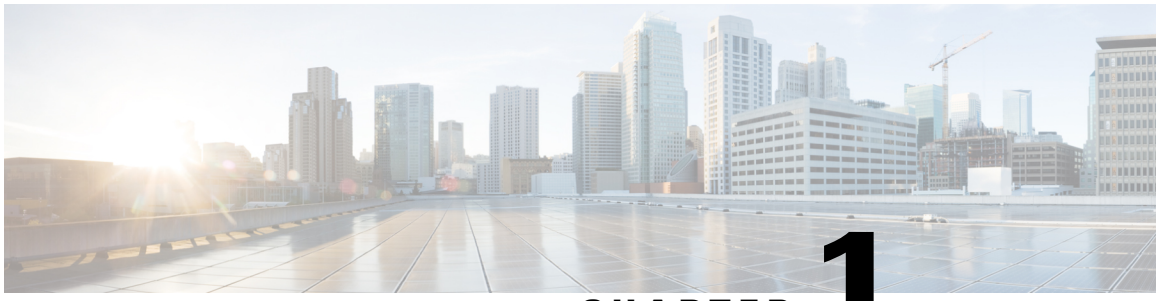
Cisco Jabber for iPad 9.3 Administration Guide

First Published: April 23, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Before you begin

Review these topics before starting the configuration of Cisco Jabber for iPad.

What is Cisco Jabber for iPad?

Cisco Jabber for iPad is a Unified Communications application that provides instant messaging (IM), video and voice calling, corporate directory search, availability, and voicemail. The underlying technologies include

- Cisco WebEx Messenger
- Cisco Unified Presence
- Cisco Unified Communications Manager
- Cisco TelePresence Video Communication Server
- Cisco Jabber Video for TelePresence (formerly known as the free Jabber Video service)
- Cisco WebEx TelePresence (formerly known as the paid Jabber Video service)

Note The video and voice quality of calls varies depending on the Wi-Fi or mobile data network connection. Cisco does not troubleshoot connectivity issues when users of Jabber for iPad are on 3G or 4G mobile data networks or non-corporate Wi-Fi networks over a VPN connection using applications such as Cisco AnyConnect Secure Mobility Client.

Note Use the **Jabber Video for TelePresence** log in for both the Cisco Jabber Video for TelePresence and Cisco WebEx TelePresence services.

How to Use this Document

This document is designed to help you set up the organization-specific technologies so they function properly on the user devices. Review this table to quickly navigate to the content that pertains to your needs.

If you want to set up…	Go to this chapter…
Domain Name Server Service Records	Set up Simple Sign-In using DNS SRV, on page 7
Cisco WebEx Messenger only	Set up for Cisco WebEx Messenger, on page 15
Cisco Unified Presence only	Set up for Cisco Unified Presence, on page 17
Cisco Unified Communications Manager only	Set up for Cisco Unified Communications Manager, on page 33
Cisco TelePresence Video Communication Server only	Set up for Cisco TelePresence Video Communication Server, on page 51
Cisco WebEx Messenger and Cisco Unified Communications Manager	Setup for Cisco WebEx Messenger and Cisco Unified Communications Manager
Cisco WebEx Messenger and Cisco TelePresence Video Communication Server	Setup for Cisco WebEx Messenger and Cisco TelePresence Video Communication Server
Cisco Unified Presence and Cisco Unified Communications Manager	Setup for Cisco Unified Presence and Cisco Unified Communications Manager

Note Domain Name Server Server Record (DNS SRV) setup should be the first step in the configuration of any Cisco Jabber for iPad deployment.

Note Cisco Jabber Video for TelePresence and Cisco WebEx TelePresence do not require any administrative setup. If your users have questions about it, direct them to the following support sites:.

- https://www.ciscojabbervideo.com/support
- http://telepresence.webex.com

Download and Installation of Cisco Jabber for iPad

Cisco Jabber for iPad is an application that you can download and install from the App Store within iTunes or on your iPad device.

Connect on Demand VPN

Cisco Jabber for iPad contains the Connect on Demand VPN feature. The Connect on Demand VPN feature enables the Cisco Jabber for iPad application to automatically establish VPN connections when needed without additional actions by end users. The Connect on Demand VPN feature requires a user to download and install the Cisco AnyConnect Secure Mobility Client from the App Store.

Cisco AnyConnect Secure Mobility Client must be configured with certificate authentication to provide the Connect on Demand VPN feature to Cisco Jabber for iPad. See the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for information and procedures for this configuration. The latest version of the *Cisco AnyConnect Secure Mobility Client Administrator Guide* is available at the following location: http://www.cisco.com/en/US/products/ps10884/products_installation_and_configuration_guides_list.html.

Additional Cisco Unified Communications Manager configuration may be required in certain network deployments. See Setting Up Connect on Demand VPN, on page 46 for additional information.

Note There is no configuration in Cisco Jabber for iPad other than turning the Connect on Demand VPN feature on or off. This feature is turned on by default after Cisco Jabber for iPad is installed.

Cross Launching Cisco Jabber for iPad

Cisco Jabber for iPad can be launched from Safari or other browsers to perform one of the following tasks:

- Call a phone number
- Start a chat session
- Place a video call

The following table lists the cross launch URLs third party applications can use to make use of Cisco Jabber for iPad functionality.

Function	Cross Launch URL	Precondition
Call a phone number	ciscotel://<phone_number>	Cisco Unified Communications Manager account
Start a chat session	xmpp://<instant_message_id>	• Cisco WebEx Messenger account • Cisco Unified Presence account

Function	Cross Launch URL	Precondition
Place a video call	• movi://<phone_number> • movi://<URI> • sip://<phone_number> • sip://<URI>	• Cisco TelePresence Video Communication Server account for movi: URLs • Cisco Unified Communications Manager or Cisco TelePresence Video Communication Server account for sip: URLs
Send instant message	ciscojabber://goim?screenname=<contact_id>& message=<message_tx>	• Cisco WebEx Messenger account • Cisco Unified Presence account
Place a VoIP or video call	ciscojabber://call?address=<user_address>& type=<call_type> Call types: • 0 - Point to Point • 1 - Cisco Unified Communications Manager • 2 - Cisco TelePresence Video Communication Server • 3 - Cisco Jabber Video for TelePresence / Cisco WebEx TelePresence • 4 - Determine the active account type and use that to place a call. **Note** If a URL uses a value of 1, 2, or 3 and that account type is not present, the URL will be ignored.	• Cisco Unified Communications Manager account • Cisco TelePresence Video Communication Server account • Cisco Jabber Video for TelePresence / Cisco WebEx TelePresence account
Add a contact	ciscojabber://addbuddy?screenname= <user_name>	
View profile	ciscojabber://goprofile?screenname= <user_name>	

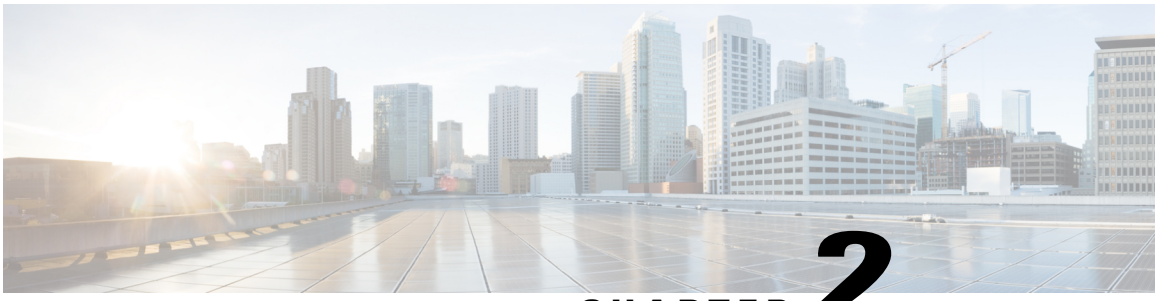
Function	Cross Launch URL	Precondition
Sign in to Cisco Jabber for iPad	ciscojabber://login?type=<account_type>&username=<user_name>&token=<login_token>&primaryserver=<primary_login_server>&secondaryserver=<secondary_login_server>&sipdomain=<sip_domain>&devicename=<ucm_device> Account types: • 1 - Cisco WebEx Messenger • 2 - Cisco WebEx Messenger Single Sign-On • 3 - Cisco Unified Presence • 4 - Cisco Unified Communications Manager • 5 - Cisco TelePresence Video Communication Server • 6 - Cisco Jabber Video for TelePresence / Cisco WebEx TelePresence	• Cisco WebEx Messenger account • Cisco Unified Presence account • Cisco Unified Communications Manager account • Cisco TelePresence Video Communication Server account • Cisco Jabber Video for TelePresence / Cisco WebEx TelePresence account

Apple iOS Support Statement

Cisco supports Cisco Jabber releases only on the latest major iOS release. Apple maintains iOS, provides free iOS updates, and actively encourages users to upgrade to new iOS releases. To help enterprise customers transition to new major iOS updates, Cisco supports the last dot release of the previous major release for three months after a new release is introduced.

Important Notice About Emergency Calls

Using your iPad as a phone may not provide the most timely or accurate location data for an emergency call such as 911, 999, and 112. Calls may be misdirected to the wrong emergency response center or the emergency response center may make errors when determining your location. Use your device as a phone only as a last resort during an emergency. Cisco is not liable for resulting errors or delays.



CHAPTER 2

Set up Simple Sign-In using DNS SRV

You can set up simple sign-in by using Domain Name Server Service Records (DNS SRV). DNS SVR adds an automated discovery mechanism that can eliminate the need for manual account configuration in many deployments. DNS SRV is a standards-based mechanism that enables an automated return of Unified Communications server addresses back to the Cisco Jabber for iPad client. The client reverts to the manual provisioning wizard if no DNS SRV records are configured.

There are two deployment models for DNS SRV when used with the client:

1 **Single Service**

   In a Single Service deployment model only Instant Messaging and Presence or Unified Communications are deployed in a corporate network, not both. This may mean only Cisco WebEx Messenger or Cisco Unified Presence is deployed for Instant Messaging and Presence or Cisco Unified Communications or Cisco TelePresence Video Communication Server is deployed for video and voice calling. Administrators must configure DNS SRV according to the service and DNS SRV mapping table if only one service is deployed. Administrators need to add multiple records if they plan to deploy multiple servers for a single service. Each record must contain the proper priority and weighting information. Port numbering in DNS SRV records is not used by the client but it should still be configured to the default value.

   The client generates a server list based on the priority and weighting it discovers in the DNS SRV records. The client moves through this server list and attempts to connect to each one, stopping when a successful connection to a reachable server is made. The client stops regardless of whether authentication to that server is successful or not.

2 **Multiple Services**

   Multiple Service deployments consist of some mix of Instant Messaging and Presence and Unified Communications services. Administrators must configure DNS SRV according to the service and DNS SRV mapping table. Administrators need to enable Unified Communications integration in Cisco WebEx Messenger or Cisco Unified Presence if they want to integrate the Unified Communications service with the Instant Messaging and Presence service. The client will not automatically sign into Unified Communication accounts after the user has signed into Instant Messaging and Presence accounts. Administrators need to add multiple records if they plan to deploy multiple servers for any single service. Each record must contain the proper priority and weighting information. Port numbering in DNS SRV records is not used by the client but it should still be configured to the default value.

   The client contains a service priority list that can be customized through a DNS TXT record. See Customize Discovery and Auto-Configuration, on page 12 for information on configuring these records. The client tries the first server in each service first. If it fails to connect to that service, it tries the next server in the same service. If it fails to authenticate with the server, it ignores the rest of the servers in this service and

tries to sign-in the first server in next service. If it fails to authenticate to every server it discovered, it displays an error message to end user.

The client remembers successful server connections and attempts to authenticate to them the next time the application is started. If authentication fails, the client automatically performs service discovery and sign-in with the current credentials.

Cisco requires administrators to set up a centralized TFTP server to enable DNS SRV for multi-cluster Cisco Unified Communications Manager deployments only. See Set Up Centralized TFTP Server, on page 11 for more information.

This section discusses this feature and how to configure it for your corporate deployment of the client.

Note The procedures presented in this section are specifically for this feature. Other procedures in other sections are still required for your service deployment. See How to Use this Document, on page 2 for information on what sections go with your specific deployment.

Client Sign-In and Auto-Discovery

The client queries the Domain Name Server (DNS) when it is launched for the first time. After users enter their email address (username@example.com), the client queries the DNS SRV records corresponding to the domain portion of the supplied email address (*example.com* in this instance). It expects responses from the DNS server that allow it to complete the configuration task and provide the user with service. The administrator creates a new DNS SRV record for each type of service the enterprise has implemented. The client supports the following services:

- **Instant Messaging and Presence**
  - Cisco Unified Communications Manager Instant Messaging and Presence (formerly known as Cisco Unified Presence)
  - Cisco WebEx Messenger (formerly known as Cisco WebEx Connect)
- **Unified Communications**
  - Cisco Unified Communications Manager
  - Cisco Telepresence Video Communication Server
  - Cisco Jabber Video for Telepresence
  - Cisco WebEx TelePresence

When both Instant Messaging and Presence and Unified Communications services are deployed (such as Cisco WebEx Messenger and Cisco Unified Communications Manager), the client uses the Unified Communications server as configured in the Instant Messaging and Presence service (Cisco WebEx Messenger or Cisco Unified Presence), rather than any Unified Communication server supplied using the DNS SRV record.

DNS SRV Record

A DNS SRV record provides information on the services available in a specific domain to a client. The client then chooses a server and uses it to connect to the deployed service or server. This section provides information on the form and format of DNS SRV records. See RFC 2782 for additional technical information about DNS SRV records.

