Setup for Cisco Unified Presence and Cisco Unified Communications Manager

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

Specifying Cisco Unified Presence Settings

Follow these steps.

Procedure

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

Additionally, perform this procedure in Cisco Unified Communications Manager:

Procedure

Step 1 Select **Cisco Unified Serviceability** > **Tools** > **Control Center - Network Services**.

Step 2 Select the desired Cisco Unified Presence server from the **Server** list box.

Step 3 Select **Go**.

Step 4 Confirm that the Cisco UP XCP Router service is running.

Step 5 If the Cisco UP XCP Router service is not running, do the following:

a) Select the radio button next to the **Cisco UP XCP Router** service in the **CUP Services** section.

b) Select **OK**.

Step 6 Select **Cisco Unified Serviceability** > **Tools** > **Service Activation**.

Step 7 Select the desired Cisco Unified Presence server from the **Server** list box.

Step 8 Select **Go**.

Step 9 Select **Cisco UP XCP Directory Service**.

Step 10 Select **Save**.

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	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

Port	Protocol	Description
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.
8443	HTTPS	Connects to the User Data Services (UDS) for contact searches in Cisco Unified Communications Manager
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**.

Setting Up Secure Connection Between Cisco Unified Presence and LDAP Directory

Before You Begin

Enable SSL for LDAP on Cisco Unified Communications Manager, and upload the LDAP directory certificate to Cisco Unified Communications Manager.

Procedure

Step 1 Select **Cisco Unified OS Administration** > **Security** > **Certificate Management**.

Step 2 Select **Upload Certificate**.

Step 3 Select **directory–trust** from the **Certificate Name** menu.

Step 4 Browse and select the LDAP server certificate from your local computer.

Step 5 Select **Upload File**.

Step 6 Restart the Tomcat service from the CLI using this command:

```
utils service restart Cisco Tomcat
```

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.

Field	Setting
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

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.

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.

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**.

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.

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.

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
- Setting Up a Dedicated SIP Profile
- 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.
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	

Parameter	Description
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.
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.
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.

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.

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 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.
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 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.

Field	Description
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
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.

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

- Determine if your Cisco Unified Presence and Cisco Unified Communications Manager servers use a Fully Qualified Domain Name or IP address for network identification.

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 On Demand VPN URL to a that resolves to an appropriate server in the corporate network if it is not identified with a FQDN.

Step 5 Select **Save**.

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**.

Preparing User Instructions

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. Select **Select Account** > **Unified Presence** after users start the application on their iPad devices
  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