Plan for Installation

Review what the client supports before you begin installation. Learn about hardware and software requirements. Find out what ports the client requires and what protocols it uses.

Hardware Requirements for Cisco Jabber for Windows

Installed RAM

2 GB RAM on Microsoft Windows 7 and Windows 8

Free Physical Memory

128 MB

Free Disk Space

256 MB

CPU Speed and Type

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

GPU

DirectX11 on Microsoft Windows 7

I/O Ports

USB 2.0 for USB camera and audio devices.

Software Requirements

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

Operating Systems for Cisco Jabber for Windows

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

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

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

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

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

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

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

Cisco Jabber supports the following on-premises servers:

- Cisco Unified Communications Manager, release 8.0(1) or later
- Cisco Unified Presence, release 8.0(3) or later

- Cisco Unity Connection, release 8.5 or later
- Cisco WebEx Meetings Server, version 1.1 or later
- Cisco Expressway Series for Cisco Unified Communications Manager
  - Cisco Expressway-E, version 8.1.1 or later
  - Cisco Expressway-C, version 8.1.1 or later
- Cisco TelePresence Video Communications Server
  - Cisco VCS Expressway, version 8.1.1 or later
  - Cisco VCS Control, version 8.1.1 or later

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

- Basic call functionality
- Ability to hold and resume calls

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

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

High Availability for Instant Messaging and Presence

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

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

Cisco Jabber supports high availability with the following servers:

Cisco Unified Presence releases 8.5 and 8.6

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

Configuration and Administration of Cisco Unified Presence Release 8.6

```
Multi-node Deployment Administration
Troubleshooting High Availability
```

Deployment Guide for Cisco Unified Presence Release 8.0 and 8.5

```
Planning a Cisco Unified Presence Multi-Node Deployment
```

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

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

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

`High Availability Client Login Profiles`

`Troubleshooting High Availability`

Active Calls on Hold During Failover

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

High Availability in the Client

Client Behavior During Failover

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

Configure Login Parameters

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

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

Related Topics

Cisco Unified Communications Manager Configuration Guides
Cisco Unified Presence Configuration Guides
Supported Services

Cloud-Based Servers

Cisco Jabber supports integration with the following hosted servers:

- Cisco WebEx Messenger service
- Cisco WebEx Administration Tool, minimum supported version is 7.5
- Cisco WebEx Meeting Center, minimum supported versions are as follows:
  - Version T26L with Service Pack EP 20
  - Version T27L with Service Pack 9

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
- Active Directory for Windows Server 2003 R2
- Cisco Unified Communications Manager User Data Server (UDS)

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

  Cisco Unified Communications Manager, version 9.1(2), with the following Cisco Options Package (COP) file: `cmterm-cucm-uds-912-5.cop.sgn`.
  Cisco Unified Communications Manager, version 10.0(1). No COP file is required.
- OpenLDAP
- Active Directory Lightweight Directory Service (AD LDS) or Active Directory Application Mode (ADAM)

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

Microsoft Internet Explorer

Cisco Jabber for Windows requires Microsoft Internet Explorer 7 or later. Cisco Jabber for Windows uses the Internet Explorer rendering engine to display HTML content.

Attention Cisco Jabber for Windows requires Internet Explorer active scripting to render instant messages. See the following Microsoft documentation for instructions to enable active scripting: http://windows.microsoft.com/en-US/windows/help/genuine/ie-active-script

Known Issues with Internet Explorer

- In cloud-based deployments that use single sign-on (SSO), an issue exists with Internet Explorer 9. Users with Internet Explorer 9 get security alerts when they sign in to Cisco Jabber for Windows. To resolve this issue, add `webexconnect.com` to the list of websites in the **Compatibility View Settings** window.

Microsoft Office

Cisco Jabber for Windows supports integration with the following software:

- Microsoft Office 2007 32 bit
- Microsoft Office 2010, 32 and 64 bit

- Microsoft Office 2013, 32 and 64 bit

Add Local Contacts from Microsoft Outlook

Cisco Jabber for Windows lets users search for and add local contacts in Microsoft Outlook. To enable this integration with Microsoft Outlook, you must enable Cached Exchange Mode on the Microsoft Exchange server.