The client queries the network for all possible services corresponding to the domain portion of the user-supplied email address. It then attempts to connect based on the services it discovers through the DNS SRV record results. If there is more than one service found, the client connects to the service in this order:

1. Cisco WebEx Messenger
2. Cisco Unified Presence
3. Cisco Unified Communications Manager
4. Cisco TelePresence Video Communication Server
5. Cisco Jabber Video for Telepresence
6. Cisco WebEx TelePresence

The administrator can override this default order. For information on modification, see Customize Discovery and Auto-Configuration, on page 12.

Set Up DNS SRV Records

DNS records consist of a series of entries that match a server name to a single IP address in a networked environment. DNS SRV records differ in that they match a service with a server, or set of servers, in a networked environment. In doing this, DNS SRV allows a client to only have to know what type of service it is looking for instead of the actual server. This aids deployment, server management, and service failover because most networked environments have multiple, load balanced servers attending to the needs of a particular service.

When multiple servers are configured for a single service, the client tries the next server if it is unable to connect to the first entry. In the case of an authentication failure for a given service, the client stops attempting to connect to that service and display an error message.

The following table lists the DNS SRV record types for the client.

Service	DNS SRV Record
Cisco WebEx Messenger	`_xmpp-client._tcp`
Cisco Unified Presence	`_cuplogin._tcp`
Cisco Unified Communications Manager TFTP	`_cisco-phone-tftp._tcp`

Service	DNS SRV Record
Cisco Unified Communications Manager CCMCIP	`_cisco-phone-http._tcp`
Cisco TelePresence Video Communication Server (Internal)	`_sip._tcp.internal`
Cisco TelePresence Video Communication Server (External)	`_sip._tcp.external`
Cisco Jabber Video for TelePresence	`_ciscowtp._tcp`
Cisco WebEx TelePresence	`_ciscowtp._tcp`

The following table gives full examples of DNS SRV records that would be used with the deployment models discussed in this document.

Deployment Model	Full DNS SRV Record Example
Cisco WebEx Messenger Cisco WebEx Messenger and Cisco Unified Communications Manager Cisco WebEx Messenger and Cisco TelePresence Video Communication Server Cisco WebEx Messenger and Cisco Jabber Video for TelePresence	`_xmpp-client._tcp.example.com SRV 0 5222 c2s.example.com.webexconnect.com`
Cisco Unified Presence Cisco Unified Presence and Cisco Unified Communications Manager	`_cuplogin._tcp.example.com SRV 0 1 8443 cup.example.com`
Cisco Unified Communications Manager	`_cisco-phone-tftp._tcp.example.com SRV 0 0 69 cucm.example.com` `_cisco-phone-http._tcp.example.com SRV 0 0 80 cucm.example.com`
Cisco TelePresence Video Communication Server	`_sip._tcp.internal.example.com SRV 0 0 5060 vcsc.example.com` `_sip._tcp.external.example.com SRV 0 0 5060 vcse.example.com`
Cisco Jabber Video for TelePresence	`_ciscowtp._tcp.jabber.com SRV 0 0 443 boot.ciscojabbervideo.com`
Cisco WebEx TelePresence	`_ciscowtp._tcp.webex.com SRV 0 0 443 boot.telepresence.webex.com`

Note Administrators do not need to configure DNS SRV records for Cisco Jabber Video for TelePresence or Cisco WebEx TelePresence. They are already configured and available through the Internet.

The following is an example of a single DNS SRV record that responds to discovery requests by providing the Cisco Unified Presence server address that the client uses.

```
_cuplogin._tcp.example.com SRV 0 1 8443 cup.example.com
```

Note The port numbers provided in the SRV records are not utilized by the client. However, the records should be configured with the provided default values.

Note Weighting and priority are supported within the same DNS SRV record type. Weight only takes effect for SRV records with the same priority.

In this example, the client queries the network for all possible services and gets a response for the defined Cisco Unified Presence server. This tells the client to connect to this server using the supplied credentials as Cisco Unified Presence credentials instead of credentials for any other service.

Use the following general steps to create a new DNS SRV record:

Procedure

Step 1 Compile information on the network services offered.

Step 2 Determine the weighting and priority to assign to each server in the case of multiple servers.

Step 3 Create the new DNS SRV records.

Step 4 Deploy the new records to the network DNS configuration.

Set Up Centralized TFTP Server

Set up a centralized TFTP server if there are multiple Cisco Unified Communications Manager clusters in the same corporate domain. You must also add a DNS SRV record so this server can be discovered. The following is an example of what such a record might look like. The items in the record appear in the following order:

- SRV Record
- Priority
- Weight
- Port
- A Record

```
cisco-phone-tftp._tcp.example.com 0 0 69 cftp.example.com
```

The `cisco-phone-tftp` record type is used to point to the centralized TFTP server. This example allows the client to discover the server `ctftp.example.com` and directly download the device configuration.

Note Note the following about devices and device configuration files:

- All device names must be well formed. The first three letters of the device name should be **TAB** followed by the user name of the person associated with the device. If John Smith's user name is **jsmith**, a well formed device name example would be **TABJSMITH**. The total length of this device name cannot exceed 15 characters.
- Cisco highly recommends that administrators enable SIP Authentication for each tablet device in every cluster.
- Administrators must not add **cisco-phone-http** records in the corporate domain to ensure the centralized TFTP server is discovered.

Customize Discovery and Auto-Configuration

The default service discovery order is:

1. Cisco WebEx Messenger
2. Cisco Unified Presence
3. Cisco Unified Communications Manager
4. Cisco TelePresence Video Communication Server
5. Cisco Jabber Video for TelePresence

System administrators can customize service discovery priority using DNS TXT records. Service discovery priority customization may be necessary in networked environments that provide multiple services. DNS TXT records are defined in RFC 1035. Examples of DNS TXT usage can be found in RFC 4408 (Sender Policy Framework) and RFC 5672 (DomainKeys Identified Mail).

Administrators deploying a DNS TXT record to customize service priority must use a custom form of the typical record called a Jabber Simple Configuration Priority (JSCP) record. A typical DNS TXT record has the following format:

```
name ttl class TXT text
```

A Jabber Simple Configuration Priority record changes that slightly:

```
name ttl class TXT JSCP-specific-text
```

The `JSCP-specific-text` parameter defines the custom service priority. This parameter contains quoted text in the following format:

```
"v=jscpv1 <dns-srv-name>; <dns-srv-name>; ..."
```

Each service is defined using the codes defined in DNS SRV record. Priority is assigned to a service by the location it appears in the service list. The first service in the list is of the highest priority and subsequent entries are of a lesser priority.

Note If your Cisco WebEx Messenger deployment uses Single Sign-On (SSO), the Cisco WebEx Messenger service must always be the first service in the list.

When customizing service priority using a DNS TXT record:

- The priorities found in the DNS TXT record always supercede the default priority list.
- The DNS SRV names in DNS TXT record are recognized by the client even if additional records are present.
- A DNS SRV name with no corresponding DNS SRV record is ignored without error.
- The default priority list is used and an error logged if the DNS TXT record uses an incorrect format or empty.
- The default priority list is used if no DNS TXT record is found.

The following is an example of DNS TXT record with DNS SRV records and using a JSCP formatted record.

```
; UC DNS SRV records

_xmpp-client._tcp.example.com 86400 IN SRV 0 5 5222 xmppserver.example.com

_cisco-phone-tftp._tcp.example.com 86400 IN SRV 0 5 6970 cucm8xserver.example.com

_sip._tcp.internal.example.com 86400 IN SRV 0 5 5060 sipserver.example.com

; JSCP TXT RR example - ignore WebEx Messenger service and favor VCS service with centralized
tftp over CUCM service.

cisco.com 30 IN TXT "v=jscpv1 _sip._tcp.internal.example.com;
_cisco-phone-tftp._tcp.example.com; "

cisco.com 30 IN TXT "v=jscpv1 _cisco-phone-tftp._tcp.example.com"
```

This example is constructed so that the client ignores the Cisco WebEx Messenger service in favor of the Cisco Telepresence Video Communications Server service with centralized TFTP over the Cisco Unified Communications Manager service.

Follow these general steps to create new DNS SRV and DNS TXT records.

Procedure

Step 1 Compile information on the network services offered.

Step 2 Determine the weighting and priority to assign to each server in the case of multiple servers.

Step 3 Determine the order of service discovery.

Step 4 Create the new DNS SRV records.

Step 5 Create the DNS TXT record based on step 3.

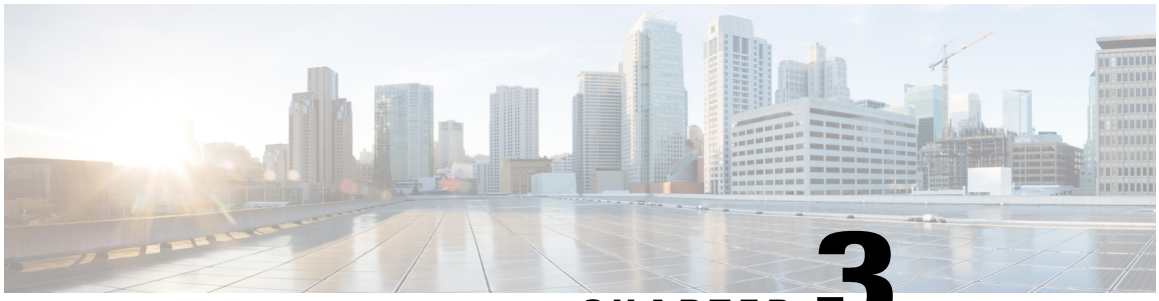
Step 6 Deploy the new DNS SRV records and DNS TXT record to the network DNS server.

Troubleshooting

Use the following information when troubleshooting:

- Troubleshoot DNS configuration from a network-connected device. Use the `NSLOOKUP` command from the Command Prompt in a Microsoft Windows environment. Information on this command can be found at http://support.microsoft.com/kb/816587.
- Select **Settings** > **Help** > **Service Discovery** to perform manual service discovery. Manual service discovery should be guided by the system administrator. Manual service discovery will sign out the current client account, perform service discovery, and automatically sign in discovered services with the current user credentials.

Note Contact your system administrator before performing manual service discovery. Performing service discovery signs you out of your current account and may remove existing account settings.



CHAPTER 3

Set up for Cisco WebEx Messenger

You can set up Cisco Jabber for iPad in a cloud environment by using the Cisco WebEx Messenger Administration Tool. To learn how to use this tool, see the Cisco WebEx Messenger Administration Guide at http://www.webex.com/webexconnect/orgadmin/help/index.htm.

You can also download a PDF of the documentation.

Setting Up with the Cisco WebEx Messenger Administration Tool

The Cisco WebEx Messenger Administration Tool allows you to specify settings for instant messaging (IM), availability, and integration with Cisco Unified Communications Manager. To learn how to use this tool, see the Cisco WebEx Messenger Administration Guide at http://www.webex.com/webexconnect/orgadmin/help/index.htm.

Cisco recommends that you perform the tasks in this order.

Note This is a list of high-level tasks that may not include every aspect of your setup. Go to the individual links for more information.

If a user already has both Cisco WebEx Messenger and Cisco Unified Communications Manager set up in the desktop application, the settings automatically take effect in Cisco Jabber for iPad.

Procedure

Step 1 Specify organization information.
Go to http://www.webex.com/webexconnect/orgadmin/help/index.htm?toc.htm?17382.htm.

Step 2 Create and provision users.
Go to http://www.webex.com/webexconnect/orgadmin/help/index.htm?toc.htm?cs_user.htm .

Step 3 Set up IM and availability.
Go to http://www.webex.com/webexconnect/orgadmin/help/index.htm?toc.htm?17169.htm.

Step 4 Set up telephony services.
Go to http://www.webex.com/webexconnect/orgadmin/help/index.htm?toc.htm?18648.htm.

Note Cisco recommends deploying Cisco Unified Communications Manager with a Fully Qualifed Domain Name (FQDN) when setting up telephony services. If you deploy Cisco Unified Communications Manager with an IP address when setting up telephony services, extra configuration is required to enable the Connect on Demand VPN feature. Refer to the appropriate Cisco Unified Communications Manager documentation for information on using a FQDN.

Step 5 Set up voicemail.
Go to http://www.webex.com/webexconnect/orgadmin/help/index.htm?toc.htm?cs_visual_voicemail.htm.

Note If voicemail parameters are configured in both the Cisco WebEx Messenger Administration Tool and the Product Specific Configuration on Cisco Unified Communications Manager, Cisco Jabber for iPad will use the configuration in Cisco Unified Communications Manager and ignore the voicemail settings in Cisco WebEx Messenger Administration Tool.

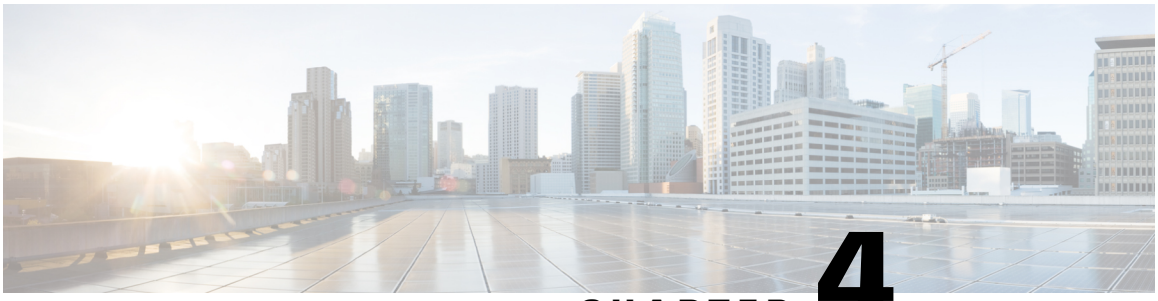
Step 6 Set up meetings.
Go to http://www.webex.com/webexconnect/orgadmin/help/index.htm?toc.htm?17386.htm.

