Cisco Jabber for iPad
Deployment Guide

Version 1.0
October 2012

For further information, questions and comments please contact ccbu-pricing@cisco.com
## Contents

**Introduction** .......................................................................................................................... 3  
Cisco Jabber Messaging Integration Platform .............................................................................. 3  
Cisco Jabber for iPad .................................................................................................................. 3  
**What You Will Learn** ............................................................................................................ 3  
**Deployment Models** ............................................................................................................. 3  
**Prerequisites** ........................................................................................................................ 4  
**Best Practices for Deployment** ............................................................................................. 5  
**Back-End Services** .............................................................................................................. 5  
**Wi-Fi Network Connectivity and Security** ........................................................................... 7  
  Apple iPad Wi-Fi Specifications ................................................................................................... 7  
  Site Survey ................................................................................................................................ 7  
  WLAN Considerations for Cisco Jabber for iPad Deployment .................................................... 8  
**Bandwidth Management and QoS** ....................................................................................... 13  
**Configuration for Large Numbers of Users** ....................................................................... 14  
  Cisco WebEx Messenger Service .............................................................................................. 14  
  Cisco Unified Communications Manager .................................................................................. 14  
  Cisco VCS and Cisco TMS ......................................................................................................... 14  
**Jabber for iPad Client Deployment** ..................................................................................... 15  
  Individual Accounts .................................................................................................................. 16  
  Company-Provided Accounts .................................................................................................... 16  
**Security Considerations** ...................................................................................................... 18  
  AnyConnect VPN ..................................................................................................................... 18  
  Port Configuration ..................................................................................................................... 19  
**Appendix A: Cisco Unified Communications Manager Bulk Provisioning** ....................... 20  
**Appendix B: Installing Cisco TMS Provisioning Template** .................................................. 22  
**Appendix C: Jabber for iPad Problem Report** .................................................................... 22
Introduction

Cisco Jabber Messaging Integration Platform

The Cisco Jabber™ Family of unified communications client applications streamlines communications and enhances productivity with unified communications capabilities including presence, instant messaging (IM), voice and video, voice messaging, desktop sharing, and conferencing capabilities. Cisco Jabber applications provide a high-quality user experiences across a broad range of platforms, browsers, and devices. You can use the Jabber® platform as a rich client, a mobile client, or a virtualized client on PCs, Macs, tablets, smartphones, and virtual desktop clients.

Cisco Jabber for iPad

Cisco Jabber for iPad is a unified communications application that allows iPad users to use Cisco Jabber on the Apple iPad to access Cisco® Unified Communications Solutions. This integrated collaboration experience is designed to take advantage of the form factor of the iPad and can work with a premises- or cloud-based collaboration architecture. Jabber for iPad delivers a complete collaboration experience for mobile workers who need instant access to information and decision makers and want to choose when, where, and how they work.

Cisco Jabber helps enterprises connect employees in bring-your-own-device (BYOD) workspaces. For more information about the Cisco BYOD Smart Solution, please visit: http://www.cisco.com/web/solutions/trends/byod_smart_solution/index.html.

What You Will Learn

This deployment guide provides information and guidance to help you deploy the Cisco Jabber for iPad solution in an enterprise environment where fully functional wireless LAN (WLAN) and security infrastructure are required in both on-premises and cloud deployments. Other clients in the Cisco Jabber application family for mobile devices, such as Cisco Jabber IM for iPhone, Cisco Jabber for iPhone, and Cisco Jabber for Android, are not covered in this document.

Before you begin, as a minimum you are expected to have a good understanding of Cisco Unified Communications Manager, Cisco Unified Presence, Cisco TelePresence® Video Communication Server (Cisco VCS), and Cisco WebEx® meeting applications. It is expected that all the components and infrastructure servers are properly installed and configured before registering Cisco Jabber for iPad clients. Provisioning, configuration, and licensing are not the focus of this document. For Jabber for iPad provisioning and configurations, refer to the Cisco Jabber for iPad Administration Guide at: http://www.cisco.com/en/US/products/ps12430/prod_installation_guides_list.html.

This document is not to be used as a substitute for existing product documents; it is intended for use as a supplementary guide.

Deployment Models

Before deploying Cisco Jabber for iPad, you have several options on the back-end architecture for voice, video, IM, and presence to ensure the deployment fits the requirements. See Figure 1 for the supported back-end services with Cisco Jabber for iPad. Cisco offers a variety of back-end services for voice and video call control and IM and presence either in the cloud or on-premises, or a combination of both.
On-premises solutions include the following:

- Cisco Unified Communications Manager (Cisco UCM) for enterprise voice and video
- Cisco TelePresence Video Communication Server (Cisco VCS) for Cisco TelePresence video
- Cisco Unified Presence for IM and Presence

Cloud solutions include the following:

- Cisco WebEx Messenger (also known as WebEx Connect) service for IM and Presence, and peer-to-peer (P2P) voice and video
- Cisco Jabber Video™ for TelePresence

Figure 1. Jabber for iPad IM, Presence, Voice, and Video Calling Options

Table 1 gives system requirements for Cisco Jabber for iPad.