To search for local contacts in Microsoft Outlook with the client, users must have profiles set in Microsoft Outlook. In addition, users must do the following:

1. Select **File** > **Options**.
2. Select the **Integration** tab (**Calendar** tab from release 11.0).
3. Select either **None** or **Microsoft Outlook**.

To add local Microsoft Outlook contacts to contact lists in the client, local contacts must have instant message addresses in Microsoft Outlook.

To show contact photos in the client interface, local contacts in Microsoft Outlook must have instant message addresses.

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

Microsoft Outlook Calendar Events

Applies to: Cisco Jabber for Windows

You must apply a setting in Microsoft Outlook so that calendar events display in Cisco Jabber for Windows.

Procedure

Step 1 Open the email account settings in Microsoft Outlook, as in the following example:

a) Select **File** > **Account Settings**.
b) Select the **Email** tab on the **Account Settings** window.

Step 2 Double-click the server name.

In most cases, the server name is **Microsoft Exchange**.

Step 3 Select the **Use Cached Exchange Mode** checkbox.

Step 4 Apply the setting and then restart Microsoft Outlook.

When users create calendar events in Microsoft Outlook, those events display in the **Meetings** tab.

Microsoft Outlook Presence Integration

Applies to: Cisco Jabber for Windows

To enable integration with Microsoft Outlook, you must specify `SIP:user@cupdomain` as the value of the `proxyAddresses` attribute in Microsoft Active Directory. Users can then share availability in Microsoft Outlook.

Use one of the following methods to modify the `proxyAddresses` attribute:

- **An Active Directory administrative tool such as Active Directory User and Computers**

  The Active Directory User and Computers administrative tool allows you to edit attributes on Microsoft Windows Server 2008 or later.

- **ADSchemaWizard.exe utility**

  The ADSchemaWizard.exe utility is available in the Cisco Jabber administration package. This utility generates an LDIF file that modifies your directory to add the `proxyAddresses` attribute to each user with the following value: `SIP:user@cupdomain`.

  You should use the ADSchemaWizard.exe utility on servers that do not support the edit attribute feature in the Active Directory User and Computers administrative tool. You can use a tool such as ADSI Edit to verify the changes that you apply with the ADSchemaWizard.exe utility.

  The ADSchemaWizard.exe utility requires Microsoft .NET Framework version 3.5 or later.

- **Create a script with Microsoft Windows PowerShell**

  Refer to the appropriate Microsoft documentation for creating a script to enable presence in Microsoft Outlook.

Enable Presence with the Active Directory User and Computers Tool

Complete the following steps to enable presence in Microsoft Outlook for individual users with the Active Directory User and Computers administrative tool:

Procedure

Step 1 Start the Active Directory User and Computers administrative tool.

You must have administrator permissions to run the Active Directory User and Computers administrative tool.

Step 2 Select **View** in the menu bar and then select the **Advanced Features** option from the drop-down list.

Step 3 Navigate to the appropriate user in the Active Directory User and Computers administrative tool.

Step 4 Double click the user to open the **Properties** dialog box.

Step 5 Select the **Attribute Editor** tab.

Step 6 Locate and select the `proxyAddresses` attribute in the **Attributes** list box.

Step 7 Select **Edit** to open the **Multi-valued String Editor** dialog box.

Step 8 In the **Value to add** text box, specify the following value: `SIP:user@cupdomain`.

For example, `SIP:msmith@cisco.com`.

Where the `user@cupdomain` value is the user's instant messaging address. `cupdomain` corresponds to the domain for Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.

Microsoft SharePoint

Cisco Jabber for Windows supports the following versions of Microsoft SharePoint:

- Microsoft SharePoint 2007
- Microsoft SharePoint 2010
- Microsoft SharePoint 2013

Important Cisco Jabber for Windows supports availability status in Microsoft SharePoint sites only if users access those sites with Microsoft Internet Explorer. You should add the Microsoft SharePoint site to the list of trusted sites in Microsoft Internet Explorer.