Cisco Unified Communications Manager Setup in Combined Deployment

When setting up Cisco Unified Communications Manager for the combined deployment of Cisco WebEx Messenger and Cisco Unified Communications Manager, use the same procedure described in the chapter for the Cisco Unified Communications Manager only deployment. See Set up for Cisco Unified Communications Manager.

VCS Setup in a Combined Deployment

When setting up Cisco TelePresence Video Communication Server (VCS) for the combined deployment of Cisco WebEx Messenger and VCS, use the same procedure described in the chapter for the VCS-only deployment. See Set up for Cisco TelePresence Video Communication Server.



CHAPTER 4

Set up for Cisco Unified Presence

This chapter describes how you can set up Cisco Jabber for iPad using Cisco Unified Presence.

Specifying Cisco Unified Presence Settings

Follow these steps.

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Application** > **Jabber** > **Settings**.

Note Cisco Unified Presence is known as Cisco Unified Communications Manager IM and Presence starting with Release 9.0. Select **Cisco Unified CM IM and Presence** > **Application** > **Legacy Client** > **Settings** if you are using Release 9.0.

Step 2 Enter the information described in this table:

Field	Setting
CSF certificate directory (relative to CSF install directory)	This field applies only if the Client Services Framework (CSF) requires you to import security certificates to authenticate with LDAP, web conferencing, and CCMCIP. For most deployments, you do not need to import security certificates. You only need to import security certificates for CSF to trust in the following scenarios: • You use a signed certificate for Cisco Unified Communications Manager Tomcat instead of the default self-signed certificate. • You want CSF to connect to the LDAP server via LDAPS. • You use a signed certificate for Cisco Unity Connection Tomcat instead of the default self-signed certificate. If you must specify a value, specify the directory that contains the security certificates as an absolute path. If you do not specify a directory, CSF looks for the certificates in the default directory and trusts any certificates in that location. Default Setting: **Not set**
Credentials source for voicemail service	If user credentials for the voicemail service are shared with another service, select the appropriate service. The user credentials automatically synchronize from the service that you select. Default Setting: **Not set** **Tip** If this value is set to **Not set**, users need to enter their credentials in Jabber for iPad.
Credentials source for web conferencing service	If user credentials for the meeting service are shared with another service, select the appropriate service. The user credentials automatically synchronize from the service that you select. Default Setting: **Not set** **Tip** If this value is set to **Not set**, users need to enter their credentials manually in the application.
Maximum message size	Enter the allowed size limit for instant messages, in bytes.
Allow cut & paste in instant messages	Check this check box to allow users to cut and paste in their chat messages. Default Setting: **On**

Step 3 Select **Save**.

Starting Essential Services

Start the following Cisco Unified Presence Extensible Communication Platform (XCP) services on all Cisco Unified Presence nodes in all clusters:

- Cisco Unified Presence XCP Authentication Service
- Cisco Unified Presence XCP Connection Manager

You may also start these Unified Presence XCP services on all Unified Presence nodes in all clusters, depending on what features you want to make available:

- Cisco Unified Presence XCP Text Conference Manager, for group chat
- Cisco Unified Presence XCP SIP Federation Connection Manager, to support federation services with third-party applications that use SIP
- Cisco Unified Presence XCP XMPP Federation Connection Manager, to support federation services with third-party applications that use XMPP
- Cisco Unified Presence XCP Counter Aggregator, if you want system administrators to be able to view statistical data on XMPP components
- Cisco Unified Presence XCP Message Archiver, for automatic archiving of all instant messages

Note Read the documentation for any feature that you are setting up before you turn on the related services. Additional work might be required.

Firewall Requirements

Configure hardware firewalls to allow the ports to carry traffic for the application. Hardware firewalls are network devices that provide protection from unwanted traffic at an organizational level. This table lists the ports required for the deployments of Cisco Unified Communications Manager and Cisco Unified Presence. These ports must be open on all firewalls for the application to function properly.

Port	Protocol	Description
Inbound		
16384-32766	UDP	Receives Real-Time Transport Protocol (RTP) media streams for video and audio. You set up these ports in Cisco Unified Communications Manager.
Outbound		
69, then Ephemeral	TFTP	Connects to the Trivial File Transfer Protocol (TFTP) server to download the TFTP file

Port	Protocol	Description
80 and 6970	HTTP	Connects to services such as Cisco WebEx Messenger for meetings and Cisco Unity Connection for voicemail features If no port is specified in a TFTP server address, Cisco Jabber for iPad will try port 6970 to obtain phone setup files and dial rule files.
5060	UDP/TCP	Provides Session Initiation Protocol (SIP) call signaling
5061	TCP	Provides secure SIP call signaling
8443	TCP	Connects to the Cisco Unified Communications Manager IP Phone (CCMCIP) server to get a list of currently assigned devices
16384-32766	UDP	UDP Sends RTP media streams for video and audio
389	TCP	Connects to the LDAP server for contact searches
443 7080	VMRest HTTPS	Connects to Cisco Unity Connection to retrieve and manage voice messages.
636	LDAPS	Connects to the secure LDAP server for contact searches

Setting Up Directory Search, IM, and Availability

Review the following topics to set up IM and availability.

Setting Up LDAP Servers

Perform this task in Cisco Unified Presence.

Before You Begin

Do the following:

- Set up the LDAP attribute map
- Obtain the hostnames or IP addresses of the LDAP directories

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **LDAP Server**.

Note LDAP server configuration is done in Cisco Unified Communications Manager starting with Release 9.0.

Step 2 Select **Add New**.

Step 3 Enter the LDAP server name.

Step 4 Enter an IP address or an FQDN (Fully Qualified Domain Name) of the LDAP server.

Step 5 Specify the port number used by the LDAP server. The defaults are:

- TCP—389
- TLS—636

Check the LDAP directory documentation or the LDAP directory configuration for this information.

Step 6 Select **TCP** or **TLS** for the protocol type.

Step 7 Select **Save**.

Creating LDAP Profiles and Adding Users

Cisco Jabber for iPad connects to an LDAP server on a per-search basis. If the connection to the primary server fails, the application attempts the first backup LDAP server, and if it is not available, it then attempts to connect to the second backup server. The application also periodically attempts to return to the primary LDAP server. If an LDAP query is in process when the system fails over, the next available server completes this LDAP query.

Before You Begin

Do the following:

- Specify the LDAP server names and addresses
- You must create the LDAP profile before you can add Cisco Jabber for iPad users to the profile.

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **LDAP Profile**.

Note LDAP profile configuration is done in Cisco Unified Communications Manager starting with Release 9.0.

Step 2 Select **Add New**.

Step 3 Enter information in the fields.

Field	Setting
Name	Enter the profile name limited to 128 characters.
Description	Optional. Enter a description limited to 128 characters.
Bind Distinguished Name	Optional. Enter the administrator-level account information limited to 128 characters. This is the distinguished name with which you bind for authenticated bind. The syntax for this field depends on the type of LDAP server that you deploy. For details, see the LDAP server documentation.
Anonymous Bind	Optional. Uncheck this option to use the user credentials to sign in to this LDAP server. For non-anonymous bind operations, Cisco Jabber for iPad receives one set of credentials. If configured, these credentials must be valid on the backup LDAP servers. **Note** If you check **Anonymous Bind**, users can sign in anonymously to the LDAP server with read-only access. Anonymous access might be possible on your directory server, but Cisco does not recommend it. Instead, create a user with read-only privileges on the same directory where the users to be searched are located. Specify the directory number and password in Cisco Unified Presence for the application to use.
Password	Optional. Enter the LDAP bind password limited to 128 characters. This is the password for the administrator-level account that you provided in the Bind Distinguished Name string to allow users to access this LDAP server.
Confirm Password	Reenter the password you entered in **Password**.
Search Context	Optional. Enter the location where you set up all the LDAP users. This location is a container or directory. The name is limited to 256 characters. Use only a single OU/LDAP search context.
Recursive Search	Optional. Check to perform a recursive search of the directory starting at the search base.
Primary LDAP Server and Backup LDAP Server	Select the primary LDAP server and optional backup servers.
Add Users to Profile	Select the button to open the **Find and List Users** window. Select **Find** to populate the search results fields. Alternatively, search for a specific user and select **Find**. To add users to this profile, select the users, and select **Add Selected**.

Step 4 Select **Save**.

Setting Up the LDAP Attribute Map

Before You Begin

Set up the LDAP attribute map on Cisco Unified Presence where you enter LDAP attributes for your environment and map them to the given Cisco Jabber for iPad attributes.

If you want to use LDAP to store your employee profile photos, use a third-party extension to upload the photo files to the LDAP server or extend the LDAP directory server schema by other means to create an attribute that the LDAP server can associate with an image.

For Cisco Jabber for iPad to display profile photos, in the LDAP attribute map, map the Jabber for iPad "Photo" value to the appropriate LDAP attribute.

Note

- Contact photos may be cropped when they are displayed in Jabber for iPad.
- The UPC UserID setting in the LDAP attribute map must match the Cisco Unified Communications Manager user ID. This mapping allows a user to add a contact from LDAP to the contact list in Cisco Jabber for iPad. This field associates the LDAP user with the corresponding user on Cisco Unified Communications Manager and Cisco Unified Presence.
- You can map an LDAP field to only one Cisco Jabber field.

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **Settings**.
Select **Cisco Unified CM IM and Presence** > **Application** > **Legacy Client** > **Settings** if you are using Release 9.0.

Step 2 Select a supported LDAP server from **Directory Server Type**.
The LDAP server populates the LDAP attribute map with Cisco Jabber user fields and LDAP user fields.

Step 3 If necessary, make modifications to the LDAP field to match your specific LDAP directory.
The values are common to all LDAP server hosts. Note the following LDAP directory product mappings:

Product	LastName Mapping	UserID Mapping
Microsoft Active Directory	SN	sAMAccountName
OpenLDAP	SN	uid

Step 4 Select **Save**.

Tip If you want to stop using the current attribute mappings and use the factory default settings, select **Restore Defaults**.

Indexing Active Directory Attributes

Index these Active Directory attributes:

- sAMAccountName
- displayName
- mail
- msRTCSIP-PrimaryUserAddress

In addition, index any attributes that are used for contact resolution. For example, you might need to index these attributes:

- telephoneNumber
- Any other directory phone number attributes that are used to find contacts, depending on the value of the DisableSecondaryNumberLookups key
- ipPhone, if this attribute is used in your environment

Turning IM Policy On or Off

This procedure describes how to turn on or off IM features for all IM applications in a Cisco Unified Presence cluster. IM features are turned on by default in Cisco Unified Presence.

Caution If you turn off IM features in Cisco Unified Presence, all group chat functionality (ad hoc and persistent chat) will not work in Cisco Unified Presence. Cisco recommends that you do not turn on the Cisco UP XCP Text Conference service or set up an external database for persistent chat in Cisco Unified Presence.

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Messaging** > **Settings**.

Step 2 Select **Enable instant messaging**.

Note
- If you turn on this setting, users can send and receive IMs.
- If you turn off this setting, users cannot send or receive IMs. Users can use IM only for availability and phone operations.

Step 3 Select **Save**.

Step 4 Restart the Cisco UP XCP Router service.

Specifying IM Policy Settings

You can specify IM policy settings by following these steps.

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Presence** > **Settings**.

Step 2 Turn on or off automatic authorization for viewing availability.

If you want to…	Do this…
Turn on automatic authorization so that Unified Presence automatically authorizes all availability subscription requests it receives from Jabber for iPad users in the local enterprise	Check **Allow users to view the availability of other users without being prompted for approval**.
Turn off automatic authorization so that Unified Presence sends all availability subscriptions to where the user is prompted to authorize or reject the subscription	Uncheck **Allow users to view the availability of other users without being prompted for approval**.

Step 3 Select **Cisco Unified Presence Administration** > **Messaging** > **Settings**.

Step 4 Turn on or off these global settings:

If you want to…	Do this…
Globally turn off instant messaging services	Uncheck **Enable instant messaging**.
Globally turn on offline instant messaging	Uncheck **Suppress Offline Instant Messaging**.

Step 5 Select **Save**.

Step 6 Restart the Cisco UP XCP Router service.

Setting Up URL Strings to Fetch Contact Pictures from Web Server

You can set up a parameterized URL string in the Photo field in the LDAP attribute map so that Cisco Jabber for iPad can fetch pictures from a web server instead of from the LDAP server. The URL string must contain an LDAP attribute with a query value containing a piece of data that uniquely identifies the photo of the user. Cisco recommends that you use the User ID attribute. However, you can use any LDAP attribute whose query value contains a piece of data that uniquely identifies the photo of the user.

Cisco recommends that you use `%%<userID>%%` as the substitution string. For example:

- `http://mycompany.example.com/photo/std/%%uid%%.jpg`
- `http://mycompany.example.com/photo/std/%%sAMAccountName%%.jpg`

You must include the double percent symbols in this string, and they must enclose the name of the LDAP attribute to substitute. Cisco Jabber for iPad removes the percent symbols and replaces the parameter inside with the results of an LDAP query for the user whose photo it resolves.

For example, if a query result contains the attribute "uid" with a value of "johndoe," then a template such as `http://mycompany.com/photos/%%uid%%.jpg` creates the URL `http://mycompany.com/photos/johndoe.jpg`. Cisco Jabber for iPad attempts to fetch the photo.

This substitution technique works only if Cisco Jabber for iPad can use the results of the query and can insert it into the template you specify above to construct a working URL that fetches a JPG photo. If the web server that hosts the photos in a company requires a POST (for example, the name of the user is not in the URL) or uses some other cookie name for the photo instead of the username, this technique does not work.

