi-Fi network, Cisco recommends that you:

- 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 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. Cisco recommends that you:

- 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 "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.

Bluetooth use can cause voice quality and connectivity issues. If users connect to the network remotely, the mobile device must be able to connect to the corporate network using a solid, high-bandwidth connection. Video and audio quality is dependent on connection quality and cannot be guaranteed.

Ports and Protocols for Cisco Jabber for Windows and Cisco Jabber for Mac

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

- Sony Ericsson Bluetooth Headset BW600
<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP (XMPP and HTTPS)</td>
<td>XMPP traffic to the Cisco 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong>: Cisco Jabber can also use this port for HTTPS traffic to Cisco Unity Connection and Cisco WebEx Meetings Server.</td>
</tr>
<tr>
<td>389</td>
<td>UDP / TCP</td>
<td>LDAP directory server</td>
</tr>
<tr>
<td>636</td>
<td>LDAPS</td>
<td>LDAP directory server (secure)</td>
</tr>
<tr>
<td>3268</td>
<td>TCP</td>
<td>Global Catalog server</td>
</tr>
<tr>
<td>3269</td>
<td>LDAPS</td>
<td>Global Catalog server (secure)</td>
</tr>
<tr>
<td>5070</td>
<td>UDP</td>
<td>Binary Floor Control Protocol (BFCP) for video desktop sharing capabilities</td>
</tr>
<tr>
<td>5222</td>
<td>TCP (XMPP)</td>
<td>XMPP traffic to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.</td>
</tr>
<tr>
<td>8443</td>
<td>TCP (HTTPS)</td>
<td>Traffic to Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service.</td>
</tr>
<tr>
<td>7080</td>
<td>TCP (HTTPS)</td>
<td>Cisco Unity Connection for notifications of voice messages (new message, message update, and message deletion)</td>
</tr>
<tr>
<td>53</td>
<td>UDP / TCP</td>
<td>Domain Name System (DNS) traffic</td>
</tr>
<tr>
<td>37200</td>
<td>SOCKS5 Bytestreams</td>
<td>Peer to peer file transfers. In on-premises deployments, the client also uses this port to send screen captures.</td>
</tr>
<tr>
<td>5060</td>
<td>UDP/TCP</td>
<td>Session Initiation Protocol (SIP) call signalling</td>
</tr>
<tr>
<td>5061</td>
<td>TCP</td>
<td>Secure SIP call signalling</td>
</tr>
<tr>
<td>49152 to 65535</td>
<td>TCP</td>
<td>IM-Only Screen Share The client randomly selects a port from the range. The actual range may vary. To find the real range, run the following command:<strong>netsh interface ipv4 show dynamicportrange tcp</strong></td>
</tr>
</tbody>
</table>
Ports for Additional Services and Protocols

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

- Cisco Unified Communications Manager, Cisco Unified Communications Manager IM and Presence Service, and Cisco Unified Presence, refer to the TCP and UDP Port Usage Guide.
- Cisco Unity Connection, refer to the System Administration Guide.
- Cisco WebEx Meetings Server, refer to the Administration Guide.
- Cisco WebEx services, refer to 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**

There are no TCP/IP services enabled in the client.