Microsoft Office 365

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

Cisco Jabber for Windows supports client-side integration with Microsoft Office 365 with the following applications:

- Microsoft Office 2013 32 bit and 64 bit
- Microsoft Office 2010 32 bit and 64 bit
- Microsoft Office 2007 32 bit
- Microsoft SharePoint 2010

Calendar Integration

You can use the following client applications for calendar integration:

- Microsoft Outlook 2013, 32 bit and 64 bit
- Microsoft Outlook 2010, 32 bit and 64 bit
- IBM Lotus Notes 9, 32 bit
- IBM Lotus Notes 8.5.3, 32 bit
- IBM Lotus Notes 8.5.2, 32 bit
- IBM Lotus Notes 8.5.1, 32 bit
- Google Calendar

Related Topics

Deployment in a Virtual Environment

Calendar Integration Issues after Upgrading to Outlook 2013

There is a known issue when upgrading to a version of Outlook 2013 that is not part of Microsoft Office Professional Plus 2013. If users find that their calendar integration does not work, do the following:

Procedure

Step 1 In the Microsoft Windows registry editor locate the following key: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Messaging Subsystem`.

Step 2 Add a new string value with the name: `MAPIX`.

Step 3 Open the new string value and enter `1` for the value data.

Step 4 Restart the Cisco Jabber client.

Computer Telephony Integration

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

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

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

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

Ports and Protocols for Desktop Clients

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

Port	Protocol	Description
443	TCP (Extensible Messaging and Presence Protocol [XMPP] and HTTPS)	XMPP traffic to the WebEx Messenger service. The client sends XMPP through this port in cloud-based deployments only. If port 443 is blocked, the client falls back to port 5222. **Note** Cisco Jabber can also use this port for: • HTTPS traffic to Cisco Unity Connection and Cisco WebEx Meetings Server. • Saving chats to the Microsoft Exchange server.
30000 to 39999	UDP	The client uses this port for far end camera control.
389	UDP/TCP	Lightweight Directory Access Protocol (LDAP) directory server.
636	LDAPS	LDAP directory server (secure).
2748	TCP	Computer Telephony Interface (CTI) used for desk phone control.
3268	TCP	Global Catalog server.
3269	LDAPS	Global Catalog server (secure).
5070 to 6070	UDP	Binary Floor Control Protocol (BFCP) for video desktop sharing capabilities.
5222	TCP (XMPP)	XMPP traffic to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.
8443	TCP (HTTPS)	Traffic to Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service.
7080	TCP (HTTPS)	Cisco Unity Connection for notifications of voice messages (new message, message update, and message deletion).
53	UDP/TCP	Domain Name System (DNS) traffic.
80	HTTP	Saving chats to Microsoft Exchange server. Depending on your server configuration on Microsoft Exchange, use either port 80 or 443, but not both.
37200	SOCKS5 Bytestreams	Peer-to-peer file transfers. In on-premises deployments, the client also uses this port to send screen captures.

Port	Protocol	Description
5060	UDP/TCP	Session Initiation Protocol (SIP) call signaling.
5061	TCP	Secure SIP call signaling.

Ports for Additional Services and Protocols

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

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

Call Control with Accessories API

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

Compatible Third Party Accessories

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

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

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

Install Vendor Plugins

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

Procedure

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

Step 2 Install the plugin separately to Cisco Jabber.

Plugin Versions

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

- Jabra PC Suite Version 2.12.3655
- Logitech UC Plugin 1.1.27

CTI Supported Devices

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

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

Supported Audio Codecs

- 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

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

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

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

COP File	Description	Cisco Unified Communications Manager Versions
ciscocm.installcsfdevicetype.cop.sgn	Adds the CSF device type to Cisco Unified Communications Manager. For more information, see *Software Requirements*.	7.1.3
cmterm-bfcp-e.8-6-2.cop.sgn	Enables CSF devices to support BFCP video desktop sharing. For more information, see *Apply COP File for BFCP Capabilities*.	8.6.2 only
ciscocm.addcsfsupportfield.cop.sgn	Adds the **CSF Support Field** field for group configuration files. For more information, see *Create Group Configurations*.	8.6.1 and earlier
cmterm-cupc-dialrule-wizard-0.1.cop.sgn	Publishes application dial rules and directory lookup rules to Cisco Jabber. For more information, see *Publish Dial Rules*.	8.6.1 and earlier

Related Topics

Download software

Client Availability

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

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

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

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

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

- Cisco Jabber Client — Applies to on-premises and cloud-based deployments. You must disable Cisco Unified Communication Manager IM and Presence and Microsoft Exchange integration for the client to

set the **In a meeting** availability. The client checks if integration between Cisco Unified Communication Manager IM and Presence and Microsoft Exchange is on or off. The client can only set availability if integration is off.