Note

- Limit a URL length to 50 characters.
- Cisco Jabber for iPad does not support authentication for this query; the photo must be retrievable from the web server without credentials.

Setting Up CTI Gateway Profiles

Create the computer telephony interface (CTI) gateway profiles in Cisco Unified Presence Administration and assign primary and backup servers for redundancy.

Before You Begin

Review the following:

- Specify the CTI gateway names and addresses by going to **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **CTI Gateway Server** before you can select the servers as primary or backup servers in this procedure.
- Cisco Unified Presence dynamically creates a TCP-based CTI gateway profile based on the hostname of Cisco Unified Communications Manager. Before using this profile, verify that Cisco Unified Presence and Cisco Jabber for iPad can ping Cisco Unified Communications Manager by the DNS name. If they cannot contact the server, you need to add the IP address of Cisco Unified Communications Manager by going to **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **CTI Gateway Server**. You do not need to delete the host profiles that are created automatically.
- If you previously set up Cisco Unified Communications Manager with an IP address through the **Cisco Unified Communications Manager Administration** > **System** > **Server** menu, Cisco Unified Presence dynamically creates a TCP-based CTI gateway profile based on that address. The fields you see by going to **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **CTI Gateway Profile** are automatically populated, and you need to only add users to the default CTI TCP profile that is created (See step 3.).

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **CTI Gateway Profile**.

Step 2 Search for the CTI gateway profile in the **Find and List CTI Gateway Profiles** window.
If the CTI gateway profile is found, no further action is required from you.

Step 3 If the CTI gateway profile is not found, select **Add New**.

Step 4 Enter the following information into the fields.

Field	Setting
Name	Enter the profile name.
Description	Enter a profile description.
Primary CTI Gateway Server and **Backup CTI Gateway Server**	Select a primary server and a backup server.
Make this the Default CTI Gateway Profile for the System	Check this option if you want any new users that are added to the system to be placed automatically into this default profile. Users who are already synchronized to Unified Presence from Unified Communications Manager are not added to the default profile. However, once the default profile is created, any users synchronized after that are added to the default profile.

Step 5 Select **Add Users to Profile**.

Step 6 Use the **Find and List Users** window to find and select users.

Step 7 Select **Add Selected** to add users to the profile.

Step 8 Select **Save** in the main **CTI Gateway Profile** window.

Setting Up Proxy Listener and TFTP Addresses

Cisco recommends that you use TCP to communicate with the proxy server. If you use UDP to communicate with the proxy server, availability information of the contacts in Cisco Jabber for iPad might be unavailable for large contact lists.

Before You Begin

Obtain the host names or IP addresses of the TFTP servers.

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **Settings**.

Step 2 Select the Proxy Listener **Default Cisco SIP Proxy TCP Listener**.

Step 3 Assign the primary (required) and backup (optional) TFTP server addresses in the fields provided. You can enter an IP address or an FQDN (Fully Qualified Domain Name).

Step 4 Select **Save**.

Setting Up Voicemail Server Names and Addresses on Cisco Unified Presence

Specify voicemail settings on Cisco Unified Presence so that Cisco Jabber for iPad can interact with the voice message web service (VMWS) on Cisco Unity Connection. The VMWS service enables the application to move deleted voicemail messages to the correct location. This service also provides message encryption capabilities to support secure messaging.

Before You Begin

Perform these tasks:

- Ensure that the voicemail server is set up.
- Obtain the hostname or IP address of the voicemail server. You might need to specify more than one hostname to provide services for the number of users in your environment.

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **Voicemail Server**.

Step 2 Select **Add New**.

Step 3 Select **Unity Connection** from the **Server Type** menu

Step 4 Enter the Cisco Unity Connection server name.

Step 5 Enter the hostname or the IP address of the voicemail server.

Step 6 Enter 443 for the **Web Service Port** value.

Step 7 Select **HTTPS** in **Web Service Protocol** menu.

Step 8 Select **Save**.

Setting Up Mailstore Server Names and Addresses on Cisco Unified Presence

Set up Cisco Unified Presence with mailstore information so that Cisco Jabber for iPad can connect to the mailstore.

Cisco Unity Connection usually provides a mailstore and hosts the mailstore on the same server.

Before You Begin

Perform these tasks:

- Obtain the hostname or IP address of the mailstore server.
- Provision mailstore servers before you can add the servers to the voicemail profiles.

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **Mailstore**.

Step 2 Select **Add New**.

Step 3 Enter the mailstore server name.

Step 4 Enter the hostname or the IP address of the mailstore server.

Step 5 Specify the port number set up for the server and the corresponding protocol to use when Cisco Jabber for iPad contacts this server.

Step 6 Select **Save**.

Creating Voicemail Profiles on Cisco Unified Presence

Create voicemail profiles before you can add users to the profiles.

Repeat this procedure for each voicemail profile you want to create.

Before You Begin

Perform these tasks:

- Specify voicemail server names and addresses.
- Specify mailstore server names and addresses.

Procedure

Step 1 Select **Cisco Unified Presence Administration** > **Application** > **Cisco Unified Personal Communicator** > **Voicemail Profile**.

Step 2 Select **Add New**.

Step 3 Enter the profile name and description.

Step 4 Enter the following information:

Field	Description
Voice Messaging Pilot	The voicemail pilot number is the directory number that a user dials to access their voice messages. Each pilot number can belong to a different voice-messaging system. Select one of these options: • **Number—**Select the voicemail pilot number for the system. This is the same as the number specified in the **Voice Mail** > **Voice Mail Pilot** menu in Cisco Unified Communications Manager Administration. • **No Voice Mail—**Select this option if you do not want to send unanswered incoming calls to voicemail.
Primary Voicemail Server	Select a primary server. Select one of the voicemail servers you specified.
Backup Voicemail Server	Enter the name of your backup voicemail server. If you do not want a backup voicemail server, select **None**.
Primary Mailstore	Select the primary mailstore server. Select one of the mailstore servers you specified.
Backup Mailstore	Enter the name of your backup mailstore server. If you do not want a backup voicemail server, select **None**.
Make this the default Voicemail Profile for the system	Check this option if you want new users to be automatically added to the default profile. Users who are already synchronized to Cisco Unified Presence from Cisco Unified CM are not added to the default profile. However, any users who are synchronized after the default profile is created are added to the default profile.

Step 5 Enter the following information:

Field	Description
Inbox Folder	Enter the name of the folder on the mailstore server in which new messages are stored. Only change this value if the mailstore server uses a different folder name from the default folder. Default folder: INBOX
Trash Folder	Enter the name of the folder on the mailstore server in which deleted messages are stored. Only change this value if the mailstore server uses a different folder name from the default folder. Default folder: Deleted Items

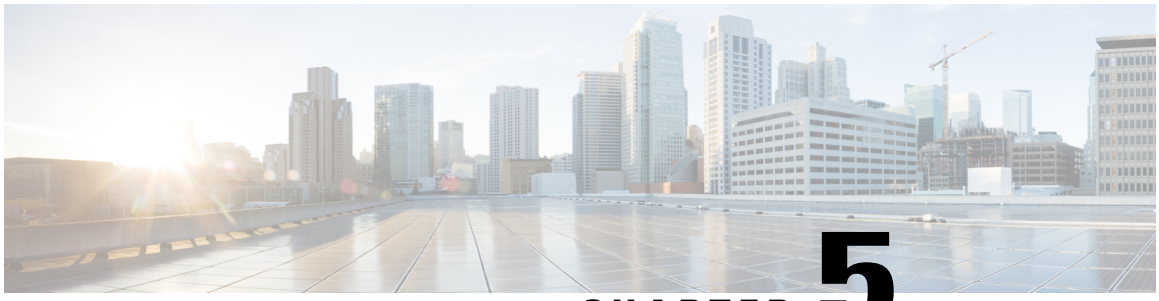
Field	Description
Allow dual folder mode	Turn off this setting if you know that UIDPLUS is not supported and you want to force the system to use Single Folder mode. Default setting: On **Note** The Microsoft Exchange 2007 server does not support UIDPLUS extensions.

Step 6 Select **Add Users to Profile**.

Step 7 Use the **Find and List Users** window to find and select users, and select **Add Selected** to add users to the profile.

Step 8 Select **Save**.

Note If you configured voicemail parameters in Product Specific Configuration on Cisco Unified Communications Manager, Cisco Jabber for iPad will use that configuration and ignore the voicemail settings in the Cisco Unified Presence server.



CHAPTER 5

Set up for Cisco Unified Communications Manager

This chapter describes how you can set up Cisco Jabber for iPad using Cisco Unified Communications Manager

System and Network Requirements

Refer to this section for information on the system and network requirements for Cisco Jabber for iPad.

Supported Audio and Video Codecs

Supported audio codecs include:

- G.722.1, including G.722.1 32k and G.722.1 24k

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

- G.711, including G.711 A-law and G.711 u-law

The supported video codec is H.264/AVC.

Maximum Negotiated Bit Rate

You specify the maximum payload bit rate in the **Region Configuration** window in Cisco Unified Communications Manager. 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.

This table describes how Cisco Jabber for iPad allocates the maximum payload bit rate:

Audio	Interactive video (Main video)
The application uses the maximum audio bit rate.	The application allocates the remaining bit rate in this way: The maximum video call bit rate minus the audio bit rate

Performance Expectations for Bandwidth

A minimal upload bandwidth of 256 - 384 Kbps is required for good VGA video quality. An upload bandwidth above 512 Kbps can produce outgoing video resolution of 480 X 360 at 20 fps and a maximum incoming video resolution of 640 X 480 at 30 fps. VPN usage increases payload size and this increases bandwidth consumption. Video resolutions and frame rates may not be as high using a VPN connection.

Video Rate Adaptation

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 being at lower resolution and scale upwards 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.

Firewall Requirements

Configure hardware firewalls to allow the ports to carry traffic for the application. Hardware firewalls are network devices that provide protection from unwanted traffic at an organizational level. This table lists the ports required for the deployments of Cisco Unified Communications Manager and Cisco Unified Presence. These ports must be open on all firewalls for the application to function properly.

Port	Protocol	Description
Inbound		
16384-32766	UDP	Receives Real-Time Transport Protocol (RTP) media streams for video and audio. You set up these ports in Cisco Unified Communications Manager.
Outbound		
69, then Ephemeral	TFTP	Connects to the Trivial File Transfer Protocol (TFTP) server to download the TFTP file
80 and 6970	HTTP	Connects to services such as Cisco WebEx Messenger for meetings and Cisco Unity Connection for voicemail features If no port is specified in a TFTP server address, Cisco Jabber for iPad will try port 6970 to obtain phone setup files and dial rule files.
5060	UDP/TCP	Provides Session Initiation Protocol (SIP) call signaling
5061	TCP	Provides secure SIP call signaling
8443	TCP	Connects to the Cisco Unified Communications Manager IP Phone (CCMCIP) server to get a list of currently assigned devices
16384-32766	UDP	UDP Sends RTP media streams for video and audio
389	TCP	Connects to the LDAP server for contact searches
443 7080	VMRest HTTPS	Connects to Cisco Unity Connection to retrieve and manage voice messages.
636	LDAPS	Connects to the secure LDAP server for contact searches

Recommended Procedure

This checklist describes general steps to set up Cisco Jabber for iPad using Cisco Unified Communications Manager. The actual procedure for your organization may vary.

1 Setting Up System SIP Parameters, on page 36
2 Installing Cisco Options Package (COP) File for Devices, on page 36
3 Setting Up a Dedicated SIP Profile, on page 38
4 Setting Up Application Dial Rules for Cisco Jabber for iPad, on page 38
5 System-level Prerequisites for Midcall Features, on page 39
6 Usage and Error Tracking, on page 39
7 Adding a User Device, on page 40
8 Bulk Configuration, on page 45
9 Firewall Requirements, on page 19
10 Setting Up Visual Voicemail, on page 45
11 Setting Up Connect on Demand VPN, on page 46
12 Cisco Unified Communications Manager, on page 71

Setting Up System SIP Parameters

Procedure

Step 1 Sign in to Cisco Unified CM Administration.
Step 2 Select **System** > **Service Parameter**.
Step 3 Set the SIP Trying Timer to 1000ms.
Step 4 Set the SIP Dual Mode Alert Timer to 4500ms.
Step 5 Select **Save**.

Installing Cisco Options Package (COP) File for Devices

Install a device-specific Cisco Options Package (COP) file on all Cisco Unified Communications Manager servers to make Cisco Jabber for iPad available as a device.

General information about installing COP files is available in the Software Upgrades chapter of the *Cisco Unified Communications Operating System Administration Guide* for your release at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Note The following Cisco Unified Communications Manager releases already contain the Tablet COP file:

- 7.1.5.35113-1 and above
- 8.5.1.16090-1 and above
- 8.6.2.23057-1 and above
- 9.0.1.11013-1-1 and above
- 9.1.1.10000-11 and above

Installation of the Tablet COP file is not required for these releases.

Important Perform this procedure at a time of low usage because it may interrupt service.

Procedure

Step 1 Download the device COP file for iPad at http://www.cisco.com/cisco/software/navigator.html?mdfid=280443139&flowid=29241.

Step 2 Place the COP file on an FTP or SFTP server that is accessible from your Unified CM servers.