<table>
<thead>
<tr>
<th>Port</th>
<th>Application Layer Protocol</th>
<th>Transport Layer Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inbound</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16384 to 32766</td>
<td>RTP</td>
<td>UDP</td>
<td>Receives Real-Time Transport Protocol (RTP) media streams for audio and video. You set these ports in Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td><strong>Outbound</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>69</td>
<td>TFTP</td>
<td>UDP</td>
<td>Connects to the Trivial File Transfer Protocol (TFTP) server.</td>
</tr>
<tr>
<td>6970</td>
<td>HTTP</td>
<td>TCP</td>
<td>Connects to the TFTP server to download client configuration files.</td>
</tr>
<tr>
<td>80</td>
<td>HTTP</td>
<td>TCP</td>
<td>Connects to services such as Cisco WebEx Meeting Center for meetings or Cisco Unity Connection for voicemail.</td>
</tr>
<tr>
<td>389</td>
<td>LDAP</td>
<td>TCP (UDP)</td>
<td>Connects to an LDAP directory service.</td>
</tr>
<tr>
<td>3268</td>
<td>LDAP</td>
<td>TCP</td>
<td>Connects to a Global Catalog server for contact searches.</td>
</tr>
<tr>
<td>Port</td>
<td>Application Layer Protocol</td>
<td>Transport Layer Protocol</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------</td>
<td>--------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>443</td>
<td>HTTPS</td>
<td>TCP</td>
<td>Connects to services such as Cisco WebEx Meeting Center for meetings or Cisco Unity Connection for voicemail.</td>
</tr>
<tr>
<td>636</td>
<td>LDAPS</td>
<td>TCP</td>
<td>Connects securely to an LDAP directory service.</td>
</tr>
<tr>
<td>3269</td>
<td>LDAPS</td>
<td>TCP</td>
<td>Connects securely to the Global Catalog server.</td>
</tr>
<tr>
<td>5060</td>
<td>SIP</td>
<td>TCP</td>
<td>Provides Session Initiation Protocol (SIP) call signaling.</td>
</tr>
<tr>
<td>5061</td>
<td>SIP over TLS</td>
<td>TCP</td>
<td>Provides secure SIP call signaling.</td>
</tr>
<tr>
<td>5222</td>
<td>XMPP</td>
<td>TCP</td>
<td>Connects to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service for instant messaging and presence.</td>
</tr>
<tr>
<td>5269</td>
<td>XMPP</td>
<td>TCP</td>
<td>XMPP federation.</td>
</tr>
<tr>
<td>8191</td>
<td>SOAP</td>
<td>TCP</td>
<td>Connects to the local port to provide Simple Object Access Protocol (SOAP) web services.</td>
</tr>
</tbody>
</table>
| 8443  | HTTPS                       | TCP                      | 8443 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 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)*.
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
• G.711 mu-law
• G.711 a-law
• G.722.1
• G.729a

Users can turn Low Bandwidth mode on and off in the client settings if they experience voice quality issues.
Low Bandwidth mode supports G.729a only.

Supported Video Codecs
H.264/AVC

Supported Voicemail Codecs
• PCM linear
• G.711 mu-law (default)
• G.711 a-law
• GSM 6.10
Note
Cisco Jabber does not support visual voicemail with G.729. However, users can access their voice messages using G.729 and the Call Voicemail feature.
Contact Source

- On-Premises Contact Source Options, page 29

On-Premises Contact Source Options

In on-premises deployments, the client requires one of the following contact sources to resolve directory lookups for user information:

- LDAP—If you have a corporate directory you can use the following LDAP-based contact source options to configure your directory as the contact source:
  - Enhanced Directory Integration (EDI)—Select this option to deploy Cisco Jabber for Windows.
  - Basic Directory Integration (BDI)—Select this option to deploy Cisco Jabber for Mac, iOS, and Android.
  - Cisco Unified Communications Manager User Data Service (UDS)—If you do not have a corporate directory, you can use this option.

IM Address Scheme

Cisco Jabber supports flexible IM Address Scheme using Cisco Unified Communications Manager IM and Presence 10.x or later. The IM Address scheme is the Jabber ID that identifies the Cisco Jabber users. The available IM address schemes in the Advanced Presence Settings are:

- UserID@[Default Domain]
- Directory URI

UserID@[Default Domain]

The User ID field is mapped to an LDAP field. This is the default IM Address Scheme. For example, user Anita Perez has an account name aperez and the User ID field is mapped to the sAMAccountName LDAP field. The address scheme used is aperez@example.com.
Directory URI

The Directory URI is mapped to the mail or msRTCSIP-primaryuseraddress LDAP fields. This option provides a scheme that is independent of the user ID for authentication.

For example, user Anita Perez has an account name aperez, the mail field is Anita.Perez@domain.com, the address scheme used is Anita.Perez@domain.com.