The following deployment scenarios describe how availability is created:

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

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

Availability Enabled in the Client	Availability Enabled by Integrating Cisco Unified Communication Manager IM and Presence with Microsoft Exchange
Offline in a meeting availability is not supported.	**Offline in a meeting** availability is supported.
In a meeting availability is supported for non-calendar events.	**In a meeting** availability is not supported for non-calendar events.
Note Offline in a meeting availability refers to when the user is not logged in to the client but an event exists in the user's calendar. Non-calendar events refer to events that do not appear in the user's calendar, such as instant meetings, **Offline**, or **On a call**.	

Related Topics

Calendar Integration, on page 8

Instant Message Encryption

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

On-Premises Encryption

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

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

Server and Client Negotiation

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

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

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

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

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

XMPP Encryption

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

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

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

Instant Message Logging

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

databases or in third party compliance servers. You must configure your external database or third party compliance server as appropriate to protect the instant messages that you log.

See the following for more information about compliance:

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

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

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

Related Topics

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

Cloud-Based Encryption

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

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

Server and Client Negotiation

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

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

XMPP Encryption

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

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

Instant Message Logging

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

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

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

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

Related Topics

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

Client-to-Client Encryption

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

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

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

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

Policy Combination	Client-to-Client Encryption	When the Remote Client Supports AES Encryption	When the Remote Client Does not Support AES Encryption
Support AES Encoding For IM = false **Support No Encoding For IM** = true	No	Cisco Jabber sends unencrypted instant messages. Cisco Jabber does not negotiate a key exchange. As a result, other clients do not send Cisco Jabber encrypted instant messages.	Cisco Jabber sends and receives unencrypted instant messages.

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

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

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

Related Topics

About Encryption Levels

Encryption Icons

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

Lock Icon for Client to Server Encryption

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

Padlock Icon for Client to Client Encryption

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

Local Chat History

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

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

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

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

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

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

Quality of Service Configuration

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

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

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

Cisco Media Services Interface

Cisco Media Services Interface provides a service that works with Cisco Prime Collaboration Manager and Cisco Medianet-enabled routers to ensure that Cisco Jabber can send audio media and video media on your network with minimum latency or packet loss.

Before Cisco Jabber sends audio media or video media, it checks for Cisco Media Services Interface.

- If the service exists on the computer, Cisco Jabber provides flow information to Cisco Media Services Interface.

The service then signals the network so that routers classify the flow and provide priority to the Cisco Jabber traffic.

- If the service does not exist, Cisco Jabber does not use it and sends audio media and video media as normal.

Note Cisco Jabber checks for Cisco Media Services Interface for each audio call or video call.

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

Related Topics

Install Cisco Media Services Interface

Set DSCP Values

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

Port Ranges on Cisco Unified Communications Manager

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

Define a Port Range on the SIP Profile

The client uses the port range to send RTP traffic across the network. The client divides the port range equally and uses the lower half for audio calls and the upper half for video calls. As a result of splitting the port range for audio media and video media, the client creates identifiable media streams. You can then classify and prioritize those media streams by setting DSCP values in the IP packet headers.

Procedure

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

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

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

The **SIP Profile Configuration** window opens.

Step 4 Specify the port range in the following fields:

- **Start Media Port** — Defines the start port for media streams. This field sets the lowest port in the range.
- **Stop Media Port** — Defines the stop port for media streams. This field sets the highest port in the range.

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

Related Topics

8.6.x: SIP Profile Configuration

9.0.x: SIP profile setup

How the Client Uses Port Ranges

Cisco Jabber equally divides the port range that you set in the SIP profile. The client then uses the port range as follows:

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

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

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

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

Options for Setting DSCP Values

The following table describes the options for setting DSCP values:

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

Set DSCP Values on Cisco Unified Communications Manager

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

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

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

Procedure

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

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

The **Service Parameter Configuration** window opens.