Step 3 Install the COP file on the Publisher server in your Unified CM cluster by following these steps:

a) Select **Cisco Unified OS Administration** in the Navigation drop-down list and then select **Go**.
b) Select **Software Upgrades** > **Install/Upgrade**.
c) Specify the location of the COP file and provide the required information.
For more information, see the online help.
d) Select **Next**.
e) Select the device COP file.
f) Select **Next**.
g) Follow the instructions on the screen.
h) Select **Next**.
Wait for the process to be completed. This process may take some time.
i) Reboot Unified CM at a time of low usage.
j) Restart the Cisco Tomcat service on the Unified CM server.
This step, which clears the Tomcat image cache, is required for the device icon to display properly on the device list page in Unified CM.
k) Enter this command from the CLI:

```
utils service restart Cisco Tomcat
```

l) Let the system fully return to service.

Important To avoid interruptions in service, ensure that each server has returned to active service before you perform this procedure on another server.

Step 4 Install the COP file on each Subscriber server in the cluster. Use the same process you use for the Publisher, including rebooting the server.

Setting Up a Dedicated SIP Profile

Set up a dedicated SIP profile that allows Cisco Jabber for iPad to stay connected to Cisco Unified Communications Manager if the application is running in the background.

Procedure

Step 1 Sign in to Cisco Unified CM Administration.

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

Step 3 Create a SIP profile or copy an existing SIP profile.
You can name the profile "Standard iPad SIP Profile."

Step 4 In the Parameters Used in Phone section, enter these values:

- Timer Register Delta (seconds)—60
- Timer Register Expires (seconds)—660
- Timer Keep Alive Expires (seconds)—660
- Timer Subscribe Expires (seconds)—660

Step 5 Select **Save**.

What to Do Next

Select this SIP profile for all user devices running Cisco Jabber for iPad.

Setting Up Application Dial Rules for Cisco Jabber for iPad

A Cisco Options Package (COP) file must be used to set up dial rules for Cisco Jabber for iPad on Cisco Unified Communications Manager 8.5 and earlier. This COP file is different from the device COP file described in other sections of this document.

Perform the series of procedures described in this topic to make all of your existing dial rules available to the application. This series of procedures will guide you in installing the required XML files in a folder named CUPC at the root level of the Cisco Unified Communications Manager TFTP server.

You can create different dial rules by copying and modifying the XML file to create a dedicated one for Cisco Jabber for iPad. This series of procedures must be repeated every time you update the dial rules on Cisco Unified Communications Manager. This makes the changes available to all applications.

See the related chapters in the *Cisco Unified Communications Manager Administration Guide* for additional information about Application Dial Rule setup. The guide specific to your release of Cisco Unified Communications Manager can be found here:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Procedure

Step 1 Obtaining Cisco Options Package (COP) File for Dial Rules
Step 2 Copying Dial Rules
Step 3 Locating Copies of Dial Rules
Step 4 Modifying Dial Rules
Step 5 Restarting the TFTP Service

System-level Prerequisites for Midcall Features

Ensure that you set up your Cisco Unified Communications Manager system for these midcall features:

- Hold and Resume
- Conference and Merge
- Transfer
- To Mobile

Note For details about setting up these features, see the *Cisco Unified Communications Manager Features and Services Guide* for your release at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Usage and Error Tracking

Cisco Jabber for iPad relies on a third-party service, Google Analytics, to collect and generate aggregated usage and error-tracking data that Cisco uses to discover defects and improve product performance. In compliance with the Google Analytics privacy statement, Cisco does not store personally identifying information.

All information collected is stored by Google and is confidential. Only Cisco has access to this information.

You can enable or disable usage and error tracking for each user when you set up each user device in Cisco Unified Communications Manager.

Depending on the setting, Cisco collects the following information:

Usage and Error Tracking Setting	Information Collected
Enabled	• Errors and warnings • Screen views in the application (for example, how often users view their lists of voice messages) • Feature activities (for example, how often users add a contact) • The TFTP server address to which the application connects • Approximate geographic location, based on mobile service provider activity
Detailed	Same information collected when Enabled is selected
Disabled	None

For more information about the reporting tool, see

- http://www.google.com/analytics/
- http://www.google.com/policies/privacy/

Adding a User Device

Add a user device to your Cisco Unified Communications Manager server and verify the setup.

Before You Begin

Perform these tasks:

- Installing Cisco Options Package (COP) File for Devices, on page 36
- Setting Up a Dedicated SIP Profile, on page 38
- Verify that the Device Pool that you will assign to the iPad device is associated with a region that includes support for all supported audio codecs. The audio codecs that Cisco Jabber for iPad supports include G.711 mu-law or A-law and G.722.1.

Procedure

Step 1 Sign in to Unified CM Administration.

Step 2 Select **Device** > **Phone**.

Step 3 Select **Add New**.

Step 4 Select **Cisco Jabber for Tablet** in the drop-down list and then select **Next**.

Step 5 Enter the information described in this table:

Parameter	Description
Device Information	
Device Name	A device name • represents only one device. If a user has Jabber for iPad on multiple devices, set up each device with a different device name. • must start with TAB, followed by up to 15 uppercased or numeric characters. Example: TABJOHND. • can contain dot (.), dash (–), or underscore (_).
Phone Button Template	Select **Standard Jabber for iPad**.
Protocol Specific Information	
Device Security Profile	Select **Cisco Jabber for iPad – Standard SIP Non-Secure Profile**.
SIP Profile	Select the SIP profile you created. For details, see Setting Up a Dedicated SIP Profile, on page 38.
Product Specific Configuration Layout	
Enable LDAP User Authentication	If you select **Enabled**, be sure to instruct the users to also turn on **LDAP User Authentication** in the application.
LDAP Username	Specify needed LDAP settings so that they are automatically entered in the application.
LDAP Password	
LDAP Server	
LDAP Search Base	
LDAP Field Mappings	**Note** Customization of this field is not currently supported.
Enable LDAP SSL	If you select **Enabled**, be sure to instruct the users to also turn on **Use SSL** in the application.
Voicemail Username	Specify voicemail settings so that they are automatically entered in the application. For details, see Setting Up Visual Voicemail, on page 45.
Voicemail Server	
Voicemail Message Store Username	
Voicemail Message Store	
Cisco Usage and Error Tracking	Select the level of usage information that is available to Cisco. For more information, see Usage and Error Tracking, on page 39.
Video Capabilities	Select **Enabled** if you want to turn on video for the users.
On-Demand VPN URL	The URL used by the Connect on Demand VPN feature.
Preset Wi-Fi Networks	Preset Wi-Fi network information for the device.

Note You will specify other settings when you set up other features.

Step 6 Select **Save**.

Step 7 Select **Apply Config**.

Step 8 Select **[Line n] - Add a new DN**.

Step 9 Enter the directory number of this device.

Step 10 If this device is a standalone device (not sharing a DN with a desk phone), specify these settings to forward calls when the application is not running and connected to the network so callers do not receive an error message:

- **Forward Unregistered Internal**
- **Forward Unregistered External**

For more information about these settings, see the online help in Cisco Unified Communications Manager.

Step 11 Set the **No Answer Ring Duration** to 24 seconds to allow time for the application to ring before calls go to voicemail.
See general restrictions in the online help in Cisco Unified Communications Manager.

Step 12 Specify other settings as appropriate for your environment.

Step 13 Select **Save**.

Step 14 Associate the device that you just created with the user by following these steps:

a) Select **User Management** > **End User**.
b) Search for and select the user.
c) In the Device Information section, select **Device Association**.
d) Check the device that you want to associate with the user.
e) Select **Save Selected/Changes**.

Step 15 If this user has a desk phone, select the desk phone as the Primary User Device.

Note The Primary User Device field is only available in Cisco Unified Communications Manager 9.0 and earlier. This field does not need to specified in later versions of Cisco Unified Communications Manager.

Step 16 If the device is a standalone device that runs without an associated desk phone, you may need to enter other information that is standard for all devices in your system.

What to Do Next

Verify your setup by performing these tasks:

- Ensure that the iPad device is connected to the corporate Wi-Fi network. Verify that you can access a web page on your corporate intranet using the browser on the device.
- Start Jabber for iPad and enter the username (or email address), password, and TFTP server address for the device you just added.
- Test basic voice features in Cisco Jabber for iPad, such as making, holding, and transferring calls.

Turning on Control of iPad as a Phone

Allow your users to control their devices as a phone by following these steps.

Procedure

Step 1 Select **User Management** > **End User** in Cisco Unified Communications Manager Administration.

Step 2 Search for and select the user you want to add.

Step 3 Select **Add to User Group** in the Permissions Information section.

Step 4 Search for "Standard CTI" in the **Find and List User Groups** window.

Step 5 Select **Standard CTI Enabled**.
If the user's phone is a Cisco Unified IP Phone 6900, 8900 or 9900 series model, also select **Standard CTI Allow Control of Phones supporting Xfer and conf**.

Step 6 Select **Add Selected**.

Step 7 Select **Save**.

Specifying LDAP Authentication Settings

The LDAP authentication feature enables Cisco Unified Communications Manager to authenticate user passwords against the corporate LDAP directory.

Note LDAP authentication does not apply to the passwords of application users; Cisco Unified Communications Manager authenticates application users in its internal database.

Before You Begin

Turn on LDAP synchronization in Cisco Unified Communications Manager.

Procedure

Step 1 Select **Cisco Unified Communications Manager Administration** > **System** > **LDAP** > **LDAP Authentication**.

Step 2 Check **Use LDAP Authentication for End Users**.

Step 3 Specify the LDAP authentication settings.

Step 4 Specify the LDAP server hostname or IP address and port number.
Note To use Secure Socket Layer (SSL) to communicate with the LDAP directory, check **Use SSL**.

Step 5 Select **Save**.
Tip If you set up LDAP over SSL, upload the LDAP directory certificate to Cisco Unified Communications Manager.

Setting Up LDAP Synchronization for User Provisioning

Perform this task in Cisco Unified Communications Manager.

LDAP synchronization uses the Cisco Directory Synchronization (DirSync) tool on Cisco Unified Communications Manager to synchronize information (either manually or periodically) from a corporate LDAP directory. When you turn on the DirSync service, Cisco Unified Communications Manager automatically provisions users from the corporate directory. Cisco Unified Communications Manager still uses its local database, but turns off its facility to allow you to create user accounts. You use the LDAP directory interface to create and manage user accounts.

Before You Begin

- Ensure that you install the LDAP server before you attempt the LDAP-specific configuration on Cisco Unified Communications Manager.
- Understand that LDAP synchronization does not apply to application users Cisco Unified Communications Manager. You must manually provision application users in the Cisco Unified Communications Manager Administration interface.
- Activate and start the Cisco DirSync service on Cisco Unified Communications Manager.

Procedure

Step 1 Select **Cisco Unified Communications Manager Administration** > **System** > **LDAP** > **LDAP System**.

Step 2 Select **Add New**.

Step 3 Set up the LDAP server type and attribute.

Step 4 Select **Enable Synchronizing from LDAP Server**.

Step 5 Click **Save**.

Step 6 Select **Cisco Unified Communications Manager Administration** > **System** > **LDAP** > **LDAP Directory**.

Step 7 Select **Add New**.

Step 8 Set up these items:

- LDAP directory account settings
- User attributes to be synchronized
- Synchronization schedule
- LDAP server hostname or IP address and port number

Step 9 Check **Use SSL** if you want to use Secure Socket Layer (SSL) to communicate with the LDAP directory.

Step 10 Click **Save**.

Tip

- If you configure LDAP over SSL, upload the LDAP directory certificate onto Cisco Unified Communications Manager.
- See the LDAP directory content in the Cisco Unified Communications Manager SRND for information on the account synchronization mechanism for specific LDAP products and general best practices for LDAP synchronization.

Bulk Configuration

Use the information in this document to set up individual users and devices as the basis for completing a bulk administration template for setting up users and devices.

When you are ready for bulk processes, follow the instructions in the bulk administration guide for your release of Cisco Unified Communications Manager, available from http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Setting Up Visual Voicemail

Before You Begin

Perform these tasks:

- Verify that VMRest secure message is enabled

  Select Allow Access to Secure Message Recordings to enable API access to secure messages. This is configured in the Cisco Unity Connection Messaging Interface (CUMI). Select **System Settings** > **Advanced** > **API Settings** in Cisco Unity Connection Administration.

- Consult your voicemail administrator if you have questions about any of the settings in this section.

Procedure

Step 1 Sign in to Cisco Unified CM Administration.

Step 2 Go to the device page for the user.

Step 3 In the Product Specific Configuration Layout section, enter these voicemail settings:

Setting	Description
Voicemail Username	Enter the unique username for voicemail access for this user.
Voicemail Server (include the port)	For the voicemail server, enter the hostname or IP address. Use the format Servername.YourCompany.com:portnumber.
Voicemail Message Store Username	Enter the username for the voicemail message store.

Setting	Description
Voicemail Message Store	For the voicemail message store, enter the hostname or IP address. This may be the same as the voicemail server. Use the format YourVoiceMessageStoreServer.yourcompany.com:portnumber.

Step 4 Select **Save**.

What to Do Next

Test your voicemail by performing these tasks:

1. Delete the existing voicemail account, if applicable, in Cisco Jabber for iPad and then restart the application.
2. Sign in using your Cisco Unified Communications Manager account.
3. When prompted for voicemail setup, enter or confirm the settings.
4. Tap **Save**, even if you make no changes.
5. Test the voicemail features.

Setting Up Connect on Demand VPN

Cisco Jabber for iPad supports two ways to enable the Connect on Demand VPN feature.

If your Cisco Unified Presence and Cisco Unified Communications Manager servers are configured with a Fully Qualified Domain Name (FQDN), the Connect on Demand VPN feature is enabled or disabled using Cisco Jabber for iPad. If your Cisco Unified Presence and Cisco Unified Communications Manager servers are configured with an IP address, configure the On Demand VPN URL parameter to enable the Connect on Demand VPN feature.