Directory Servers

You can use the following directory servers with Cisco Jabber:

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

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

Restriction

Directory integration with OpenLDAP, AD LDS, or ADAM requires you to define specific parameters in a Cisco Jabber configuration file. See LDAP Directory Servers for more information.

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.

The following table lists the different dimensions for contact photos in Cisco Jabber:

<table>
<thead>
<tr>
<th>Location</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio call window</td>
<td>128 pixels by 128 pixels</td>
</tr>
<tr>
<td>Invitations and reminders, for example:</td>
<td>64 pixels by 64 pixels</td>
</tr>
<tr>
<td>• Incoming call windows</td>
<td></td>
</tr>
<tr>
<td>• Meeting reminder windows</td>
<td></td>
</tr>
<tr>
<td>Lists of contacts, for example:</td>
<td>32 pixels by 32 pixels</td>
</tr>
<tr>
<td>• Contact lists</td>
<td></td>
</tr>
<tr>
<td>• Participant rosters</td>
<td></td>
</tr>
<tr>
<td>• Call history</td>
<td></td>
</tr>
<tr>
<td>• Voicemail messages</td>
<td></td>
</tr>
</tbody>
</table>

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 upwards 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 non-square 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.
Certificates

- Certificate Validation, page 33
- Required Certificates for On-Premises Servers, page 34
- Certificate Requirements for Cloud-Based Servers, page 36

Certificate Validation

The Certificate Validation Process
Cisco Jabber validates server certificates when authenticating to services. When attempting to establish secure connections, the services present Cisco Jabber with certificates. Cisco Jabber validates the presented certificate against what is in the client device's local certificate store. If the certificate is not in the certificate store, the certificate is deemed untrusted and Jabber prompts the user to accept or decline the certificate.

If the user accepts the certificate, Jabber connects to the service and saves the certificate in the certificate store or keychain of the device. If the user declines the certificate, Jabber does not connect to the service and the certificate is not saved to the certificate store or keychain of the device.

If the certificate is in the local certificate store of the device, then Jabber trusts the certificate. Jabber connects to the service without prompting the user to accept or decline the certificate.

Jabber authenticates to two services on the Cisco Unified Communications Manager server. The service names are Cisco Tomcat and XMPP. A certificate signing request (CSR) must be generated for each service. Some public certificate authorities do not accept more than one CSR per FQDN. As such, the CSR for each service may need to be sent to separate public certificate authorities.

Ensure that you specify FQDN in the service profile for each service, instead of IP Address or Host Name.

Signed Certificates
Certificates can be self-signed or signed by the certificate authority (CA). Self-signed certificates are signed by the services that are presenting the certificates, and users are always prompted to accept or decline the certificate. If you use CA-signed certificates, users are not prompted because you are installing the certificate on the devices yourself. CA-signed certificates can be signed by a Private CA or a Public CA. Many certificates that are signed by a Public CA are stored in the certificate store or keychain of the device.
Certificate Validation Options

Before setting up certificate validation, you must decide how you want the certificates to be validated:

- Whether you are deploying certificates for on-premises or cloud-based deployments.
- Whether you want to deploy self-signed certificates or CA-signed certificates.
- If you are deploying CA-signed certificates, whether you are going to use public CA or private CA.
- Which services you need to get certificates for.

Required Certificates for On-Premises Servers

On-premises servers present the following certificates to establish a secure connection with Cisco Jabber:

<table>
<thead>
<tr>
<th>Server</th>
<th>Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service</td>
<td>HTTP (Tomcat)</td>
</tr>
<tr>
<td></td>
<td>XMPP</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>HTTP (Tomcat) and CallManager certificate (secure SIP call signaling for secure phone)</td>
</tr>
<tr>
<td>Cisco Unity Connection</td>
<td>HTTP (Tomcat)</td>
</tr>
<tr>
<td>Cisco WebEx Meetings Server</td>
<td>HTTP (Tomcat)</td>
</tr>
<tr>
<td>Cisco VCS Expressway</td>
<td>Server certificate (used for HTTP, XMPP and SIP call signaling)</td>
</tr>
<tr>
<td>Cisco Expressway-E</td>
<td></td>
</tr>
</tbody>
</table>

