Setup for Unified Communications Manager

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

System and network requirements

Review these requirements for 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 Unified Communications Manager 8.6.1 or later.

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

The supported video code is H.264/AVC.

Maximum negotiated bit rate

You specify the maximum payload bit rate in the **Region Configuration** window in Unified CM. 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 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

This table helps you understand what performance you should be able to achieve per bandwidth. Note that VPN (Virtual Private Network) increases the size of the payload, which increases the bandwidth consumption.

Upload speed	Audio	Audio + interactive video (main video)
125 Kbps with VPN	At bandwidth threshold for G.711 Sufficient bandwidth for G.722.1	Insufficient bandwidth for video
384 Kbps with VPN	Sufficient bandwidth for any audio codec	w288p (512x288) at 30 fps
384 Kbps in an enterprise network	Sufficient bandwidth for any audio codec	w288p (512x288) at 30 fps
1000 Kbps	Sufficient bandwidth for any audio codec	w576p (1024x576) at 30 fps

Upload speed	Audio	Audio + interactive video (main video)
2000 Kbps	Sufficient bandwidth for any audio codec	w720p30 (1280x720) at 30 fps

Video rate adaptation

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.

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

For Jabber for iPad to work properly, 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 deployments of Unified Communications Manager and 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 Unified CM.
Outbound		
69	TFTP	Connects to the Trivial File Transfer Protocol (TFTP) server to download the TFTP file
80, 7080, and 6970	HTTP	Connects to services such as WebEx Connect for meetings and Cisco Unity Connection for voicemail features If no port is specified in a TFTP server address, Jabber for iPad will try port 6970 to obtain phone setup files and dial rule files.

Port	Protocol	Description
5060	UDP/TCP	Provides Session Initiation Protocol (SIP) call signaling
5061	TCP	Provides secure SIP call signaling
8443	TCP	Connects to the 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
143	IMAP (TCP/TLS)	Connects to Unity Connection to retrieve and manage the voice messages
389	TCP	Connects to the LDAP server for contact searches
443 8443	TCP HTTPS	Connects to services such as WebEx Connect for meetings and Unity Connection for voicemail features
8443	HTTPS	Connects to the User Data Services (UDS) for contact searches in Unified CM
636	LDAPS	Connects to the secure LDAP server for contact searches
993	IMAP (SSL)	Connects to Unity Connection to retrieve and manage the voice messages
7993	IMAP (TLS)	Connects to Unity Connection to retrieve and manage the voice messages

Recommended procedure

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

1 Installing Cisco Options Package (COP) file for devices, on page 5
2 Setting up a dedicated SIP profile, on page 6
3 Setting up application dial rules for Jabber for iPad, on page 7
4 System-level prerequisites for midcall features, on page 11
5 Usage and error tracking, on page 11

Installing Cisco Options Package (COP) file for devices

To make Jabber for iPad available as a device in Unified Communications Manager, install a device-specific Cisco Options Package (COP) file on all your Unified CM servers.

General information about installing COP files is available in the "Software Upgrades" chapter in 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.

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

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 Jabber for iPad to stay connected to Unified Communications Manager if the application is running in the background.

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 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 Jabber for iPad.

Using dial rules for Jabber for iPad

Jabber for iPad uses these two sets of dial rules to make it easier for users to dial phone numbers from their iPad devices:

- Application Dial Rules (AppDialRules.xml)
- Directory Lookup Dial Rules (DirLookupDialRules.xml)

Unified CM generates these files when the Cisco Options Package (COP) file for dial rules is installed.

Directory Lookup Dial Rules use Microsoft Active Directory to identify callers. Jabber for iPad displays the caller ID from the main iPad Address Book instead of any name provided by the Unified CM or Microsoft Active Directory.

About application dial rules

Because people are accustomed to dialing numbers differently from a mobile device versus from a desk phone, consider setting up Unified Communications Manager to accommodate the different number patterns that mobile device users dial.