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

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

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

Set DSCP Values with Group Policy

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

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

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

Attributes	Audio Policy	Video Policy	Signaling Policy
Application name	`CiscoJabber.exe`	`CiscoJabber.exe`	`CiscoJabber.exe`
Protocol	UDP	UDP	TCP
Port number or range	Corresponding port number or range from the SIP profile on Cisco Unified Communications Manager.	Corresponding port number or range from the SIP profile on Cisco Unified Communications Manager.	5060 for SIP 5061 for secure SIP
DSCP value	46	34	24

Set DSCP Values on the Network

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

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

- Media Streams — Because the client uses different port ranges for audio streams and video streams, you can differentiate audio media and video media based on those port range. Using the default port ranges in the SIP profile, you should mark media packets as follows:
  - Audio media streams in ports from 16384 to 24574 as EF
  - Video media streams in ports from 24575 to 32766 as AF41
- Signaling Streams — You can identify signaling between the client and servers based on the various ports required for SIP, CTI QBE, and XMPP. For example, SIP signaling between Cisco Jabber and Cisco Unified Communications Manager occurs through port 5060.

  You should mark signaling packets as AF31.

Protocol Handlers

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

- XMPP: or XMPP://

  Starts an instant message and opens a chat window in Cisco Jabber.

- IM: or IM://

  Starts an instant message and opens a chat window in Cisco Jabber.

- TEL: or TEL://

  Starts an audio or video call with Cisco Jabber.

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

- CISCOTEL: or CISCOTEL://

  Starts an audio or video call with Cisco Jabber.

- SIP: or SIP://

  Starts an audio or video call with Cisco Jabber.

- CISCOTELCONF:

  Starts a conference call with Cisco Jabber.

Registry Entries for Protocol Handlers

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

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

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

Related Topics

Protocol Handlers on HTML Pages, on page 24

Protocol Handlers on HTML Pages

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

TEL and IM Protocol Handlers

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

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

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

CISCOTEL and SIP Protocol Handlers

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

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

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

CISOTELCONF Protocol Handler

Example of the CISCOTELCONF protocol handler on an HTML page:

```
<html>
  <body>
       <a href="CISCOTELCONF:msmith@domain;amckenzi@domain">Weekly conference call</a>
  </body>
</html>
```

In the preceding example, when users click the *Weekly conference call* hyperlink, a conference call is set up between Mary, Adam, and the user who clicked the link.

Tip Add lists of contacts for the CISCOTELCONF: handler to create conference calls. Use a semi-colon to delimit contacts, as in the following example:

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

XMPP Protocol Handlers

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

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

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

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

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

Related Topics

Registry Entries for Protocol Handlers, on page 23

Audio and Video Performance Reference

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

Audio Bit Rates for Cisco Jabber Desktop Clients

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

Codec	RTP (kbits/second)	Actual bit rate (kbits/second)	Notes
G.722.1	24/32	54/62	High quality compressed
G.711	64	80	Standard uncompressed
G.729a	8	38	Low quality compressed

Video Bit Rates for Cisco Jabber Desktop Clients

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

Resolution	Pixels	Measured bit rate (kbits per second) with g.711 audio
w144p	256 x 144	156

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

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

Presentation Video Bit Rates

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

The values in this table do not include audio.

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

Maximum Negotiated Bit Rate

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

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

Desktop sharing session	Audio	Interactive video (Main video)	Presentation video (Desktop sharing video)
No	Cisco Jabber uses the maximum audio bit rate.	Cisco Jabber allocates the remaining bit rate as follows: The maximum video call bit rate minus the audio bit rate.	—

Desktop sharing session	Audio	Interactive video (Main video)	Presentation video (Desktop sharing video)
Yes	Cisco Jabber uses the maximum audio bit rate.	Cisco Jabber allocates half of the remaining bandwidth after subtracting the audio bit rate.	Cisco Jabber allocates half of the remaining bandwidth after subtracting the audio bit rate.

Bandwidth Performance Expectations for Cisco Jabber Desktop Clients

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

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

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

Video Rate Adaptation

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

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