Plan for Installation

Device Requirements

Device Support

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

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

- iPhone model 4, 4S, 5, 5C, and 5S
- iPad second, third, fourth generation, iPad mini with Retina display, and iPad Air

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

Device Operating System Support

iOS support: iOS 7

Bluetooth Headset Support

iPhone: supported (optional)

iPad: Supported (optional)

Software Requirements

For a successful deployment, you must ensure that your environment meets the Cisco Jabber for iPhone and iPad software requirements.

On-Premises Servers

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 and it requires:

- Cisco Jabber for iPhone and iPad client, Release 9.6

Cisco Unified Presence

- Cisco Unified Presence Release 8.6

Cisco Unified Communications Manager IM and Presence

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

- Cisco Unified Communications Manager IM and Presence Release 9.1
- Cisco Unified Communications Manager IM and Presence 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 a (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*.
- Certificate Authority (CA) if using certificate-based authentication: Cisco IOS Certificate Server, Cisco IOS Certificate Server or Microsoft Windows Server 2003 Enterprise Certificate Authority

Related Topics

Cisco Unified Communications Manager Maintain and Operate Guides
VPN License and Feature Compatibility

Cloud-Based Servers

Cisco Jabber for iPhone and iPad supports the following cloud-based servers:

- Cisco WebEx Messenger Release 7.5 or later
- Cisco WebEx Administration Tool Release 7.5
- Cisco WebEx Meeting Center as follows:
  - Version T26L with Service Pack 20
  - Version T27L with Service Pack 9

Directory Servers

You can use the following directory servers with Cisco Jabber for iPhone and iPad.

Note Cisco Unified Communications Manager User Data Services (UDS) is not supported for directory integration in this release.

LDAP

Use one of the following sources for Lightweight Directory Access Protocol (LDAP):

- Microsoft Active Directory 2008
- Microsoft Active Directory 2003
- OpenLDAP 2.4

Cloud-based

Cisco WebEx Messenger Contact Service

Accessibility

Screen Readers

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

Assistive Touch

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

Supported Codecs

Supported Audio Codecs

- G.711
- G.729a
- G.722.1

Minimum requirement for low-bandwidth availability: G.729a.

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

Normal mode supports G.711 and G.729a.

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 does not support visual voicemail with G.729. However, users can access their voice messages using G.729 and the **Call Voicemail** feature.

Network Requirements

If you deploy Phone Services, the mobile device must be able to connect to the corporate network using voice-ready Wi-Fi.

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 4.1 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 VPN connection. Video and audio quality is dependent on connection quality and cannot be guaranteed.

Related Topics

Enterprise Mobility 4.1 Design Guide
Cisco Unified Wireless IP Phone 7925G Deployment Guide
Capacity Coverage and Deployment Considerations for IEEE 802.11g
Solutions Reference Network Design (SRND)

Ports and Protocols

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.

Port	Protocol	Description
Inbound		
16384 to 32766	UDP	Receives Real-Time Transport Protocol (RTP) media streams for audio and video. You set these ports in Cisco Unified Communications Manager.
Outbound		
69	UDP	Connects to the Trivial File Transfer Protocol (TFTP) server.
6970	HTTP	Connects to the TFTP server to download client configuration files.
80	TCP (HTTP)	Connects to services such as Cisco WebEx Meeting Center for meetings or Cisco Unity Connection for voicemail.
389	UDP / TCP	Connects to an LDAP directory service.
3268	TCP	Connects to a Global Catalog server for contact searches.
443	TCP (HTTPS)	Connects to services such as such as Cisco WebEx Meeting Center for meetings or Cisco Unity Connection for voicemail.
636	LDAPS	Connects securely to an LDAP directory service.
3269	LDAPS	Connects securely to the Global Catalog server.
5060	TCP	Provides Session Initiation Protocol (SIP) call signaling.

Port	Protocol	Description
5061	TCP	Provides secure SIP call signaling.
5222	TCP (XMPP)	Connects to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence for instant messaging and presence.
5269	XMPP	XMPP federation.
8191	TCP	Connects to the local port to provide Simple Object Access Protocol (SOAP) web services.
8443	HTTPS	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	UDP	Sends RTP media streams for audio and video.
53	DNS	Provides hostname resolution.
3804	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.

Device COP File for Cisco Jabber for iPhone and iPad

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

1. Go to the software download site: http://www.cisco.com/go/jabber_iphone_cop..
2. Locate `cmterm-iphone-install-130917.cop.sgn` for TCT device and `cmterm-jabberipad-130917.cop.sgn` for TAB device..
3. Download the file.

Audio and Video Performance Reference

Learn about audio and video performance for Cisco Jabber for iPhone and iPad.

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

The following table describes bit rates for audio:

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

Bit Rates for Video

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

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

Notes about the preceding table:

- The client captures and transmits at 20 fps.
- The values in this table do not include audio.

Maximum Negotiated Bit Rate

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

Audio

The client uses the maximum audio bit rate.

Interactive Video

The client allocates the remaining bit rate as follows: The maximum video call bit rate minus the audio bit rate.

Performance Expectations for Bandwidth

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

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

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

Video Rate Adaption

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

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

Quality of Service Configuration

Review the supported methods to configure Quality of Service (QoS) for the client.

Port Ranges on Cisco Unified Communications Manager

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

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

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

Related Topics

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

Cross-Launching the Client

Users can launch the client from web browsers to perform one of the following tasks:

- Call a phone number
- Start a chat session

The following table lists the cross-launch URLs that you can use in third-party applications to start Cisco Jabber conversations.

Function	Cross-Launch URL	Prerequisites
Call a phone number	`ciscotel://<phone_number>`	Cisco Unified Communications Manager account
Start a chat session	• `xmpp://<instant_message_id>` • `im://<instant_message_id>` • `ciscoim://<instant_message_id>`	One of the following accounts: • Cisco WebEx Messenger • Cisco Unified Presence • Cisco Unified Communications Manager IM and Presence