Note Cisco recommends that Cisco Unified Presence and Cisco Unified Communications Manager be deployed with a FQDN. Use of the Connect on Demand VPN feature requires no additional Cisco Unified Presence and Cisco Unified Communications Manager configuration when deployed with a FQDN.

Before You Begin

- The iPad must be set up for on-demand access to VPN with **certificate-based authentication**. Contact the providers of your VPN client for assistance with setting up VPN access.
- Determine if your Cisco Unified Presence and Cisco Unified Communications Manager servers use a Fully Qualified Domain Name or IP address for network identification.
- Identify a URL that is set up to launch VPN on demand. Enter the URL in the Cisco AnyConnect client. Cisco Jabber for iPad triggers VPN on demand if a DNS query on this domain fails. Use one of the following methods:

- Configure Cisco Unified Communications Manager to be accessed through a domain name and not an IP address. Ensure this domain name is not resolvable outside the firewall. Include this domain in the **Connect If Needed** list in the **Connect On Demand Domain List** of the Cisco AnyConnect client connection.
- If you cannot use a domain name to access Cisco Unified Communications Manager or cannot make the DNS lookup of that domain name fail from outside the firewall, set the parameter in the following procedure to a nonexistent domain. This nonexistent domain would cause a DNS query to fail when the user is inside or outside the firewall. Add that domain to the **Always Connect** list in the **Connect On Demand Domain List** of the Cisco AnyConnect client connection. The URL must include only the domain name. Do not include a protocol or a path. See the following example for more information:

Use	Do Not Use
cm8ondemand.company.com	https://cm8ondemand.company.com/vpn

Procedure

Step 1 Sign in to Cisco Unified CM Administration.

Step 2 Go to the device page for the user.

Step 3 Go to the **Product Specific Configuration Layout** section.

Step 4 Enter the URL you identified before beginning this procedure in the **On-Demand VPN URL** field.

Note The URL must be a domain name only. Do not include a protocol or path.

Step 5 Select **Save**.

What to Do Next

Do the following to test this feature:

- Enter the URL identified in the procedure into Safari on the iPad and verify that VPN launches automatically. You should see a VPN icon in the status bar.
- Verify the iPad can connect to the corporate network using VPN by performing a task such as accessing a corporate intranet site. Contact your VPN provider for assistance if the connection does not work properly.

Disabling Connect on Demand VPN in the Corporate Wireless Network

Perform the following steps to disable the Connect on Demand VPN feature in the corporate wireless network.

Before You Begin

- Collect a list of corporate Wi-Fi SSIDs

Procedure

Step 1 Sign in to Cisco Unified CM Administration.
Step 2 Go to the device page for the user.
Step 3 Go to the **Product Specific Configuration Layout** section.
Step 4 Set the Preset Wi-Fi Networks to up to three corporate Wi-Fi SSIDs separated by a slash (/).
Step 5 Select **Save**.

Set Up SIP Digest Authentication Options

SIP Digest Authentication is a Unified CM security feature that authenticates user devices. For more information, see the *Cisco Unified Communications Manager Security Guide* and the *Cisco Unified Communications Manager Administration Guide*, available from the maintenance guides list.

Note Cisco Jabber does not support SIP Digest Authentication feature with the Dial via Office - Reverse feature.

For Cisco Jabber, you have three options:

- Disable SIP Digest Authentication—Disable SIP Digest Authentication if your deployment does not use this feature.

  See Disable SIP Digest Authentication, on page 48.

- Enable SIP Digest Authentication with automatic password authentication
  - Users do not have to manually enter this password.
  - There is less chance of entry error that prevents Cisco Jabber from registering with Unified CM.

  See Enable SIP Digest Authentication with Automatic Password Authentication, on page 49.

- Enable SIP Digest Authentication with manual password authentication
  - The password is encrypted.
  - Users must manually enter this password.

  See Enable SIP Digest Authentication with Manual Password Authentication, on page 50.

Disable SIP Digest Authentication

Follow these steps on each device page in Unified CM.

Procedure

Step 1 Sign in to the Unified CM Administration portal.

Step 2 Navigate to the device page.

Step 3 In the Device Security Profile drop-down list, select "Cisco Jabber for Tablet - Standard SIP Non-secure profile."

Step 4 Complete the authentication details in the Product Specific Configuration Layout section.

a) In the Enable SIP Digest Authentication drop-down list, select “Disabled.”

b) Leave **SIP Digest Username** blank.

Step 5 Restart Cisco Jabber.

Enable SIP Digest Authentication with Automatic Password Authentication

Procedure

Step 1 Create a new security profile for Cisco Jabber For Tablet under **System** > **Security** > **Phone Security Profile**.

a) Select **Enable digest authentication**.

b) Deselect **Exclude digest credentials in configuration file**.

Step 2 On each End User page, in the User Information section, complete the following tasks:

a) In the User ID field, verify that the user ID is entered.

b) In the Digest Credentials field, enter the digest credentials.

c) In the Confirm Digest Credentials field, reenter the digest credentials.

Step 3 On each Cisco Jabber for Tablet device page, complete the profile information in the **Protocol Specific Information** section.

a) In the **Device Security Profile** list, select the phone security profile you just created.

b) In the **DigestUser** list, select the digest user.

Step 4 On the same device page, complete the authentication details in the Product Specific Configuration Layout section:

a) Leave **SIP Digest Username** blank.

Step 5 Restart Cisco Jabber.

Enable SIP Digest Authentication with Manual Password Authentication

Procedure

Step 1 Create a new profile for Cisco Jabber For Tablet under **System** > **Security** > **Phone Security Profile**.

a) Select **Enable digest authentication**.
b) Select **Exclude digest credentials in configuration file**.

Step 2 On each End User page, in the User Information section, complete the following tasks:

a) In the User ID field, verify that the user ID is entered.
b) In the Digest Credentials field, enter the digest credentials.
c) In the Confirm Digest Credentials field, reenter the digest credentials.

Make a note of this password. You provide this password to the user later.

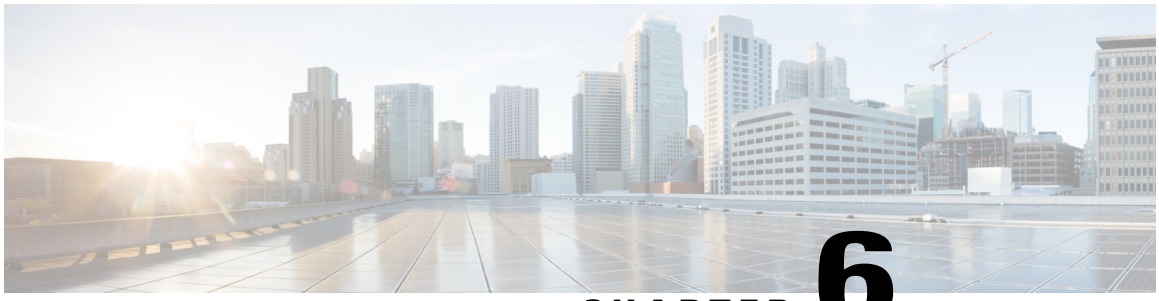
Step 3 On each Cisco Jabber for Tablet device page, complete the profile information in the **Protocol Specific Information** section.

a) In the **Device Security Profile** list, select the phone security profile you just created.
b) In the **DigestUser** list, select the digest user.

Step 4 On the same device page, complete the authentication details in the Product Specific Configuration Layout section:

a) In the Enable SIP Digest Authentication list, select **Enabled**.
b) For the **SIP Digest Username**, enter the digest user you just selected.

Step 5 Restart Cisco Jabber and step through the setup wizard again.



CHAPTER 6

Set up for Cisco TelePresence Video Communication Server

This chapter provides comprehensive information about setting up Cisco Jabber for iPad using Cisco TelePresence Video Communication Server (VCS).

Prerequisites

Perform these tasks:

- Ensure that your versions of the Cisco VCS and Cisco TMS (TelePresence Management Suite) meet the following requirements.

Product	Required version
TMS	13.1 or later
VCS	6.0 or later

- Determine if NTLM authentication is necessary in your network environment. If so, set up NTLM authentication with VCS and Jabber for iPad. For instructions, see the *Cisco TelePresence Video Communication Server Authenticating Devices Deployment Guide* for your release at http://www.cisco.com/en/US/products/ps11337/products_installation_and_configuration_guides_list.html.

Note Cisco Jabber for iPad does not support NTLMv2 authentication.

TMS Setup for Provisioning

To deploy VCS on Cisco Jabber for iPad, provision the user devices with appropriate settings. You add and manage desired settings in TMS. The data is then transferred to the VCS, from which it is distributed to the devices through the Provisioning Server running on the VCS.

Perform these two required procedures to set up TMS for provisioning.

Defining Device Address Pattern

Device address patterns are templates that TMS Provisioning Extension (TMSPE) uses to create addresses for provisioned devices. Assign device address patterns so that TMSPE can connect users to their devices.

To specify a device address pattern for Cisco Jabber for iPad, set the attribute `{device.model}` to jabbertablet. Optionally, add an alias conversion from jabbertablet to jabber to simplify naming.

For detailed instructions about creating address patterns, see the *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide* at http://www.cisco.com/en/US/products/ps11472/prod_installation_guides_list.html.

Setting Up Provisioning Template and Assigning It to Users

Cisco Jabber for iPad requires a specific template—an XML file containing all the possible settings supported by the application. After you download the template and upload it in TMS, you can then set up the template and assign it to groups of users.

For detailed instructions about each of the steps in the procedure, consult the appropriate documentation:

- If you are using the TMS Agent Legacy, included in TMS versions 13.2 and earlier, see the *Cisco TelePresence Management Suite Agent Legacy Deployment Guide* at http://www.cisco.com/en/US/products/ps11338/products_installation_and_configuration_guides_list.html.
- If you are using the TMS Provisioning Extension (TMSPE), included in TMS versions 13.2 and later, see the *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide* at http://www.cisco.com/en/US/products/ps11472/prod_installation_guides_list.html.

Procedure

Step 1 Download the template to your local server from http://www.cisco.com/cisco/software/navigator.html?mdfid=280443139&flowid=29241.

Step 2 Upload the template or template schema in TMS.
The term "template schema" is used in TMSPE while the term "template" is used in TMS Agent Legacy.

Step 3 Add these server addresses, in addition to any other necessary settings, in the template:

- Public SIP Server Address
- SIP Server Address
- Phone Book Server URI

Step 4 Assign the template to the appropriate groups of users.
Any template you assign to a group is inherited by all users in the group, all subgroups, and all users in subgroups. You cannot assign a template directly to an individual user.

Note Cisco recommends keeping all VCS templates for backwards client compatibility. Multiple templates can exist for a specific device type on each VCS and it is the client subscription request that indicates to the provisioning server which template to use. The provisioning server uses the Model and Version fields from the request to determine the correct template. If the Version string from the request is lower than all installed templates for that model, the provisioning request will fail. If the Version string from the request is higher than any installed templates for that model, a best effort attempt is made to find the closest matching template of equal or lower version.

Understanding Provisioning Options

Provisioning allows you to specify settings that control how VCS works with Cisco Jabber for iPad. After subscribing to VCS, Cisco Jabber for iPad receives provisioning information from the Cisco TMS Agent and acts on it.

This table explains the provisioning options that are applicable for Cisco Jabber for iPad and includes tips on how you can use them.

Field	Default	Description
Bandwidth Prober Auto Scheduling	Off	This option allows bandwidth probing. Bandwidth probing also requires these settings to be provisioned: • **TurnAuthPassword** • **TurnAuthUsername** • **TurnServer**

Field	Default	Description
ClearPath	On	ClearPath is a Cisco TelePresence solution that minimizes the negative effects of packet loss in a non-optimal network. Among the mechanisms used are H.264-specific error recovery techniques, feedback from decoders, and forward error correction (FEC). Both call participants must be using devices that support ClearPath for it to take effect.
Default Mediatype Candidate	Host	This is the address to use • before ICE negotiation has completed; • if ICE fails; or • if the remote side does not understand ICE. The available options are • **Host—**the local network address • **Rflx—**the corporate public IP address seen from outside of the organization's network (public IP) • **Relay—**the address of the TURN relay server You can use **Relay** if you are deploying Jabber for iPad in environments where most other devices do not understand ICE.
Encryption Policy	Auto	Determines the encryption policy for the account. This option affects both the SIP communication (Transport TLS or TCP) and the media communication (SRTP or no SRTP). For a call to be encrypted, both the SIP and the media communication must be encrypted, and all parties must support encryption. Encrypted media communication is sent using the Secure Real-time Transport Protocol (SRTP) with a 128-bit Advanced Encryption Standard (AES). The Encryption policy setting is provisioned to the client as configured in **Systems** > **Provisioning** > **Directory** in Cisco TMS. Force TLS/TCP determines whether the SIP communication is encrypted (TLS) or not (TCP). The TLS version is 1.0.cForce/No Srtp determines whether the media communication is encrypted or not. Auto means the client will try to have an encrypted call, but if not possible, it will allow the call to be unencrypted.
ICE	Off	Interactive Connectivity Establishment (ICE) dynamically discovers the best possible path for media to travel among call participants.