You can create these rules in Unified CM so that they apply to all calls and devices or edit an XML file, described later, so that the rules apply to only users of Jabber for iPad. You can also set up different rules that apply to devices in different countries or area codes.

Mobile device users may dial numbers in these ways:

- Mobile device users may not be in the habit of dialing 9 before they dial a number outside the company.
- If the mobile device number is in a different area code from the desk phone number, users may dial the area code when using their mobile devices and would not dial the area code when using their desk phones, and vice versa.
- Mobile device users who dial an international number may begin the number with a plus sign (+).

You can set up application dial rules to successfully connect calls, for which the numbers are dialed with the patterns described earlier. For complete information about setting up application dial rules, see the online help in Unified CM.

If you need to create rules that apply only to Jabber for iPad and do not apply to all other applications that use the same XML files to access dial rules, you can enter them directly as XML text into the file that makes the rules available to Jabber for iPad. See Setting up application dial rules for Jabber for iPad, on page 7.

Setting up application dial rules for Jabber for iPad

Use a Cisco Options Package (COP) file to set up dial rules for Jabber for iPad. This COP file is different from the device COP file described in another topic of this document.

Perform the series of procedures described in this topic to make all of your existing dial rules available to the application. With this series of procedures, you install required XML files in a folder called "CUPC" at the root level of the Unified CM TFTP server.

If you need different rules for Jabber for iPad, use the optional procedure to copy and modify the XML file to create a dedicated file for Jabber for iPad. Every time you update the dial rules on Unified CM, you must repeat this series of procedures to make the changes available to applications, including Jabber for iPad.

Step 1 See Obtaining Cisco Options Package (COP) file for dial rules , on page 8

Step 2 See Copying dial rules, on page 8.

Step 3 See Locating copy of dial rules, on page 9.

Step 4 See Modifying dial rules, on page 9.

Step 5 See Restarting TFTP service, on page 10.

Obtaining Cisco Options Package (COP) file for dial rules

Use a COP file that is also used for this purpose for other Cisco products.

Note This procedure applies to only Unified CM Release 8.5 and earlier versions.

The COP file described in this procedure is different from the device COP file that is used to make Jabber for iPad available as a device in Unified CM.

Step 1 Go to the Software Downloads page for Cisco UC Integration for Microsoft Office Communicator at http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=282588075.

Step 2 Select the release number that most closely matches your Unified CM release.

Step 3 Look for the bundle that contains the Administration Toolkit.

Step 4 Select **Download Now**.

Step 5 Find the instructions on the screen.

Step 6 Unzip the downloaded file.

Step 7 Locate the dial rules COP file in the CUCM folder.
You do not need any other files in this download.

Step 8 Place the dial rules COP file on a server that is accessible by TFTP.

Copying dial rules

Create copies of dial rules in Unified CM by following these steps.

Step 1 Sign in to the Publisher server in your Unified CM cluster.

Step 2 Select **Cisco Unified OS Administration** in the Navigation drop-down list and then select **Go**.

Step 3 Select **Software Upgrades** > **Install/Upgrade**.

Step 4 Specify the location of the COP file `Dial Rules COP` in the **Software Installation/Upgrade** window.

Step 5 Select **Next**.

Step 6 In the Available Software drop-down list, select the COP file.

Step 7 Select **Next**.

Step 8 Select **Install**.

Step 9 Repeat this procedure for every Unified CM server that runs on a TFTP server.

Locating copy of dial rules

Follow these steps.

Step 1 In Cisco Unified Operating System Administration, select **Software Upgrades** > **TFTP File Management**.

Step 2 In the **TFTP File Management** window, search for a directory name that begins with `CUPC`.