<table>
<thead>
<tr>
<th>Component</th>
<th>System Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple iPad¹</td>
<td>iPad 2, new iPad (iPad 3), and Apple iOS 5.1.1 or later</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>Voice: 7.1.5</td>
</tr>
<tr>
<td></td>
<td>Voice and video: 8.03, 8.5.1, 8.6.2, and 9.0</td>
</tr>
<tr>
<td>Cisco Unified Presence</td>
<td>8.0, 8.5, 8.6.2, and 9.0</td>
</tr>
<tr>
<td>Cisco TelePresence Video Communication Server</td>
<td>6.0 or later</td>
</tr>
<tr>
<td>Cisco TelePresence Management Suite (Cisco TMS)</td>
<td>13.1 or later</td>
</tr>
</tbody>
</table>

¹ The video and voice quality of calls varies depending on the Wi-Fi or mobile data network connection. Cisco does not troubleshoot voice and video quality and connectivity problems when you use Jabber for iPad on third- or fourth-generation (3G or 4G, respectively) mobile data networks or noncorporate Wi-Fi networks over a VPN connection.
Table 1: System Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>System Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco WebEx Messenger</td>
<td>7.6</td>
</tr>
<tr>
<td>Cisco Jabber Video for TelePresence</td>
<td>1.0 or later</td>
</tr>
<tr>
<td>Cisco Unity® Connection</td>
<td>8.5, 8.6, and 9.0</td>
</tr>
<tr>
<td>Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST)</td>
<td>8.6 and 9.0 (voice only)</td>
</tr>
<tr>
<td>Corporate Directory (optional)</td>
<td>Microsoft AD 2008 and OpenLDAP v3</td>
</tr>
<tr>
<td>Cisco Adaptive Security Appliance (ASA)</td>
<td>Cisco AnyConnect® 2.5 or later</td>
</tr>
<tr>
<td></td>
<td>Cisco ASA 8.4 or later</td>
</tr>
<tr>
<td></td>
<td>Cisco Adaptive Security Device Manager (ASDM) 6.4 or later</td>
</tr>
</tbody>
</table>


**Best Practices for Deployment**

You should go through the following deployment checklist to ensure a successful Cisco Jabber for iPad deployment:

- Back-end services
- Wi-Fi network connectivity and security
- Bandwidth management and quality of service (QoS)
- Bulk configuration
- Cisco Jabber for iPad client deployment
- AnyConnect® client

**Back-End Services**

Cisco Jabber for iPad enables various deployment options for on-premises and cloud back-end services for unified communications and collaborations, with flexibility to support different combinations of functions based on your requirements. The Cisco Jabber for iPad Administration Guide provides details of administration and provisioning steps for the back-end services, including the following deployment scenarios:

- Instant messaging and presence only
  - Cisco Unified Presence (on-premises)
  - Cisco WebEx Messenger service (cloud)
- Voice and video call control only
  - Cisco Unified Communications Manager (on-premises)
  - Cisco TelePresence Video Communication Server (on-premises)
  - Cisco Jabber Video for TelePresence (cloud)
- Instant messaging, presence, voice, and video
  - Cisco Unified Presence + Cisco Unified Communications Manager
  - Cisco WebEx Messenger service + Cisco Unified Communications Manager
  - Cisco WebEx Messenger service + Cisco TelePresence Video Communication Server
  - Cisco WebEx Messenger service + Cisco Jabber Video for TelePresence
- Corporate Directory
  - Microsoft Active Directory 2008
  - Open Lightweight Directory Access Protocol (OpenLDAP) Version 3
- Unified messaging
  - Cisco Unity® Connection
- VPN
  - Cisco Adaptive Security Appliance (ASA)

Figure 2 illustrates the high level architecture for on premise and cloud backend components for Jabber for iPad.

Figure 2. Jabber for iPad Architecture

Not all the services and functions are required for deploying Cisco Jabber for iPad, so during the design and deployment timeframe you should consider a combination of functions such as IM, call control, and secure remote. From a user perspective, as a minimum you need to decide to set up individual accounts or company-provided accounts for IM and voice and video call-control services for Cisco Jabber for iPad users before the deployment.

Administrators are responsible for following the Cisco Jabber for iPad Administration Guide for configuration and provisioning servers and user accounts. Cisco Unified Communications Manager Lightweight Directory Access Protocol (LDAP) synchronization with corporate directories and bulk administration tools are also available for adding and updating a large number of users. The Cisco Jabber for iPad Administration Guide contains detailed information and is available at the following link:


Wi-Fi Network Connectivity and Security

Apple iPad is a mobile device that requires wireless network connectivity by using Wi-Fi or mobile wireless data services. Although a mobile wireless network provided by mobile wireless carriers is capable of delivering IM, presence status, voice, video capabilities, and other communication capabilities to Cisco Jabber for iPad, this document focuses on important deployment concepts and expectations for Cisco Jabber for iPad in an enterprise wireless LAN (WLAN) environment.

Apple iPad Wi-Fi Specifications

Apple iPad 2 and the new iPad (iPad 3) support 2.4- and 5-GHz 802.11a/b/g/n Wi-Fi with Wi-Fi Multimedia (WMM) capability. Details about WLAN data rates, modulation schemes, RF characteristics, antenna, and other specifications are available at the Apple website and at the Federal Communications Commission (FCC) website.

Site Survey

A site survey is strongly recommended before you deploy Cisco Jabber for iPad in a production environment, as shown in Figure 3. Because Cisco Jabber for iPad requires a low end-to-end latency and packet-loss rate to prevent delay in real-time communications, you must have a well-designed and -planned wireless network. During the site survey, you must analyze and validate RF spectrum, coverage, data rates, capacity, signal levels, noise, roaming, interference, and locations of access points to ensure a high-quality WLAN for real-time communications.

Figure 3. Wi-Fi Site Survey Heap Map
You can use the following tools and applications to verify coverage, quality, and configuration:


WLAN Considerations for Cisco Jabber for iPad Deployment

You have many wireless standards and technologies options; the intent of this document is not to provide a comparison of each option but to provide a list of recommendations and considerations for a successful deployment of Cisco Jabber for iPad for real-time communications.