Field	Default	Description
Maximum In Bandwidth	512 KB/s	The value you specify determines the maximum bandwidth allowed in the user accounts for receiving and sending data. High bandwidth is directly related to good video quality. However, bandwidth control can prevent an application from trying to receive or send data beyond its capacity, which may result in packet loss, jitter, and low video quality.
Maximum Out Bandwidth	384 KB/s	
Media Port Range End	21900	The upper/lower bound of the port numbers that are used in the video and audio communication. You can set these up to control security and firewall issues. You must specify a range of minimum of 10 ports; otherwise, Jabber for iPad will revert to default.
Media Port Range Start	21000	
MNS Mode	Off	Enabling this option forces relayed media to be relayed via private HD links with guaranteed capacity to ensure quality of video. This setting relies on ICE being enabled. Private dedicated links are provided by companies such as Media Network Services.
Multiway Participant URI		When Multiway is initiated, participants are directed to this Uniform Resource Identifier (URI).
Phone Book Server URI		Allows the account to search for other accounts in the Cisco TMS Agent database. Set up the URI in this format: phonebook@<sip_domain>.com **Important** If you do not specify any value, Cisco Jabber for iPad cannot search for contacts.
Presence Server URI		Allows the account to send availability status to the VCS server. Set up the URI in this format: presence@<sip_domain>.com **Note** Cisco Jabber for iPad uses the availability status from Cisco WebEx Messenger if a server has been identified. If you do not specify any value, Cisco Jabber for iPad cannot publish availability status and will appear offline.

Field	Default	Description
Public Default Mediatype Candidate	Uses the value set for **Default Mediatype Candidate** Changes dynamically	This is the address to use • before ICE negotiation has completed; • if ICE fails; or • if the remote side does not understand ICE. The available options are • **Host—**the local network address • **Rflx—**the corporate public IP address seen from outside of the organization's network (public IP) • **Relay—**the address of the TURN relay server Cisco recommends that you use **Relay** if your users will connect from outside your organization's network. ICE negotiation can take a few seconds to complete, and using the TURN relay helps media flow through the firewalls from the beginning of the call. Upon completion of ICE negotiation, media is redirected if a superior media path has been located.
Public Maximum In Bandwidth	Uses the value set for **Maximum In Bandwidth** Changes dynamically	The value you specify determines the maximum bandwidth allowed for receiving and sending data after users sign in to the application using their VCS accounts. The settings may be useful for controlling the bandwidth for users who connect from outside their organizations' networks. These users may have slow network connections or the company may want to limit their bandwidth usage.
Public Maximum Out Bandwidth	Uses the value set for **Maximum Out Bandwidth** Changes dynamically	
Public Phone Book Server URI	Uses the value set for **Phone Book Server URI** Changes dynamically	It is sufficient to set the **Phone Book Server URI** setting.

Field	Default	Description
Public Presence Server URI	Uses the value set for **Presence Server URI** Changes dynamically	It is sufficient to set the **Presence Server URI** setting.
Public SIP Server Address	Uses the value set for **SIP Server Address** Changes dynamically	the server address to which a registration request is sent after users sign in with an external VCS server address Generally, this information is the same as the external server address the users specify in Jabber for iPad.
Resolution Preferences	High	Restricts incoming and outgoing video resolution. Cisco Jabber for iPad overrides this value. The restrictions depend on many factors, but as a general rule • **High** allows the highest resolution possible up to wide-screen HD (1920x1080 or 1280x720). • **Medium** restricts resolutions to wide CIF (512x288) or lower. • **Low** restricts resolutions to wide QCIF (256x144) or lower.
SIP Server Address	the VCS server that Jabber for iPad is subscribed to	the server address to which a registration request is sent It is the same as the internal server address users specify in Cisco Jabber for iPad.
AuthUserName		SIP Authentication Username. The endpoint uses the AuthUsername and AuthPassword values to authenticate with the VCS server.
AuthPassword		SIP Authentication Password. The endpoint uses the AuthUsername and AuthPassword values to authenticate with the VCS server.
TurnAuthPassword		TURN server settings that are required for enabling ICE. See Turning on ICE, on page 61 for more information.
TurnAuthUsername		
TurnServer		

VCS Setup

Review this topic if you use the registration Allow List or search rules.

In order for the user devices to work with the VCS, the devices must first register with the VCS. The suffix in the registration URIs for Cisco Jabber for iPad users is `.jabbertablet` or `.jabber`. For example, a user's URI may be in this format with the new suffixes: `userName.jabbertablet@DomainName` or `userName.jabber@DomainName`. Because of the URI suffix additions, you may need to make these changes:

- Update the registration Allow List (**VCS configuration** > **Registration** > **Allow List**) to allow the new URI suffixes.

  Example: If you have deployed both VCS and VCSE (VCS Expressway) and used the Allow List to control registration from external locations, add the new suffixes to the Allow List.

- Update or create search rules to include the new URI suffixes. In creating search rules, specify a pattern string that resembles the format `.+\.(jabbertablet|jabber).*@%localdomains%.*`.

  Example: If you have multiple VCS clusters (zones) within your organization, you may have to update the rules that control call routing between the VCS and VCSE zones.

Firewall Requirements

Set up hardware firewalls to allow the ports to carry traffic for the application. Hardware firewalls are network devices that provide protection from unwanted traffic at an organizational level. This table lists the ports required for the deployment of VCS. These ports must be open on all firewalls for the application to function properly.

Protocol	Port and description
DNS	• When VCS accesses the DNS server, it usually listens on port 53. • VCS does not try to control from which src port the request is sent.
SIP	• No server port is opened unless it is provisioned to open. If VCS receives provisioning to open 5060, it opens 5060 for UDP and TCP and 5061 for TLS/TCP. • Under normal usage, only one outgoing TCP connection is established towards the SIP proxy. VCS does not try to control which TCP src port it uses. • VCS uses DNS SRV to discover on which ports the SIP server is listening. VCS accepts well-known ports such as 80 or 443, but under normal usage, the SIP default server ports are 5060 and 5061.
HTTP	• Under normal usage, only one outgoing TCP connection is established towards the http or https server. VCS does not try to control which TCP src port it uses. • The application uses DNS to discover the server port; normal usage is 80 or 443.

Protocol	Port and description
media	• VCS gets provisioned with a port range that it can use for media (RTP/UDP). • For each call, the application opens nine ports within that range and listens for incoming UDP traffic. • The default port range is 21000 to 21900, and you need to specify a proper range for the application.
TURN	• The application tries to discover the best media path by using ICE. • VCS allocates nine ports on the TURN server for each call. • The TURN allocations use the media port range used for media. • The application uses DNS SRV to discover on which ports the TURN server is listening. VCS accepts well-known ports such as 80 or 443, but the ports that are used under normal usage are 3478 or 5349 (TURN standards). • Due to the STUN and TURN standards, the application cannot use the same ports for each call. Therefore, the port range should have a minimum of 100 ports.

Main Types of Communication

Review these topics to understand the main types of communication for VCS on Cisco Jabber for iPad.

SIP Communication

Cisco Jabber for iPad communicates with the VCS using Session Initiation Protocol (SIP). With the exception of video and audio, SIP is responsible for all communications, including subscribing, registering, availability querying, and call invitations. SIP messages are sent by TCP, with or without TLS encryption, depending on the provisioned settings.

The default SIP listening ports used in the VCS are

- 5060 (unencrypted)
- 5061 (encrypted)

To change those listening ports, go to **VCS Configurations** > **Protocols** > **SIP** > **Configuration**.

Note Jabber itself uses ephemeral TCP ports for these communications. These ports are handed over to Cisco Jabber for iPad by the TCP stack and are not configurable.

To enable communication with devices that rely on H.323 and do not support SIP, interworking on the Cisco VCS can be used.

Media Communication

Media data is transferred through up to nine UDP links (ports). These are the media streams used in Cisco Jabber for iPad:

- audio
- primary video
- secondary video (presentation sharing)
- BFCP (management of presentation sharing). Cisco Jabber for iPad can receive a presentation shared using BFCP but it cannot send a presentation using BFCP.

With the exception of BFCP, each of these streams requires two links—one link for RTP packets and one link for RTCP packets. The SRTP protocol is used if encryption is enabled.

Changing Port Range in TMS

The default port range for Cisco Jabber for iPad to receive media is 21,000-21,900. You can change the range in the TMS.

Note The port numbers used are consecutive, but they are chosen randomly within the specified range.

Procedure

Step 1 Go to **Systems** > **Provisioning** > **Directory**

Step 2 Specify your range using **Media Port Range Start** and **Media Port Range End**.
Specify a minimum range of 10 ports; otherwise, the default range is used.

Changing Port Range in VCS

The default port range used on the VCS is 50,000-52,399. You can change it.

Note The port numbers used are consecutive, but they are chosen randomly within the specified range.

Procedure

Step 1 Go to **VCS Configuration** > **Local zone** > **Traversal subzone**.

Step 2 Specify your range using **Traversal media port start** and **Traversal media port end**.
Specify a minimum range of 10 ports; otherwise, the default range is used.

About Binary Floor Control Protocol (BFCP)

Cisco Jabber for iPad supports single BFCP streams from multipoint control units (MCUs) for handling the control of presentation sharing. BFCP communication can be sent over a UDP or a TCP link. Cisco Jabber for iPad uses the same ports as for audio and video for this communication.

On VCS a port is chosen randomly from the same range that has been assigned to the media links.

Media Routing

Cisco Jabber for iPad supports Interactive Connectivity Establishment (ICE) for better media routing. During a call, ICE is used if enabled for all participants' applications. Review these topics to learn more.

Media Routing Without ICE

Media links can be established directly between two devices in non-traversal calls or between Cisco Jabber for iPad and the VCS in traversal calls. As a general rule, non-traversal calls are defined as calls between two participants that are on the same network and do not require interworking.

SIP-to-H.323 calls require interworking. Such calls are traversal calls, whether or not the devices are on the same network. For details, see the *Cisco TelePresence Video Communication Server Administrator Guide* for your VCS release at http://www.cisco.com/en/US/products/ps11337/prod_maintenance_guides_list.html.

Media Routing with ICE

ICE dynamically discovers the best possible path for media to travel among call participants. You can improve the routing of media and force it through dedicated links by using the **Enable MNS Mode** provisioning setting.

Turning on ICE

Set up Cisco VCS Expressway to turn on ICE.

Media routing using ICE requires a TURN server. VCS Expressway running version X5.2 or later can function as a TURN server if it has TURN Relay licenses. The TURN server option key is required.

Note ICE provisioning is not available by default.

Procedure

Step 1 In VCS Expressway, go to **VCS configuration** > **Expressway** > **TURN** and specify these settings:

Setting	Change to…
TURN services	On

Setting	Change to…
Port	3478
Media port range start	60000
Media port range end	61399

Step 2 Go to **VCS configuration** > **Authentication** > **Devices** > **Configuration** and then specify LocalDatabase for **Database type**.

Step 3 Go to **VCS configuration** > **Authentication** > **Devices** > **Local database** and create a username and password. The username and password are required for use of TURN Relay licenses.

Step 4 Go to **Systems** > **Provisioning** > **Directory** > **Configurations** and set the following fields with these values:

Setting	Change to...
Enable ICE	On
TurnAuthPassword	Password created when setting up the Cisco VCS Expressway
TurnAuthUsername	Username created when setting up the Cisco VCS Expressway
TurnServer	The address of the server media is relayed through in an ICE call. Typically the address of the Cisco VCS Expressway.

TURN Port for Cisco Jabber for iPad

TURN port setup should be controlled through DNS. Cisco Jabber for iPad does an SRV lookup for the TURN IP, priority, weight, and port. As TURN runs over UDP, the lookup is for `_turn._udp.<domain>`. If no SRV record for TURN is found, Cisco Jabber for iPad performs an A record lookup (IPv4) or an AAAA lookup (IPv6) but defaults to port 3478.

If the port needs to be provisioned, you can append it to the IP address in the TurnServer field, for example `192.0.2.0:3478`.

How Does Communication Work at Sign-in?

After signing in to Cisco Jabber for iPad, users specify the internal and external VCS server addresses. The application first attempts to subscribe to the internal address. In such situations as the iPad device being connected to non-corporate Wi-Fi, the application then tries to subscribe to the external address.

If the internal VCS server address is a DNS address that translates to more than one IP address, the application attempts to connect to all these IP numbers before trying the external VCS server address. If the DNS server

contains SRV records, the application adheres to the priority and weight of the IP addresses; otherwise they are tried in a random order.

Typically, the VCS or the TMS Agent challenges the first subscription message. The application answers this challenge by sending another SUBSCRIBE message with the authentication information.

After the subscription has been authenticated, the TMS Agent sends provisioning information to the application.

The application registers to the VCS according to the provisioning information for **SIP Server URI** or **Public SIP Server URI** in the TMS. If this provisioning information is identical to the internal and external VCS server addresses users specify upon signing in (Cisco recommends that they are identical.), the application registers to the same VCS it subscribes to. As long as the application is registered, the VCS knows to forward messages to the application.

After initial registration, the application continues to send registration messages to the VCS according to the **Standard registration refresh maximum (seconds)** setting in the VCS server. The application sends the messages after 75% of the specified time interval has elapsed.

Note The **Standard registration refresh maximum (seconds)** setting is not available in version X6.0 of VCS.

Specifying Maximum Time for Registration Refresh

When a user temporarily leaves Cisco Jabber for iPad to do something else on the device, the application goes into the background and is set to wake up every 10 minutes. You must set the maximum value for a standard SIP registration refresh period to 900 so the application can continue registering to the VCS server.

Procedure

Step 1 In the VCS server, go to **VCS configuration** > **Protocols** > **SIP** > **Configuration**.

Step 2 In the "Registration controls" section, enter 900 for **Standard registration refresh maximum (seconds)**.

Step 3 Select **Save**.

How Does Communication Work after Sign-in?

After users sign in to Cisco Jabber for iPad, the application continuously performs these tasks.

Connectivity Checks

Cisco Jabber for iPad uses DNS to find TURN servers and ports after users sign in to the application. If specified in the SRV records and supported by the TURN server, the application can use any port, including 80 (HTTP) and 443 (HTTPS).