Important Notes

- SAML SSO and the IdP require an X.509 certificate.
- You should apply the most recent Service Update (SU) for Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service before you begin the certificate signing process.
- The required certificates apply to all server versions.
- Each node in a cluster, subscribers and publishers, runs a Tomcat service and can present the client with a 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.
Certificate Signing Request Formats and Requirements

A public Certificate Authority (CA) typically requires Certificate Signing Request (CSR) to conform to specific formats. For example, a public CA might only accept CSRs that:

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

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

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

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

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

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. If a CA revokes a certificate, the client 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 ensure that your certificates are validated when you get a certificate issued by a Certificate Authority (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.
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, and the server certificate identifies the server with an FQDN, the client cannot identify the server as trusted and prompts the user.

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

**Certificate Requirements for Cloud-Based Servers**

Cisco WebEx Messenger and Cisco WebEx Meeting Center present the following certificates to the client:

- **CAS**
- **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 certificate that is stored in the Intermediate Certificate Authority validates the 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, you can find more information for the root certificate on the Apple support website at http://support.apple.com.
Service Discovery

• About Service Discovery, page 39
• How the Client Locates Services, page 40
• Cisco UDS SRV Record, page 42
• CUP Login SRV Record, page 43
• Collaboration Edge SRV Record, page 45

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:

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

Important: 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 you can deploy and explains the purpose and benefits of each record:
### SRV Record

<table>
<thead>
<tr>
<th>SRV Record</th>
<th>Purpose</th>
<th>Why You Deploy</th>
</tr>
</thead>
</table>
| _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 CCMCIP profiles or 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. |
| _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. **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 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.

To create a URL configuration link, you include:

• 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 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

When all three parameters are included, service discovery will not happen and the user will be 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
&ServiceDiscoveryExcludeServices=WEBEX,CUP`

Provide the link to users using email or a web site.

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 web site.

3. The client gets the address of the DNS name server from the DHCP settings.
4. The client 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.
5. The client queries the name server for the following SRV records in order of priority:
   • _cisco-uds
   • _cuplogin
The client caches the results of the DNS query to load on subsequent launches.

The following is an example of an SRV record entry:

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

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 following SRV record: `_cisco-uds`.

The following image illustrates how the client uses the `_cisco-uds` SRV record:

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

---

Cisco Jabber Planning Guide

42
As a result of automatically locating the user's home cluster, 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, 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*.

---

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`:

```plaintext
_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
```

**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 following SRV record: `_cuplogin`.

The following image illustrates how the client uses the `_cuplogin` SRV record:
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 SRV record: _collab-edge.

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 either 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 the Cisco Unified Communications Manager.
   The service profile contains the user's home cluster, the primary source of authentication, and the client configuration.
Security

• Federal Information Processing Standards (FIPS), page 47
• Compliance and Policy Control for File Transfer and Screen Capture, page 47
• Instant Message Encryption, page 48

Federal Information Processing Standards (FIPS)

Cisco Jabber for Windows only.

The Federal Information Processing Standard (FIPS) 140 is a US and Canadian government standard that specifies security requirements for cryptographic modules, including the set of hardware, software, and firmware that implements approved security functions and is contained within the cryptographic boundary.

FIPS requires that all encryption, key exchange, digital signatures, hash and random number generation functions used within Cisco Jabber for Windows be compliant with the FIPS 140.2 requirements for the security of cryptographic modules.

Cisco Jabber for Windows is compliant with FIPS 140.2. In order to run the client in FIPS mode, you must enable FIPS on your Windows operating system. The client detects that the operating system is in FIPS mode and correspondingly runs in FIPS mode.

FIPS mode results in the client managing certificates more strictly. Users in FIPS mode may see certificate errors be displayed in the client if a certificate for a service expires and users do not re-enter their credentials prior to expiry. Users also see a FIPS icon in their hub window to indicate the client is running in FIPS mode.