After a site-survey analysis, administrators should have a clear view of how their WLAN is implemented. It is essential for administrators to improve and correct any existing deficiency, including identifying and eliminating sources of interference in the WLAN, before deploying Cisco Jabber for iPad. Implementation involves making decisions about the following parameters:

- **Band selection**: The 2.4-GHz frequency band used by 802.11b, 802.11g, and 802.11n is shared with other unlicensed devices, including Bluetooth devices, cordless phones, etc., and these devices generally increase noises and interference and result in air-time congestion. On the other hand, the 5-GHz band is less crowded compared to the 2.4-GHz band. IEEE 802.11n on 5 GHz, which also operates on the 2.4-GHz band, is recommended; it provides a faster speed and data rate with the latest wireless technologies.

- **Overlapping channel**: Whether you use the 2.4- or 5-GHz band, the band is divided into channels, similar to the way radio and TV broadcast bands are divided. For example, the 2.4-GHz band is divided into 13 channels (Japan has a 14th channel for 802.11g only), each 5 MHz apart, as shown in Figure 4.

![Figure 4. Channel Frequencies in 2.4 GHz Band](image-url)
Overlapping channels causes unacceptable and degraded signal quality and throughput, and users could have a bad overall experience when using real-time communication applications such as Jabber for iPad. Therefore, it is essential that you allocate nonoverlapping channels when designing a WLAN network. In the United States, the channels 1, 6, and 11 are the only nonoverlapping channels available when 802.11b/g used. In 802.11a and 802.11n at 5 GHz, on the other hand, there is a larger range of band frequency and more nonoverlapping channels to allocate. We recommend at least one channel of separation for adjacent access points in the 5-GHz band.

In 802.11n, two adjacent 20-MHz channels can be bounded into a 40-MHz channel, doubling the amount of available bandwidth and increased throughput. In the 2.4-GHz frequency band, only one bounded channel is available, either channels 1 and 6 or 6 and 11. Because only three nonoverlapping channels in the 2.4-GHz band are available, channel bonding in the 2.4-GHz band is not recommended. However, because there are more nonoverlapping channels in the 5-GHz frequency band, you can consider channel bonding configuration and design in the 5-GHz band. Table 2 shows the 802.11 channels and center frequencies in 5-GHz band.

Table 2. 802.11 Channels and Center Frequencies in 5-GHz Unlicensed National Information Infrastructure (UNII) Spectrum

<table>
<thead>
<tr>
<th>Spectrum</th>
<th>UNII-1</th>
<th>UNII-2</th>
<th>UNII-2 Extended</th>
<th>UNII-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11 channel</td>
<td>36</td>
<td>40</td>
<td>44</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>52</td>
<td>56</td>
<td>60</td>
<td>64</td>
</tr>
<tr>
<td></td>
<td>100</td>
<td>104</td>
<td>108</td>
<td>112</td>
</tr>
<tr>
<td></td>
<td>116</td>
<td>132</td>
<td>136</td>
<td>140</td>
</tr>
<tr>
<td></td>
<td>149</td>
<td>153</td>
<td>157</td>
<td>161</td>
</tr>
<tr>
<td></td>
<td>165</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Center frequency</td>
<td>5180</td>
<td>5200</td>
<td>5220</td>
<td>5240</td>
</tr>
<tr>
<td></td>
<td>5260</td>
<td>5280</td>
<td>5300</td>
<td>5320</td>
</tr>
<tr>
<td></td>
<td>5500</td>
<td>5520</td>
<td>5540</td>
<td>5560</td>
</tr>
<tr>
<td></td>
<td>5580</td>
<td>5600</td>
<td>5660</td>
<td>5680</td>
</tr>
<tr>
<td></td>
<td>5700</td>
<td>5745</td>
<td>5765</td>
<td>5785</td>
</tr>
<tr>
<td></td>
<td>5805</td>
<td>5825</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Coverage area:** The coverage area typically includes office area, conference rooms, cafeterias, etc.
  Capacity, data rate, and transmit power configurations affect the coverage-area design. In general, faster data rates translate to smaller cells, meaning an access point that operates in 5-GHz frequency covers less footage than an access point in 2.4-GHz frequency. Similar to data rates, if the transmit power settings in an access point are higher, the coverage area of a cell is larger.
  The general rule for supporting real-time communications is smaller cells and more cells in a coverage area. Figure 5 shows a comparison of larger and less cells vs. smaller and more cells in a coverage area.
  However, the numbers of access points that are deployed in a coverage area depend on the numbers of wireless devices in the area, how those devices are used, and other factors such as budgets (more access points cost more money) and lobbies and conference rooms (a lobby may need less coverage, whereas a conference room may need more, etc.).
Figure 5. Lesser Access Points with Larger Coverage Area vs. More Access Points with Smaller Coverage Area (Recommended)

- **Channel cell capacity and density:** The coverage area of an antenna is the collision domain of the access point. Cisco Jabber for iPad delivers real-time voice and video. It supports up to 448p at 30 fps, and the suggested bandwidth allocation per call is 768 kbps end-to-end, which includes the transmission over the air from and to the iPad. Therefore, it is important to check the specifications of your access points and wireless infrastructure to carefully calculate the number of calls an access point can support. Pay special attention to the high-density area where Cisco Jabber for iPad will be used, such as conference rooms, to avoid bandwidth exhaustion.

Because there are more channels in the 5-GHz frequency band, using co-location of access points on nonoverlapping channels increases per-channel cell capacity on a floor. Figure 6 shows a deployment option by using nonoverlap channels in the 5-GHz band. However, if a dense deployment with many devices in a small area is required, we recommend that you increase the numbers of access points with a smaller coverage by each access point.

These voice and video call-capacity values are highly dependent upon the RF environment, the configured or supported video resolution and bit rates, and the underlying WLAN system features. Actual capacities for a particular deployment could be less. Coverage area, channel cell capacity, and density are the main factors for a successful WLAN deployment.

