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 Mac

Installed RAM

2 GB RAM

Free Physical Memory

1 GB

Free Disk Space

300 MB

CPU Speed and Type

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

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

I/O Ports

USB 2.0 for USB camera and audio devices.

Software Requirements

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

Operating Systems for Cisco Jabber for Mac

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

- Apple OS X Lion Version 10.7.4 (or later)
- Apple OS X Mountain Lion 10.8.1 (or later)
- Apple OS X Mavericks 10.9 (or later)

This version of Cisco Jabber for Mac is not supported on Apple OS X Yosemite 10.10

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 8.0(1) or later
- Cisco Unified Presence version 8.0(3) or later
- Cisco Unity Connection version 8.5 or later
- Cisco WebEx Meetings Server version 2.0 or later
- Cisco Expressway Series for Cisco Unified Communications Manager
    - Cisco Expressway-E Version 8.1.1
    - Cisco Expressway-C Version 8.1.1

- Cisco TelePresence Video Communication Server
  - Cisco VCS Expressway Version 8.1.1
  - Cisco VCS Control Version 8.1.1

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.

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.

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**

Related Topics

8.6: How To Configure High Availability Cisco Unified Presence Deployments
8.6: High Availability Client Login Profiles
8.6: Configuring the Advanced Service Parameters for the Server Recovery Manager
8.6: Impact of Failover to Cisco Unified Presence Clients and Services
9.0(1): High Availability IM and Presence deployments configuration
9.0(1): High Availability client login profiles
9.0(1): Configure advanced service parameters for Server Recovery Manager
9.0(1): Impact of failover to IM and Presence clients and 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 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

Restriction Directory integration with OpenLDAP requires you to define specific parameters in a Cisco Jabber configuration file. See *LDAP Directory Servers* for more information.

Local Contacts in Mac Address Book

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

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

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

To enable the Address Book plug-in:

1 Select **Jabber** > **Preferences** > **General** > **Enable "Mac Address Plug-in"**.

2 Restart the client for this to take effect.

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

CTI Servitude

Cisco Jabber for Windows and Cisco Jabber for Mac support Computer Telephony Integration (CTI) servitude, or CTI control of Cisco Jabber from a third party application.

For more information on CTI servitude, see the CTI documentation for the appropriate version of Cisco Unified Communications Manager.

See the following sites on the Cisco Developer Network for more information about creating applications for CTI control through Cisco Unified Communications Manager APIs:

- Cisco TAPI: http://developer.cisco.com/web/tapi/home
- Cisco JTAPI: http://developer.cisco.com/web/jtapi/home

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:

Port	Protocol	Description
443	TCP (XMPP and HTTPS)	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. **Note** Cisco Jabber can also use this port for HTTPS traffic to Cisco Unity Connection and Cisco WebEx Meetings Server.
389	UDP / TCP	LDAP directory server
636	LDAPS	LDAP directory server (secure)
3268	TCP	Global Catalog server
3269	LDAPS	Global Catalog server (secure)
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
37200	SOCKS5 Bytestreams	Peer to peer file transfers. In on-premises deployments, the client also uses this port to send screen captures.
5060	UDP/TCP	Session Initiation Protocol (SIP) call signalling

Port	Protocol	Description
5061	TCP	Secure SIP call signalling

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*.

CTI Supported Devices

Cisco Jabber supports the same CTI devices as Cisco Unified Communications Manager version 8.6(1). See the *CTI Supported Device Matrix* in the *CTI Supported Devices* topic.

Related Topics

CTI Supported Devices

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

Supported Audio Codecs

- G.722.1
  - G.722.1 32k
  - G.722.1 24k

Note G.722.1 is supported on Cisco Unified Communications Manager 8.6.1 or later.

- G.711
  - G.711 A-law

- G.711 u-law

- G.729a

Supported Video Codecs

- 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
ciscocm.addcsfsupportfield.cop.sgn	Adds the **CSF Support Field** field for group configuration files. For more information, see *Create Group Configurations*.	8.6.x and lower
cmterm-cupc-dialrule-wizard-0.1.cop.sgn	Publishes application dial rules and directory lookup rules to Cisco Jabber. For more information, see *Publish Dial Rules*.	All supported versions

Related Topics

Download software

Availability Presence on Client

For on-premise deployments, the Cisco Jabber for Mac client displays the **In a meeting (according to my calendar)** checkbox on the **Preferences** > **Status** window.