Compliance and Policy Control for File Transfer and Screen Capture

If you send file transfers and screen captures using the Managed file transfer option on Cisco Unified Communications Manager IM and Presence 10.5(2) or later, you can send the files to a compliance server for audit and policy enforcement.

For more information about compliance, see the Instant Messaging Compliance for IM and Presence Service on Cisco Unified Communications Manager guide.
For more information about configuring file transfer and screen capture, see the *Cisco Unified Communications Manager IM and Presence Deployment and Installation Guide*.

## Instant Message Encryption

Cisco Jabber uses TLS to secure 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:

<table>
<thead>
<tr>
<th>Connection</th>
<th>Protocol</th>
<th>Negotiation Certificate</th>
<th>Expected Encryption Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client to server</td>
<td>XMPP over TLS v2</td>
<td>X.509 Public Key Infrastructure certificate</td>
<td>AES 256 bit</td>
</tr>
</tbody>
</table>

### 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 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 Presence and Cisco Unified Communications Manager IM and Presence Service:

<table>
<thead>
<tr>
<th>Version</th>
<th>Key Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager IM and Presence Service versions 9.0.1 and higher</td>
<td>2048 bit</td>
</tr>
<tr>
<td>Cisco Unified Presence version 8.6.4</td>
<td>2048 bit</td>
</tr>
<tr>
<td>Cisco Unified Presence versions lower than 8.6.4</td>
<td>1024 bit</td>
</tr>
</tbody>
</table>

### XMPP Encryption

Cisco Unified Presence and Cisco Unified Communications Manager IM and Presence Service both use 256 bit length session keys 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 Presence or Cisco Unified Communications Manager IM and Presence Service. See the following documents 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**

If required, 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 Presence and Cisco Unified Communications Manager IM and Presence Service do not encrypt instant messages 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 you log.

See the following documents 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.

For more information about X.509 Public Key Infrastructure certificates, see the Internet X.509 Public Key Infrastructure Certificate and CRL Profile document.

## Cloud-Based Encryption

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

<table>
<thead>
<tr>
<th>Connection</th>
<th>Protocol</th>
<th>Negotiation Certificate</th>
<th>Expected Encryption Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client to server</td>
<td>XMPP within TLS</td>
<td>X.509 Public Key Infrastructure certificate</td>
<td>AES 128 bit</td>
</tr>
<tr>
<td>Client to client</td>
<td>XMPP within TLS</td>
<td>X.509 Public Key Infrastructure certificate</td>
<td>AES 256 bit</td>
</tr>
</tbody>
</table>

**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 length session keys 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 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 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.

For more information about X509 Public Key Infrastructure certificates, see the Internet X.509 Public Key Infrastructure Certificate and CRL Profile document.

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 you can set with these policies:

<table>
<thead>
<tr>
<th>Policy combination</th>
<th>Client to client encryption</th>
<th>When the remote client supports AES encryption</th>
<th>When the remote client does not support AES encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support AES Encoding For IM = false</td>
<td>No</td>
<td>Cisco Jabber sends unencrypted instant messages.</td>
<td>Cisco Jabber sends and receives unencrypted instant messages.</td>
</tr>
<tr>
<td>Support No Encoding For IM = true</td>
<td></td>
<td>Cisco Jabber does not negotiate a key exchange. As a result, other clients do not send Cisco Jabber encrypted instant messages.</td>
<td></td>
</tr>
<tr>
<td>Support AES Encoding For IM = true</td>
<td>Yes</td>
<td>Cisco Jabber sends and receives encrypted instant messages.</td>
<td>Cisco Jabber sends encrypted instant messages.</td>
</tr>
<tr>
<td>Support No Encoding For IM = true</td>
<td></td>
<td>Cisco Jabber displays an icon to indicate instant messages are encrypted.</td>
<td>Cisco Jabber receives unencrypted instant messages.</td>
</tr>
</tbody>
</table>
### 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:

![Lock Icon](image)

#### Padlock Icon for Client to Client Encryption

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

![Padlock Icon](image)

---

**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 the *About Encryption Levels* topic in the Cisco WebEx documentation.
Local Chat History

Cisco Jabber for iPhone and iPad does not encrypt archived instant message stored locally on a mobile device when local chat history is enabled. Disable local chat history if you do not want unencrypted instant messages to be stored locally.