Figure 6. Use Nonoverlap Channels in 5 GHz to Increase Call Capacity
When deploying wireless devices within the enterprise WLAN, it is important to consider the call capacity of the WLAN infrastructure. Oversubscription of the enterprise WLAN infrastructure in terms of number of devices or number of active calls results in dropped wireless connections, poor voice and video quality, and delayed or failed call setup. The chances of oversubscribing a deployment of voice and video over WLAN (VVoWLAN) are greatly minimized by deploying sufficient numbers of access points to handle required call capacities. Access-point call capacities are based on the number of simultaneous voice and video bidirectional streams that can be supported in a single channel cell area. When deploying Cisco Jabber for iPad, the following WLAN call capacities apply:

- Maximum of 27 simultaneous voice-over-WLAN (VoWLAN) bidirectional streams per 802.11g/n (2.4 GHz) with Bluetooth disabled or 802.11 a/n (5 GHz) channel cell and 24 Mbps or higher data rates.
- Assuming a video resolution of 448p and a video bit rate of up to 1 Mbps, a maximum of eight simultaneous VVoWLAN bidirectional streams per 802.11 g/n (2.4 GHz) with Bluetooth disabled or 802.11 a/n (5 GHz) channel cell.
- WLAN QoS support: Wi-Fi Multimedia (WMM), also known as Wireless Multimedia Extensions (WME), is a subset of the 2005 IEEE 802.11e specification, which provides basic QoS and a power-saving mechanism to the IEEE 802.11 network. WMM prioritizes traffic in four categories: voice, video, best effort, and background. Applications such as Jabber for iPad can request QoS level support over Wi-Fi. Without QoS, all applications running on different devices have equal opportunity to transmit data, and it may result a slow transmission for voice and video data.

WMM provides differentiated services by tagging the Layer 3 and Layer 2 protocol layer bit fields, and gives real-time communication applications a priority preference over other traffic. You should configure WMM policy in the wireless infrastructure wherever possible.

- Roaming: The iPad is a mobile device that allows you to move around without losing connectivity by roaming from one access point to another. Roaming is the process of a client moving an established Wi-Fi network association among access points within the same Service Set Identification (SSID), as shown in Figure 7. Without a well-planned and well-designed wireless network, roaming can cause dropped calls or long delays for mobile users.

**Figure 7.** Layer 2 and Layer 3 Roaming
The goal of roaming for any wireless client is to minimize the time required to transition between access points to avoid disruptions of the client applications. Fast roaming and session caching mechanisms can be used to eliminate some of the unnecessary authentication steps. However, the algorithm to decide when to roam and how to roam is implemented by the clients. Because Apple iPad does not support Cisco Compatible Extensions or the IEEE 802.11r specification for fast secure roaming, users may experience delay during the process of roaming.

Opportunistic Key Caching (OKC), also known as Proactive Key Caching, is also used to minimize latency and overhead in the authentication process during a roaming process. iPad does not support OKC; however, it supports Pairwise Master Key ID (PMKID) or “sticky key caching” for roaming, meaning the client remembers or “sticks” the PMKID with its initial associated and authenticated access point or Basic Service Set Identification (BSSID), not to another access point. Therefore, during the roaming process, the client may disconnect until it completes the authentication process again with a new PMKID. If you are in a call using Jabber for iPad, your call may be disrupted by a long delay or may even be disconnected during roaming.

In addition, calls may be dropped or experience long delays during roaming in the following scenarios:

- When an IP address assigned to your iPad changes
- When you roam from one WLAN to another
- When you roam within a WLAN that does not broadcast SSID
- **Bluetooth**: Bluetooth is a wireless standard for short-range communications that operates in the 2.4-GHz Industrial, Scientific, and Medical (ISM) band. Jabber for iPad users can use the built-in Bluetooth technologies in iPad with Bluetooth headsets for voice communications during audio or video calls. Apple iPad2 supports Bluetooth 2.1 + Enhanced Data Rate (EDR), and the new iPad supports Bluetooth 4.0 technology. Users are responsible to ensure the Bluetooth devices are compatible with iPad and the association (pairing) is properly established before placing or receiving calls with Jabber for iPad. Because both Bluetooth and 802.11 b/g/n devices operate in the 2.4-GHz frequency ISM band, it is important to understand that users may experience interference from Bluetooth devices using the same spectrum, meaning uninterrupted communications cannot be guaranteed, and there may be voice or video gaps during multimedia conversations. We recommend that you deploy WLAN in the 5-GHz frequency band to avoid inference from Bluetooth and other devices using the 2.4-GHz band.
- **Wi-Fi security and authentication**: Apple iPad supports a variety of wireless security features, including 802.1X authentication for end-user and device authentication and Wi-Fi Protected Access (WPA) with Advanced Encryption Standard (AES) for data encryption. Other security and authentication features for iPad include:
  - Wired Equivalent Privacy (WEP)
  - WPA Personal and Enterprise
  - WPA2 Personal and Enterprise
  - EAP- Transport Layer Security (EAP-TLS)
  - EAP with Tunneled TLS (EAP-TTLS)
  - EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)
  - EAP- Subscriber Identity Module (EAP-SIM)
  - Protected Extensible Authentication Protocol Version 0 (PEAPv0) (EAP- Microsoft Challenge Handshake Authentication Protocol Version 2 [EAP-MS-CHAPv2])
- PEAPv1 (EAP-Generic Token Card [GTC])
- Lightweight Extensible Authentication Protocol (LEAP)

**Note:** WEP, which has publicly known security and encryption weaknesses, is not a recommended method for wireless security and authentication.