The application looks for ports in the following order:

1 UDP

2 TCP (if supported)

3 TLS (if supported)

If no ports are detected, the application defaults to ports 3478 and 5349.

Note Firewall traversal using TCP relay is not supported if you use the VCS as a TURN server at this time.

Bandwidth Probing

If bandwidth probing is provisioned, Cisco Jabber for iPad routes dummy media to the TURN server and back from the server after users sign in to the application. This functionality relies on a TURN server being successfully provisioned.

The results of bandwidth probing are used for the application's dynamic resource adaptation. The results also depend on the provisioned time for probing and in many cases represent a worst case bandwidth scenario in which more bandwidth may be available during an actual call.

Directory Search

Every time a user types a character in the search field of Cisco Jabber for iPad, the application queries the TMS Agent on the VCS, and the TMS Agent answers with matching results. When a search result is selected, the application also queries the VCS for the availability of the contact.

Call Setup

Call setup is communicated by SIP messages passed through VCS. Review these topics to learn how attributes of a call are determined during call setup.

Encryption

For a call to be encrypted, both the SIP and the media communication must be encrypted, and all parties must support encryption. Encrypted media communication is sent by the Secure Real-time Transport Protocol (SRTP) with 128-bit Advanced Encryption Standard (AES).

You can specify these encryption policy settings by going to **Systems** > **Provisioning** > **Directory** in the TMS:

- **Force TLS/TCP—**Determines whether the SIP communication is encrypted (TLS) or not (TCP). The TLS version used by Cisco Jabber for iPad is currently 1.0.
- **Force/No Srtp—**Determines whether the media communication is encrypted or not.
- **Auto—**Cisco Jabber for iPad tries to have an encrypted call. If not possible, the application allows the call to be unencrypted.

Sent and Received Bandwidth

During call setup, Cisco Jabber for iPad signals the maximum bandwidth it wants to receive according to the settings in the server. It is up to the system on the other end of the call to respect this signaling.

Both the maximum bandwidth to be sent during a call and the bandwidth sent at the start of a call are determined during call setup.

During a call, the application can send more or less bandwidth, but the sent bandwidth never goes beyond the maximum bandwidth decided during call setup.

Video Resolution

The Resolution Preferences setting in provisioning controls the resolution for both incoming and outgoing video. See Understanding Provisioning Options, on page 53. It is up to the systems used by the other participants in a call to obey restrictions on incoming video.

Many factors contribute to good video quality. Frame rate, high image resolution, scene lighting, and optical quality of the cameras used in a call are all important factors.

Outgoing Video Resolution

Cisco Jabber for iPad uses these criteria when determining the resolution when it sends video:

- The resolution in native format from the camera
- The resolution must be permitted by the receiving end.
- Sending high resolution at low bandwidth results in poor quality. The bandwidth sent must be sufficient for the resolution. See these guidelines:
  - Best: 640x368 requires at least 768 Kbps
  - Good: 480x360 requires at least 512 Kbps

Increasing bandwidth improves image quality. You can specify bandwidth permissions using **Maximum Out Bandwidth**. For more information, see Understanding Provisioning Options, on page 53.

If a high resolution is not achieved despite sufficient bandwidth as described above, this can usually be attributed to one or both of the following:

- Issues with network connection, including packet loss
- High CPU usage

Incoming Video Resolution

You can specify bandwidth permissions for incoming video by using **Maximum In Bandwidth** in provisioning. For more information, see Understanding Provisioning Options, on page 53. The bandwidth required for incoming high-resolution video varies with the capabilities and limitations of the device of each call participant.

Note If a participant device is capable of sending high-resolution video and you specify no restrictions on bandwidth for incoming video, network connection issues, such as packet loss, may still cause incoming video to achieve less-than-desired resolution.

Presentation Resolution

The maximum resolution for a shared presentation is dependent on the available bandwidth and the capabilities of the devices of the call participants. For a Jabber-to-Jabber call using unlimited bandwidth, the presentation resolution is 448 p.

You cannot change the resolution for presentations.

Video and Audio Standards

Cisco Jabber for iPad supports these standards for both sending and receiving. The application always uses the best standard that is supported by the devices or applications of other participants in a call.

- Audio—G.722.1 and G.711
- Video—H.264

ICE Negotiation

After a call has been connected, ICE is negotiated if enabled and supported by both or all call participants. ICE negotiations take a couple of seconds and require nine TURN server licenses, with one license for each media link.

Actions During a Call

After a call has been set up, a number of actions can be prompted in Cisco Jabber for iPad, either as a result of a user action or as an automated response to changing conditions. Review these topics to learn more.

Multiway

Multiway is the ability for a user to join a call and seamlessly create a multi-participant conference. Cisco Jabber for iPad cannot initiate multiway. If multiway is initiated from devices that other participants are using, the call is redirected to a multi-conference system according to the **Multiway Participant URI** provisioning option.

Mute Media Streams

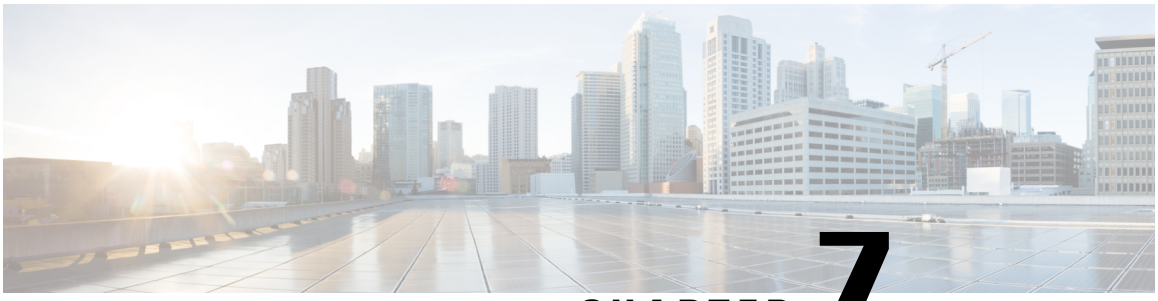
If a camera or microphone is muted during a call, Cisco Jabber for iPad allocates the bandwidth for the other media links to use. If a user does not have enough bandwidth for two streams, it is possible to mute one stream and improve the quality of the other stream.

To prevent the unused link from being closed, for example by a firewall, the application sends STUN (keep alive) messages every 7 seconds.

Automatic Bandwidth Adaptation

In situations where Cisco Jabber for iPad is sending or receiving bandwidth that exceeds the network capabilities, high packet loss may occur and the user may experience poor call quality. The application uses automatic bandwidth adaptation mechanisms to tackle such bandwidth issues.

Note Automatic adaptations take time. Cisco recommends that you set up the application to fit the network and system capabilities.



CHAPTER 7

Prepare user instructions

This section contains information on preparing instructions for application users.

Note It will not be necessary to provide information such as server addresses if you have configured DNS SRV as outlined in Set up Simple Sign-In using DNS SRV, on page 7. Administrators will still have to provide other information such as user names, passwords, and email addresses regardless of the configuration chosen.

Cisco WebEx Messenger

Send an email message with the information that your users need to sign in to Cisco Jabber for iPad. The information includes the following:

- Directions to download and install the app, named **Cisco Jabber for iPad** from the App Store
- Email address for the user's account
- Directions to input email address after the user starts the application on their iPad
- Directions to access the FAQs, which users can view by selecting **Settings icon** > **Help** > **FAQs**
- Anything else you may want to communicate with your users

Cisco WebEx Messenger and Cisco Unified Communications Manager

Send an email message with the information that your users need to use Cisco WebEx Messenger and Cisco Unified Communications Manager in Cisco Jabber for iPad. The information includes the following:

- Directions to download and install the app, named **Cisco Jabber for iPad**, from the App Store
- Credentials for the user's accounts:
  - email address for the Cisco WebEx Messenger account
  - username or email address and the TFTP server address for the Cisco Unified Communications Manager account
- Directions to set up accounts in this order:
  1. Directions to input email address after the user starts the application on their iPad.
  2. Set up Cisco Unified Communications Manager from **Settings** in the application.

Caution If users sign in to their Cisco Unified Communications Manager accounts first, they cannot set up Cisco WebEx Messenger in the application.

- Directions to access the FAQs, which users can view by selecting **Settings icon** > **Help** > **FAQs**
- Anything else you may want to communicate with your users

Cisco WebEx Messenger and Cisco TelePresence Video Communication Server

Send an email message with the information that your users need to use Cisco WebEx Messenger and VCS in Cisco Jabber for iPad. For VCS users, send a customized email message from the TMS. The default email template contains a simple message and the username and password.

Note To learn more about sending account information from the TMS, consult the appropriate documentation:

- If you use the TMS Agent Legacy, see the *Cisco TelePresence Management Suite Agent Legacy Provisioning Guide* at http://www.cisco.com/en/US/products/ps11338/products_installation_and_configuration_guides_list.html.
- If you use the TMS Provisioning Extension (TMSPE), see the *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide* at http://www.cisco.com/en/US/products/ps11472/prod_installation_guides_list.html.

Your email message should include the following information:

- Directions to download and install the app, named **Cisco Jabber for iPad**, from the App Store
- Credentials for the user's accounts:
  - email address for the Cisco WebEx Messenger account
  - username, internal and external server addresses, and SIP domain address for the VCS account

    If your users are dispersed on different VCS clusters, ensure to communicate the correct server addresses to the different groups of users.
- Directions to set up accounts in this order:
  1. Directions to input email address after the user starts the application on their iPad.
  2. Set up VCS from **Settings** in the application.

Caution If users sign in with their VCS accounts first, they cannot set up Cisco WebEx Messenger in the application.

- Directions to access the FAQs, which users can view by selecting **Settings icon** > **Help** > **FAQs**
- Anything else you may want to communicate with your users

Cisco Unified Communications Manager

When you finish setting up Cisco Unified Communications Manager, send your users an email message that includes the following information:

- Directions to download and install the app, named **Cisco Jabber for iPad**, from the App Store
- The TFTP server address, the user's username or email address, and the optional CCMCIP server address
- Directions to input email address after the user starts the application on their iPad
- Instructions for connecting the device to the corporate Wi-Fi network. This process is independent of Cisco Jabber for iPad.
- Instructions for setting up VPN (Virtual Private Network) access on the device, if you allow users to use Cisco Jabber for iPad through VPN connections. This process is independent of Cisco Jabber for iPad.
- Instruct whether the users need to turn on **Use SSL** and **LDAP User Authentication** from the application

  Ensure that you have specified all the needed LDAP settings in the Product Specific Configuration Layout section for the user device in Cisco Unified CM Administration so that the settings are automatically entered in the application. For details, see Adding a User Device, on page 40.
- Directions to access the FAQs, which users can view by selecting **Settings icon** > **Help** > **FAQs**
- Anything else you want to communicate with your users

Cisco Unified Presence

When you finish setting up Cisco Unified Presence, send your users an email message that includes the following information:

- Directions to download and install the app, named **Cisco Jabber for iPad**, from the App Store
- The user's username or email address
- Directions to input email address after the user starts the application on their iPad
- Instructions for connecting the device to the corporate Wi-Fi network. This process is independent of Cisco Jabber for iPad.
- Instructions for setting up VPN (Virtual Private Network) access on the device, if you allow users to use Cisco Jabber for iPad through VPN connections. This process is independent of Cisco Jabber for iPad.
- Directions to access the FAQs, which users can view by selecting **Settings icon** > **Help** > **FAQs**
- Anything else you want to communicate with your users

Cisco Unified Presence and Cisco Unified Communications Manager

Send an email message with the information that your users need to use Cisco Unified Presence and Cisco Unified Communications Manager in Cisco Jabber for iPad. The information includes the following:

- Directions to download and install the app, named **Cisco Jabber for iPad**, from the App Store
- Credentials for the user's accounts:
  - username or email address and the server address for the Cisco Unified Presence account
  - username or email address and the TFTP server address for the Cisco Unified Communications Manager account
- Directions to set up accounts in this order:
  1. Directions to input email address after the user starts the application on their iPad.
  2. Set up Cisco Unified Communications from **Settings** in the application.

Caution If users sign in to their Cisco Unified Communications Manager accounts first, they cannot set up Cisco Unified Presence in the application.

- Instructions for connecting the device to the corporate Wi-Fi connection. This process is independent of Cisco Jabber for iPad.

- Instructions for setting up VPN (Virtual Private Network) access on the device, if you allow users to use Cisco Jabber for iPad through VPN connections. This process is independent of Cisco Jabber for iPad.
- Directions to access the FAQs, which users can view by selecting **Settings icon** > **Help** > **FAQs**
- Anything else you may want to communicate with your users

Cisco TelePresence Video Communications Server

To provide users with the information they need to use VCS in Cisco Jabber for iPad, send a customized email message from the TMS to the users. The default email template contains a simple message and the username and password.

Also include the following information in your email message:

- The internal and external server addresses. If your users are dispersed on different VCS clusters, ensure to communicate the correct server addresses to the different groups of users.
- The SIP domain address
- Directions to input email address after the user starts the application on their iPad
- Directions to download and install the app, named **Cisco Jabber for iPad** from the App Store
- Directions to access the FAQs, which users can view by selecting **Settings icon** > **Help** > **FAQs**
- Anything else you may want to communicate with your users

To learn more about sending account information from the TMS, consult the appropriate documentation:

- If you use the TMS Agent Legacy, see the *Cisco TelePresence Management Suite Agent Legacy Deployment Guide* at http://www.cisco.com/en/US/products/ps11338/products_installation_and_configuration_guides_list.html.
- If you use the TMS Provisioning Extension (TMSPE), see the *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide* at http://www.cisco.com/en/US/products/ps11472/prod_installation_guides_list.html.