Cisco Jabber for Android does not encrypt archived instant message stored locally on a mobile device when local chat history is enabled. Disable local chat history if you do not want unencrypted instant messages to be stored locally.

If you enable local chat history, Cisco Jabber for Windows does not archive instant messages in an encrypted format. In order to restrict access to chat history, the client saves archives to the following directory: %USERPROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\History\uri.db.

If you enable local chat history, Cisco Jabber for Mac does not archive instant messages in an encrypted format. In order to restrict access to chat history, Cisco Jabber saves archives to the following directory: ~/Library/Application Support/Cisco/Unified Communications/Jabber/CSF/History/uri.db.

For on-premises deployment, 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.

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.
Planning Considerations

• DNS Configuration, page 53
• How the Client Connects to Services, page 62
• High Availability for Instant Messaging and Presence, page 66
• Computer Telephony Integration Servitude, page 69

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 Jabber looks 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 Cisco Jabber 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 version 9.6 or later
  - Cisco Jabber for Mac version 9.6 or later
  - Cisco Jabber for iPhone and iPad version 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 version 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 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 version 9.6 or later
  - Cisco Jabber for Mac version 9.6 or later
  - Cisco Jabber for iPhone and iPad version 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 version 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 diagram illustrates the flow that the client uses to connect to services:

To discover available services, the client:

1. Checks if the network is inside or outside the firewall and if Expressway for Mobile and Remote Access is deployed. A query is sent 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.

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 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:

http://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:

http://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 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.

Note

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

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

• Web Proxy Auto-Detection (WPAD) protocol lookup is not supported.
• Proxy Authentication is not supported.
• Wildcards in the bypass list are not supported. Use example.com instead of *.example.com, for example.

Client Queries 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 diagram illustrates how the client connects to internal services:

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

There are three possible authenticators that 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:
   a. Determines that the Cisco WebEx Messenger service is the primary source of authentication.
   b. Automatically connects to the Cisco WebEx Messenger service.
   c. Prompts the user for credentials.
   d. Retrieves client and service configuration.

2. If the client discovers a `_cisco-uds` record, then the client:
   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 may have no practical effect if the client 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.
If the client discovers a _cuplogin record, the client:

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, then the client attempts to connect to internal servers through Expressway for Mobile and Remote Access.

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

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 _cisco-uds, 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 illustrates a 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.

With a separate domain design:

- 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.

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.

**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.

**Same Domain, Split-Brain**

The following figure illustrates a same domain, split-brain domain design:

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.
**Same Domain, Not Split-Brain**

The following figure illustrates a same domain, not split-brain domain design:

![Diagram](example.com)

In the same 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.

---

**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 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.

### On-Premises Deployments for Cisco Jabber for Windows

<table>
<thead>
<tr>
<th>Product Mode</th>
<th>Server Versions</th>
<th>Discovery Method</th>
<th>Non-DNS Method</th>
</tr>
</thead>
</table>
| Full UC (Default Mode) | Version 9.1.2 and higher:  
  - 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) | Version 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) | Version 9 and higher:  
  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> |
| IM Only (Default Mode) | Version 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> |
### Recommended Connection Methods

<table>
<thead>
<tr>
<th>Product Mode</th>
<th>Server Versions</th>
<th>Discovery Method</th>
<th>Non-DNS Method</th>
</tr>
</thead>
</table>
| Phone Mode   | Version 9 and higher: 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 |
| Phone Mode   | Version 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 |

---

**Note**

Cisco Jabber version 9.6 and higher can still discover full Unified Communications and Instant Messaging 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 wish users to bypass the email screen during the first login of a fresh installation.