- **Wi-Fi deployment recommendations:** Wi-Fi technologies; band selections; data-rate settings; overlapping channel interference; non-Wi-Fi interference; amount of voice, video, and data transmission; Call Admission Control (CAC) and QoS configuration; locations of access points; roaming between access points; and wireless security, etc. - all of these factors affect the quality of the wireless network. Administrators have to understand the pros and cons of each factor that may affect WLAN and set the expectations of the user experience when real-time communications on Jabber for iPad are in place. Table 3 lists the recommended settings in Wi-Fi deployment.

**Table 3. Recommended Wi-Fi Deployment Settings**

<table>
<thead>
<tr>
<th>Factor</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data rate</td>
<td>Data rate lower than 11 Mbps should be disabled</td>
</tr>
<tr>
<td>RF bands</td>
<td>5 GHz</td>
</tr>
<tr>
<td>Signal level</td>
<td>-67 dBm with 20-30% overlap of the cell edge on nonadjacent channels</td>
</tr>
<tr>
<td>Channel usage</td>
<td>&lt; 50%</td>
</tr>
<tr>
<td>Noise</td>
<td>&lt;-92 dBm</td>
</tr>
<tr>
<td>Packet loss</td>
<td>&lt; 1%</td>
</tr>
<tr>
<td>Jitter</td>
<td>&lt; 100 ms</td>
</tr>
<tr>
<td>Retries</td>
<td>&lt; 20%</td>
</tr>
</tbody>
</table>

**Bandwidth Management and QoS**

When deploying Cisco Jabber for iPad, it is important that the network infrastructure support necessary QoS classes of service, including priority queuing for voice media and dedicated video and signaling bandwidth, to ensure the quality of Cisco Jabber voice and video calls. Table 4 give a generic guideline for recommended bandwidth requirements for audio and video calls. It is critical to minimize the end-to-end latency to avoid delay, packet loss, and jitter for real-time communications.

**Table 4. Recommended Bandwidth Guidelines for Audio and Video Calls**

<table>
<thead>
<tr>
<th>Upload Speed</th>
<th>Audio</th>
<th>Audio + Interactive Video (Main Video)</th>
</tr>
</thead>
</table>
| 125 kbps     | • At bandwidth threshold for G.711  
                   • Sufficient bandwidth for G.722.1 | Insufficient bandwidth for video |
| 384 kbps     | • Sufficient bandwidth for any audio codec | w288p (512x288) at 30 fps |
| 1000 kbps    | • Sufficient bandwidth for any audio codec | 448p (576x448) at 30 fps |

Cisco Jabber for iPad supports G.711 and G.722 for audio and H.264 for video, and for video calls, up to 448p at 30 fps. We recommend that the minimum bandwidth allocated per call should be >768 kbps.

Cisco Jabber for iPad uses video rate adaptation to negotiate optimal video quality based on your network conditions. Video rate adaptation dynamically scales video quality when video transmission begins.
Cisco Jabber for iPad automatically adapts video to suit available bandwidth. When users make video calls, the application rapidly and incrementally increases bit rate and resolution to achieve the optional settings. Users should expect video calls to begin at lower resolution and scale upward to higher resolution over a short period of time. The application saves history so that subsequent video calls should begin at the optimal resolution. However, users can expect some fluctuation and scaling of video transmissions until the optimal resolution is achieved.

In addition, the bandwidth-specific configurations for regions, locations, and CAC need to be provisioned correctly for Cisco Unified Communications Manager. Similarly, administrators need to properly configure bandwidth control, subzones, and links and pipes in Cisco TelePresence Video Communication Server to ensure sufficient bandwidth for codec, audio, and video calls.

Please refer to the following documents for details:


Configuration for Large Numbers of Users

**Cisco WebEx Messenger Service**

You can import a large number of users into Cisco WebEx Messenger by using a comma-separated values (CSV) file. To find the instructions and examples of how to use the CSV files for user bulk configuration for WebEx Messenger, please visit:


**Cisco Unified Communications Manager**

We recommend that you synchronize Cisco Unified Communications Manager with a corporate LDAP server to provision a large number of users. Alternatively, the Cisco UCM Bulk Administration Tool (BAT) is a web-based application that performs bulk transactions for devices to Cisco UCM. BAT allows administrators to add, update, or delete a large number of similar phones, users, profiles, or ports at the same time. Administrators can use BAT to add Jabber users by importing a text-based CSV data file or BAT spreadsheet.


**Cisco VCS and Cisco TMS**

Cisco TelePresence Management Server (Cisco TMS) Provisioning allows videoconferencing network administrators to create and manage mass-deployable videoconferencing solutions. It uses the Cisco TMS Agent to replicate and distribute the Cisco TMS Provisioning User Directory and Provisioning information from Cisco TMS through a single or clustered Cisco VCSs to endpoint devices such as Cisco Jabber Video for TelePresence and Cisco TelePresence System EX90. To support Jabber for iPad, the Jabber for iPad template needs to be installed and the users assigned. Administrators can download the provisioning template at: [http://download.cisco.com/swc/esd/06/284288351/contract/jabbertablet_provisioning_template.xml](http://download.cisco.com/swc/esd/06/284288351/contract/jabbertablet_provisioning_template.xml).
For Cisco TMS Version 13.2 and earlier, Cisco TMS Agent Legacy is recommended for planning and implementing a simplified provisioning deployment. For Cisco TMS Version 13.2 and later, network administrators can use Cisco TMS Provisioning Extension (TMSPE) to import or synchronize a group of user accounts from an external source; for instance, Active Directory or LDAP sources. We recommend that users running Cisco TMS Agent Legacy migrate to the Cisco TMSPE.

More information about TMSPE is available at:  

More information about Cisco TMS Agent Legacy is available at:  

Jabber for iPad Client Deployment

Jabber for iPad is a free application that you can download and install on Apple iPad through the Apple App Store or Apple iTunes. Many utilities or mobile device management (MDM) applications provided by Apple and third-party vendors are available for deploying, configuring, and managing apps on the Apple iPad. Cisco is not responsible for troubleshooting and debugging these tools and utilities.