The client displays the 'In a meeting' availability status when events occur in your calendar:

'In a meeting' availability status comes from Microsoft Exchange

Requires Cisco Unified Presence and Microsoft Exchange integration or Cisco Unified Communications IM and Presence and Microsoft Exchange integration. Applies to on-premise deployments.

Availability status changes to 'In a meeting' if events occur in your calendar when:

Deployment	Select In a meeting (according to my calendar)	Do Not Select In a meeting (according to my calendar)
You enable integration between Cisco Unified Presence and Microsoft Exchange or Cisco Unified Communications IM and Presence and Microsoft Exchange.	Cisco Unified Presence or Cisco Unified Communications IM and Presence sets availability status	Availability status does not change

Note **In a meeting** availability status refers to calendar meetings that are created using the Cisco Unified Presence and Microsoft Exchange integration or Cisco Unified Communications IM and Presence and Microsoft Exchange integration. **In a WebEx meeting** availability status refers to Cisco WebEx meetings. The client does not display other availability statuses from other calendar sources (such as Microsoft Outlook for Mac).

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-premise deployments:

Connection	Protocol	Negotiation Certificate	Expected Encryption Algorithm
Client to server	XMPP over 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 following:

- Cisco Unified Presence

- Cisco Unified Communications IM and Presence

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 IM and Presence:

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

XMPP Encryption

Cisco Unified Presence and Cisco Unified Communications IM and Presence 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 IM and Presence. See the following documents for more information about security settings:

- Cisco Unified Presence: *Configuring Security on Cisco Unified Presence*
- Cisco Unified Communications IM and Presence: *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 IM and Presence 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 IM and Presence: *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 X509 Public Key Infrastructure certificates, see the *Internet X.509 Public Key Infrastructure Certificate and CRL Profile* document.

Related Topics

Instant Messaging Compliance Guide
Configuring Security on Cisco Unified Presence
Instant Messaging Compliance for IM and Presence Service

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

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.

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.

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.

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 you can set with these policies:

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

Note

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

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

Related Topics

About Encryption Levels

Local Chat History

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.

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

Cisco Media Services Interface provides a Mac daemon 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.

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.

Specify a Port Range on the SIP Profile

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

Procedure

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

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

Step 3 Find the appropriate SIP profile or create a new SIP profile.
The **SIP Profile Configuration** window opens.

Step 4 Specify the port range in the following fields:

Start Media Port

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

Stop Media Port

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

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

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

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.

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 on the Client

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

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

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

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

Procedure

Step 1 Select **Jabber > Preferences > Calls > Advanced**

Step 2 Select **Enable Differentiated Service for Calls**.

Set DSCP Values on the Network

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

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

Media Streams

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

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

Signaling Streams

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

You should mark signaling packets as AF31.

Protocol Handlers

Cisco Jabber registers protocol handlers with the OSX launch services database to enable click-to-call or click-to-IM functionality from web browsers or other applications.

Click to Call protocol handlers - Starts an audio or video call with Cisco Jabber:

- TEL:
- SIP:

- CiscoTEL:

Click to IM protocol handlers - Starts an instant message and opens a chat window in Cisco Jabber:

- XMPP:
- Jabber:
- CiscoIM:

Audio and Video Performance Reference

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

Bit Rates for Audio for Cisco Jabber for Windows and Cisco Jabber for Mac

The following table describes bit rates for audio:

Codec	RTP payload in kilobits (kbits) per second	Actual bitrate (kbits per second)	Notes
g.722.1	24/32	54/62	High quality compressed
g.711	64	80	Standard uncompressed
g.729a	8	38	Low quality compressed

Bit Rates for Video for Cisco Jabber for Windows and Cisco Jabber for Mac

The following table describes bit rates for video with g.711 audio:

Resolution	Pixels	Measured bit rate (kbits per second) with g.711 audio
w144p	256 x 144	156
w288p This is the default size of the video rendering window for Cisco Jabber.	512 x 288	320
w448p	768 x 448	570
w576p	1024 x 576	890
720p	1280 x 720	1300

Notes about the preceding table:

- This table does not list all possible resolutions.
- The measured bit rate is the actual bandwidth used (RTP payload + IP packet overhead).

Maximum Negotiated Bit Rate

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

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

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

Performance Expectations for Bandwidth for Cisco Jabber for Windows and Cisco Jabber for Mac

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

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

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.