---

**Note**

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

---

### On-Premises Deployments for Cisco Jabber for Mac

<table>
<thead>
<tr>
<th>Product Mode</th>
<th>Server Versions</th>
<th>Discovery Method</th>
</tr>
</thead>
</table>
| Full UC (Default Mode) | Version 9 and higher:  
  - Cisco Unified Communications Manager  
  - Cisco Unified Communications Manager IM and Presence Service | A DNS SRV request against _cisco-uds.<domain> |
### Discovery Method

<table>
<thead>
<tr>
<th>Product Mode</th>
<th>Server Versions</th>
<th>Discovery Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full UC (Default Mode)</td>
<td>Version 8.x:</td>
<td>A DNS SRV request against _cuplogin.&lt;domain&gt;</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Presence</td>
<td></td>
</tr>
</tbody>
</table>

### On-Premises Deployments for Cisco Jabber for Android and Cisco Jabber for iPhone and iPad

<table>
<thead>
<tr>
<th>Product Mode</th>
<th>Server Versions</th>
<th>Discovery Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full UC (Default Mode)</td>
<td>Version 9 and higher:</td>
<td>A DNS SRV request against _cisco-uds.&lt;domain&gt; and _cuplogin.&lt;domain&gt;</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager IM and Presence Service</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Product Mode</th>
<th>Server Versions</th>
<th>Discovery Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full UC (Default Mode)</td>
<td>Version 8.x:</td>
<td>A DNS SRV request against _cuplogin.&lt;domain&gt;</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Presence</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Product Mode</th>
<th>Server Versions</th>
<th>Discovery Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM Only (Default Mode)</td>
<td>Version 9 and higher:</td>
<td>A DNS SRV request against _cisco-uds.&lt;domain&gt; and _cuplogin.&lt;domain&gt;</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager IM and Presence Service</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Product Mode</th>
<th>Server Versions</th>
<th>Discovery Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM Only (Default Mode)</td>
<td>Version 8.x:</td>
<td>A DNS SRV request against _cuplogin.&lt;domain&gt;</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Presence</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Product Mode</th>
<th>Server Versions</th>
<th>Discovery Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone Mode</td>
<td>Version 9 and higher:</td>
<td>A DNS SRV request against _cisco-uds.&lt;domain&gt;</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Product Mode</th>
<th>Server Versions</th>
<th>Discovery Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone Mode</td>
<td>Version 8.x:</td>
<td>Manual connection settings or bootstrap file</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager</td>
<td>Manual connection settings</td>
</tr>
</tbody>
</table>
Cisco Unified Communications Manager version 9 and higher can still discover full Unified Communications and Instant Messaging only services using the _cuplogin DNS SRV request but a _cisco-uds request will take precedence if it is present.

**Hybrid Cloud-Based Deployments**

<table>
<thead>
<tr>
<th>Server Versions</th>
<th>Connection Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco WebEx Messenger</td>
<td>HTTPS request against <a href="http://loginp.webexconnect.com/cas/FederatedSSO?org=">http://loginp.webexconnect.com/cas/FederatedSSO?org=</a>&lt;domain&gt;</td>
</tr>
</tbody>
</table>

**Cloud-Based Deployments**

<table>
<thead>
<tr>
<th>Deployment Type</th>
<th>Connection Method</th>
</tr>
</thead>
</table>
| 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.

There are three possible sources of authentication, as follows:

**Cisco Unified 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.

**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.
Cisco Jabber supports high availability with the following servers:

**Cisco Unified Presence version 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 IM and Presence version 9.0 and higher**
Use the following Cisco Unified Communications IM and Presence 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 Re-Login Parameters**
In Cisco Unified Presence and Cisco Unified Communications IM and Presence, 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**
Client Behavior During Failover

The following workflow describes the client's behavior when the Cisco Unified Presence server failover:

1. When a 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.

**Computer Telephony Integration Servitude**

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.

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

For more information on CTI servitude, 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 JTAPI: [http://developer.cisco.com/web/jtapi/home](http://developer.cisco.com/web/jtapi/home)