At a minimum, administrators need to provide instructions for downloading and installing Jabber for iPad clients and credentials for signing in to the back-end service of choice. The instructions can be distributed through different formats, such as email or web.

After launching the Jabber for iPad application for the first time, you need to choose to sign in by using the Individual Accounts or Company-Provided Accounts. The difference between an individual account and a company-provided account is that you can sign in by using a personal WebEx Messenger or Cisco Jabber Video for TelePresence account for Individual Accounts, rather than business accounts.
Individual Accounts
If you select Individual Accounts, Cisco WebEx Messenger or Cisco Jabber Video for TelePresence account information is required. We recommend that you use a WebEx Messenger account for IM and presence, and Jabber Video for TelePresence for voice and video calling, as shown in Figure 8.

Figure 8. Individual Account Settings for Jabber for iPad

![Individual Account Settings for Jabber for iPad](image)

Table 5 provides a sample checklist of Individual Account Settings for Jabber for iPad.

Table 5. Configuring Individual Account Settings for Jabber for iPad

<table>
<thead>
<tr>
<th>Individual Account</th>
<th>Instructions to Download Cisco Jabber for iPad</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use either WebEx Messenger or Jabber Video for TelePresence account</td>
<td>Jabber Video for TelePresence, Username and password</td>
</tr>
<tr>
<td>Optional</td>
<td>Instructions to use Jabber Problem Report tool, Instructions to set up Wi-Fi connectivity, Instructions to download and use Cisco AnyConnect for iPad, Instructions to use SSL and LDAP User Authentication, Instructions to use Visual Voicemail, Instructions to download and use Cisco WebEx Meetings</td>
</tr>
</tbody>
</table>

Company-Provided Accounts
Similar to setting up Individual Accounts, we recommend that you set up an IM and Presence account first before a Video and Voice Calling account, unless no IM and Presence account is available. If you select a Cisco Unified Presence account, then Cisco UCM is your only valid option for video and voice calling. On the other hand, if a Cisco WebEx Messenger account is configured, then you can select one of three options, including Cisco UCM, Cisco VCS, and Cisco Jabber Video for TelePresence, for video and voice calling. See Figure 9 for Company-Provided Account Settings.
During a deployment, administrators should provide an instruction to end-users on what features are available and how to configure Jabber for iPad. Table 6 shows a sample instruction on what administrators should provide to end-users for configuring Company-Provided Account settings for Jabber for iPad.

Table 6. Configuring Company-Provided Account Settings for Jabber for iPad

<table>
<thead>
<tr>
<th>Company-Provided Account</th>
<th>Instructions to Download Cisco Jabber for iPad</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM</td>
<td>Choose either of the following:</td>
</tr>
<tr>
<td></td>
<td>• WebEx Messenger</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Presence</td>
</tr>
<tr>
<td></td>
<td>WebEx Messenger</td>
</tr>
<tr>
<td></td>
<td>• WebEx Messenger username and password</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified Presence</td>
</tr>
<tr>
<td></td>
<td>• Username</td>
</tr>
<tr>
<td></td>
<td>• Password</td>
</tr>
<tr>
<td></td>
<td>• Server address</td>
</tr>
<tr>
<td>Voice and video calling</td>
<td>Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Cisco UCM</td>
</tr>
<tr>
<td></td>
<td>• Cisco VCS</td>
</tr>
<tr>
<td></td>
<td>• Cisco Jabber Video for TelePresence</td>
</tr>
<tr>
<td></td>
<td>Note:</td>
</tr>
<tr>
<td></td>
<td>• If you use only video and voice calling, you must select either Cisco UCM or Cisco VCS.</td>
</tr>
<tr>
<td></td>
<td>• If you select Cisco Unified Presence for IM and presence, Cisco UCM is the only option for video and voice calling.</td>
</tr>
<tr>
<td></td>
<td>Cisco UCM</td>
</tr>
<tr>
<td></td>
<td>• Username</td>
</tr>
<tr>
<td></td>
<td>• Password</td>
</tr>
<tr>
<td></td>
<td>• Trivial File Transfer Protocol (TFTP) server address</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager IP phone server address (optional)</td>
</tr>
<tr>
<td></td>
<td>Cisco VCS</td>
</tr>
<tr>
<td></td>
<td>• Username</td>
</tr>
<tr>
<td></td>
<td>• Password</td>
</tr>
<tr>
<td></td>
<td>• Internal server address</td>
</tr>
<tr>
<td></td>
<td>• External server address</td>
</tr>
<tr>
<td></td>
<td>• SIP domain address</td>
</tr>
<tr>
<td></td>
<td>Jabber Video for TelePresence</td>
</tr>
<tr>
<td></td>
<td>• Username and password</td>
</tr>
<tr>
<td>Company-Provided Account</td>
<td>Instructions to Download Cisco Jabber for iPad</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Optional</td>
<td>Instructions to use Jabber Problem Report tool</td>
</tr>
<tr>
<td></td>
<td>Instructions to set up Wi-Fi connectivity</td>
</tr>
<tr>
<td></td>
<td>Instructions to download and use Cisco AnyConnect for iPad</td>
</tr>
<tr>
<td></td>
<td>Instructions to use Secure Sockets Layer (SSL) and LDAP User Authentication</td>
</tr>
<tr>
<td></td>
<td>Instructions to use Visual Voicemail</td>
</tr>
<tr>
<td></td>
<td>Instructions to download and use Cisco WebEx Meetings</td>
</tr>
</tbody>
</table>

**Note:** If you sign in to your Cisco VCS accounts first, you cannot set up WebEx Messenger later in the application.

**Security Considerations**

**AnyConnect VPN**

The Cisco Jabber for iPad application requires Cisco Unified Communications back-end services either in the cloud or on-premises. If one or all back-end services are deployed on-premises, then an established secure VPN connection is required for the Cisco Jabber for iPad clients that are outside of corporate network to communicate with those back-end services behind a firewall over public Wi-Fi or mobile wireless networks. We strongly recommend that you deploy Cisco AnyConnect Secure Mobility Client alongside Cisco Jabber for iPad².