Step 3 Verify the dial rules.
For example, you may see

- `AppDialRules.xml`
- `DirLookupDialRules.xml` (for Jabber for iPad)

Modifying dial rules

Use this optional procedure only if you want to modify the dial rules file for use by Jabber for iPad. For example:

- You may require rules that are unique to Jabber for iPad and are not used for other clients.
- You may need to create multiple files and assign different rules to the iPad device of each user. For example, if users have mobile devices that are issued in different countries or area codes and your existing rules do not accommodate the way users may dial numbers or stored contacts from mobile devices based in multiple countries or area codes.

Before You Begin

Do the following:

- Determine the application dial rules you need by using the guidelines in About application dial rules.
- If you do not know how to use the TFTP server on Unified CM, see the following documents for your release:
  - Instructions for managing TFTP server files in the "Software Upgrades" chapter of the *Cisco Unified Communications Manager Operating System Administration Guide*
  - The *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*

Both the documents are available at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Step 1 Navigate to the CUPC folder at the root level of the Unified CM TFTP server.

Step 2 Copy the rules file you want to modify for Cisco Jabber.

For example, using the built-in TFTP application on a Windows or Mac computer, enter these commands:

tftp server-name

get CUPC/AppDialRules.xml

Step 3 Rename the file as needed.
Example: `AppDialRulesFrance.xml`

Step 4 Open the file in a text editor

Step 5 Following the example of the existing rules, modify or add rules as needed.

Step 6 Save your changes.

Step 7 Upload the modified file by following these steps:

1. In Unified CM Administration, select **Cisco Unified OS Administration** in the Navigation drop-down list.
2. Select **Software Upgrade** > **TFTP File Management**.
3. Select the file on your hard drive.
4. Specify the folder on the TFTP server.
   Example: `ciscojabber`
5. Select **Upload**.

Step 8 Repeat for any other rules files that you want to customize.

What to Do Next

After you complete and upload all customized Dial Rules files, continue with the next procedure in this section.

If you are using Unified CM Release 8.5 or an earlier version and you want the iPad devices to apply Application Dial Rules, you must specify the path to these dial rules files, including the filenames. If you move or rename these files, make sure to update this path in the Application Dial Rules URL field on the configuration page for each deployed device.

Restarting TFTP service

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

For more information, see the "Starting, Stopping, Restarting, and Refreshing Status of Services in Control Center" topic in the *Cisco Unified Serviceability Administration Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Step 1 In Unified CM Administration, select **Cisco Unified Serviceability** in the Navigation drop-down list and then select **Go**.

Step 2 Select **Tools** > **Control Center-Feature Services**.

Step 3 Select the server and select **Go**.

Step 4 Select **Cisco TFTP**.

Step 5 Select **Restart**.

Step 6 Repeat this procedure on every server on which you ran this COP file.

System-level prerequisites for midcall features

Ensure that you set up your Unified CM 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

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 personal identifying information.

All information that is 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 Unified CM.

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 user device

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

Before You Begin

Perform these tasks:

- Installing Cisco Options Package (COP) file for devices, on page 5
- Setting up a dedicated SIP profile, on page 6
- 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 Jabber for iPad supports include G.711 mu-law or A-law and G.722.1.

Step 1 Sign in to Unified CM Administration.

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

Step 3 Select **Add New**.

Step 4 Select **Cisco Jabber for iPad** 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 6.
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. For details, see Specifying directory search settings, on page 16.
LDAP Password	
LDAP Server	
LDAP Search Base	
LDAP Field Mappings	
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 15.
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 11.
Video Capabilities	Select **Enabled** if you want to turn on video for the users.

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 Unified CM.

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 Unified CM.

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.

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 Jabber for iPad, such as making, holding, and transferring calls.

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 Unified CM, 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 IMAP is enabled.

  See the "Configuring IMAP Settings" topic in the *System Administration Guide for Cisco Unity Connection* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

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

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.
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 Jabber for iPad and then restart the application.
2. Sign in using your 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.

Specifying directory search settings

Before You Begin

Perform these tasks:

- Make sure the **telephoneNumber** attribute in Active Directory (or its equivalent, if you are using a different attribute) is indexed.
- Collect the required information in the table in the procedure.
- If you have any questions about the values in the tables in this procedure, consult your directory administrator.
- Identify attributes in your corporate directory schema that are different from or additional to the defaults in the following table. Map changed attributes later in this procedure.