Cisco AnyConnect client on iPad provides a full VPN tunnel for Cisco Jabber and other applications that need secure access to the enterprise network from outside the corporate firewall. AnyConnect is a VPN client that provides secure connect features, including:

- VPN on-demand³, which is available for iOS and allows the AnyConnect tunnel to be established whenever a particular destination is contacted (that is, Cisco UCM).
- Split Include, which allows you to configure specific traffic to be sent through the encrypted tunnel; for example, using Split Include, Cisco UCM voice traffic could be sent through the encrypted tunnel, and Safari browser data would not.
- AnyConnect also has a built-in diagnostics and reporting tool and statistics reporting to help troubleshoot VPN problems.

The following services do not require AnyConnect VPN for remote access:

- Cisco Jabber Video for TelePresence Service.
- Cisco WebEx Messenger Service.
- Cisco WebEx Meetings.
- Cisco TelePresence Video Communication Server (TelePresence VCS Expressway is required).

---

² Cisco is not responsible for debugging or troubleshooting Cisco Jabber for iPad problems related to VPN connectivity provided by other vendors.

³ Although there is a known problem with the On-Demand AnyConnect feature working with the Jabber for iPad 1.0 release, which will be fixed in a future maintenance release, you can use this feature for other applications running on iPad; for instance, browsing your company website behind the firewall.
Administrators should also consider the following configurations for a more integrated user experience with Jabber for iPad and AnyConnect:

- Enable Certificate Authentication, so end users do not need to enter VPN credentials manually.
- Properly configure split tunneling, to ensure only the traffic destined for Cisco UCM goes into the encrypted tunnel.

If you plan to support Cisco Jabber on iPad with on-premises services such as Cisco UCM and Cisco Unified Presence for remote users who are not in the enterprise network, Cisco AnyConnect is recommended to provide secure remote access from the iPad directly to enterprise networks. You can download and install Cisco AnyConnect client for Apple iOS from the Apple App Store. Cisco Adaptive Security Appliance (ASA) is the secure gateway that admits access to the AnyConnect client.

Additional information is available at:


### Port Configuration

Table 7 lists ports and protocols used in Cisco Jabber for iPad. The duration for each entry is “ephemeral”.

<table>
<thead>
<tr>
<th>Component</th>
<th>Protocol</th>
<th>Network Protocol</th>
<th>Port</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCM registration</td>
<td>• User Datagram Protocol (UDP) with TCP</td>
<td>• UDP and TCP</td>
<td>5060</td>
<td>• Session Initiation Protocol (SIP) port for Cisco UCM registration</td>
</tr>
<tr>
<td></td>
<td>• TCP</td>
<td>• TCP</td>
<td>5061</td>
<td>• Secure SIP</td>
</tr>
<tr>
<td></td>
<td>• TFTP</td>
<td>• UDP</td>
<td>69</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CCMCIP</td>
<td>• TCP</td>
<td>8443</td>
<td></td>
</tr>
<tr>
<td>Internet calling</td>
<td>• Extensible Messaging and Presence Protocol (XMPP)</td>
<td>• XMPP</td>
<td>5269</td>
<td>• Federation</td>
</tr>
<tr>
<td>IM</td>
<td>• Real-Time Transport Protocol (RTP)</td>
<td>• UDP</td>
<td>16384-32766</td>
<td>• Range specified by Cisco UCM in device configuration file</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Default values</td>
</tr>
<tr>
<td>Directory</td>
<td>• LDAP</td>
<td>• TCP</td>
<td>389</td>
<td>• LDAP with optional TLS</td>
</tr>
<tr>
<td></td>
<td>• Secure LDAP</td>
<td></td>
<td>636</td>
<td>• LDAPS</td>
</tr>
</tbody>
</table>
Component | Protocol | Network Protocol | Port | Notes
--- | --- | --- | --- | ---
Cisco Unity Connection Voicemail | Internet Message Access Protocol (IMAP) | TCP | 143 | IMAP with SSL and TLS
| | | | 993 and 7993 | |
Audio/video server (Cisco WebEx Messenger service) | TCP | TCP | 80 | Used if a direct connection is not possible because of firewall
| | SSL | 443 | |
| | UDP | 5101 | |
Peer-to-peer (Cisco WebEx Messenger service) | TCP | TCP with UDP | 1024-65525 | Range specified in OrgAdmin > Configuration tab > P2P Port Settings
| | | | |

**Appendix A: Cisco Unified Communications Manager Bulk Provisioning**

This section provides step-by-step instructions for using the Cisco Bulk Administration Tool available on the Cisco Unified Communications Manager Administration page to insert several phones and users from a BAT file. Before starting the following steps, make sure you log in to the Cisco Unified Communications Manager Administration page successfully. Then navigate to "Bulk Administration".

**Note:** If there are existing BAT scripts, you may skip steps 1 and 2 because you do not need to create a new BAT script.

Instructions for inserting several new phones and new users:

**Step 1.** Download File Format.

1.1 Go to Bulk Administration -> Upload/Download Files.

1.2 Select the bat.xlt file and then download it to your computer.

**Step 2.** Open File Format.

2.1 Open the bat.xlt file that was downloaded from step 1.

2.2 Go to the Phone-Users sheet. Make sure you enable Macros in the spreadsheet before doing the next step.

2.3 Click the Create File Format button (macros must be enabled).

2.4 The Field Section window appears.

2.5 Choose or select Owner User ID under Device Fields and then press the >> button to assign it into Selected Device Fields.

2.6 Choose or select Directory Number under Line Fields and then press the >> button to assign it into Selected Line Fields.

2.7 Click the Create button to generate a new format with selected fields.

2.8 Check that the names in row 1 are updated in the Phones-Users field accordingly.

2.9 Enter data for all mandatory fields: Last Name, User ID and MAC Address/Device Name, and other optional fields such as Password, PIN, Description, Owner User ID, and Directory Number 1.

2.10 Click the Export to BAT Format button in column AD (make sure macros are enabled).

2.11 Save a new bat file (.txt) to your local computer drive.
Step 3. Upload the created BAT file.

3.1 Go to Bulk Administration -> Upload/Download Files.
3.2 Click Add New, and then Select a new BAT file (.txt) that was saved from step 2.
3.3 Select the target with Phones/users and select the transaction type with Insert phones/users.
3.4 Click Save.


4.1 Go to Bulk Administration -> Users -> User Template.
4.2 Click Add New.
4.3 Enter the user template name.
4.4 The rest of fields are optional.
4.5 Click Save.

**Note:** The same user template can be used by multiple phone types. You may need to create only one user template to be used for multiple phone templates.

Step 5. Create Phone Template.

5.1 Go to Bulk Administration -> Phones -> Phone Template.
5.2 Click Add New.
5.3 Select Phone Type Cisco Jabber for Tablet.
5.4 Click Next.
5.5 Fill in the mandatory and optional information on the Phone Template page.
5.6 Click Save.
5.7 Click Line [1] - Add a new DN on the Phone Template Configuration page.
5.8 Enter Line Template Name on the Line Template Configuration page.
5.9 Click Save.

Step 6. Insert Phones and Users.

6.1 Go to Bulk Administration -> Phones & Users -> Insert Phones with Users.
6.2 For File Name, select a file from the drop-down menu.
6.3 For Phone Template Name, select a phone template from the drop-down menu.
6.4 For User Template Name, select a user template from the drop-down menu.
6.5 Click a radio button next to “Run Immediately” if you would like to run the BAT file right away.
6.6 Click Submit.

Step 7. Verify and Troubleshoot.

7.1 Go to Bulk Administration -> Job Scheduler.
7.2 Monitor the status of the job id.
7.3 If Job Result Status is Error, click the log file name to review the error. This message should indicate where the failure could be.
7.4 If Job Result Status is Success or Complete, verify that new phones are shown on the Phone page, and new users are shown on the End User page.
An example of a BAT file follows:

FIRST NAME,LAST NAME,USER ID,PASSWORD,MANAGER USER ID,DEPARTMENT,PIN,DEFAULT PROFILE,USER LOCALE,TELEPHONE NUMBER,PRIMARY EXTENSION,ASSOCIATED PC,IPCC EXTENSION,MAIL ID,PRESENCE GROUP,SUBSCRIBE CALLING SEARCH SPACE,DIGEST CREDENTIALS,REMOTE DESTINATION LIMIT,MAXIMUM WAIT TIME FOR DESK PICKUP,PRIMARY USER DEVICE,ENABLE EMCC,ENABLE MOBILITY,ALLOW CONTROL OF DEVICE FROM CTI,NAME DIALING,DEVICE NAME,DESCRIPTION,OWNER USER ID,DIRECTORY NUMBER 1
test1,test1,test1,cisco,,,12345,,,,,,,,,,,4,10000,......,TABIPADTEST1,,test1,60001
test2,test2,test2,cisco,,,12345,,,,,,,,,,,,,,,,,,TABIPADTEST2,,test2,60002

Appendix B: Installing Cisco TMS Provisioning Template


Step 2. In Cisco TMS, go to Systems > Provisioning > Users.

Step 3. On the Users page, click the Configuration Templates container.

Folders are displayed representing models and versions of devices for which template schemas have already been uploaded.

Step 4. In the Configuration Templates container, click Add schema.

The Upload Template Schema dialog box will open.

Step 5. Click the Browse button, navigate to the folder on your local server to where you downloaded the schema, select it, and then click OK.

Appendix C: Jabber for iPad Problem Report

The Jabber for iPad Problem Report, which generates detailed configuration and logging information, is helpful for debugging and troubleshooting problems. After you generate the report, you can mail it directly to system administrators or copy it to a computer that is connected to the iPad with a USB cable for further analysis.

Step 1. In the Jabber app, tap on Settings.

Step 2. Tap on Help. Make sure Detailed Logging for Video is ON.

Note: Tap on FAQs to open Cisco Jabber for iPad End-User Guides.
Step 3. Reproduce the problem.


A Problem Report creates an email message with logs attached. The description of the problem is important for troubleshooting. Create screen captures and attach them to the email message. (To create a screen capture, press and hold the Home button and quickly depress the On/Off button.) In the empty To field of the email message, enter the email address of the IT administrator or technical support representative.

You can copy a log file directly from the iPad, if the Send Problem Report function is not available; for example, if the client cannot restart after a crash.

- Download iPhone Explorer from the App Store.
- Start iPhone Explorer and connect the iPad through a USB cable.
- Open a file folder under your iPad as shown in the following screenshot.
- Copy log files to the OS file systems using drag-and-drop.
Log files are in zip format. There are three kinds of logs: xxx-console.log, xxx.log, and .wbt. The most important log is the xxx-console.log, which is a superset of all the logs including the .wbt. You can view the xxx-console.log using Wordpad on Windows or using a browser on a Mac. The .wbt file shows network activity, whereas the console log shows both client and network activity.

Note: To open a .wbt file, you need a WBX tracer tool, which you can download at: http://support.webex.com/support/downloads.html.