Element	Element Name	Default Directory Attribute	Your Value, if Different
Unique identifier	identifier	distinguishedName	
Display name	displayName	displayName	
Email address	emailAddress	mail	
First name	firstName	givenName	
Last name	lastName	sn	
User ID	userid	userPrincipalName	
Main phone number	mainPhoneNumber	telephoneNumber	
Home phone number	homePhoneNumber	—	
Second home phone number	homePhoneNumber2	—	
Mobile phone number	mobilePhoneNumber	mobile	
Second mobile phone number	mobilePhoneNumber2	—	
Direct to voicemail phone number	voicemailPhoneNumber	voicemail	
Fax number	faxPhoneNumber	facsimileTelephoneNumber	
Other phone number	otherPhoneNumber	—	

Important In Active Directory,

- phone numbers must be unformatted; and
- Global Catalog must be enabled.

Step 1 Sign in to Unified CM Administration.

Step 2 Navigate to the iPad device page for the user.

Step 3 Enter LDAP User Authentication settings:

- If credentials are not required to access directory services, select **Disabled**.
- If users must enter credentials to access directory services, select **Enabled**.

Step 4 Enter the LDAP username and password.
Do one of the following:

- Enter credentials for a single read-only account that all users will use to access Active Directory. These credentials will be sent in clear text in the TFTP file. Users will not need to enter credentials in the application.
- Enter a username with access to the directory and leave the password blank. Communicate what the password is to each user and ask users to enter the password in the application.
- If authentication is not required, leave these settings blank.

By default, the LDAP Username is the userPrincipalName (UPN) and may be in the form of an email address, for example, userid@example.com.

Step 5 Enter the LDAP server address.

- Enter the hostname or IP address and port number for your Active Directory server in this format:

  YourDirectoryServer.YourCompany.com:portnumber

- Use port 3269 for secure SSL connections or 3268 for nonsecure connections.

If you enter no port or SSL settings, the application, by default, attempts an SSL connection to port 3269.

Step 6 Enter the LDAP Search Base using the format: CN=users,DC=corp,DC=yourcompany,DC=com.
By default, the application uses the search base that is found in a RootDSE search on the defaultNamingContext attribute. If you need to specify a different search base, enter the Distinguished Name of the root node in your corporate directory that contains user information. Use the lowest node that includes the necessary names. Using a higher node will create a larger search base and thus reduce performance if the directory is very large.

To help determine the optimal search base, you can use a utility such as Active Directory Explorer (available from Microsoft) to view your data structure.

Step 7 Enter the LDAP field mappings.
LDAP field mappings identify the attributes in your directory that hold the information to be searched and displayed for directory searches.

Enter any field mappings that do not match the default as "name=value" pairs, separating each field with a semicolon (;).

Example: displayName=nickname;emailAddress=email. Use the Element Name value as the name value.

Step 8 Select **Save**.

What to Do Next

Test the corporate directory settings by following these steps:

1. Delete the corporate directory account, if applicable, from Settings in Jabber for iPad, and then restart the application.
2. Sign in using your Unified Communications Manager account and then enter or confirm the corporate directory settings when prompted.
3. Tap **Save**, even if you make no changes.
4. Test directory search.

Preparing user instructions

When you finish setting up 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
- Instructions to select **Select Account** > **Unified Communications Manager** after users start the application on their iPad devices
- Instructions for connecting the device to the corporate Wi-Fi network. This process is independent of Jabber for iPad.
- Instructions for setting up VPN (Virtual Private Network) access on the device, if you allow users to use Jabber for iPad through VPN connections. This process is independent of 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 user device, on page 12.
- Directions to access the FAQs, which users can view by selecting **Settings icon** > **Help** > **FAQs**
- Anything else you want to communicate with your users