Cisco Jabber for Android Release 8.6.2 Administration Guide

First Published: July 29, 2011

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

CONTENTS

CHAPTER 1

Cisco Jabber for Android

Cisco Jabber for Android provides users with Enterprise VoIP calling and access to the corporate directory while users are connected to the corporate network.

With Cisco Jabber for Android, you can do the following:

- Place and receive VoIP calls from your corporate phone number through Cisco Unified Communications Manager using your mobile device, while Cisco Jabber is running and connected to the corporate network.
- Securely connect to your corporate network from any remote location, using Wi-Fi or mobile data networks.
- Use the native Android phone application to place work calls from the Keypad, Logs, Favorites, or Contacts tab.
- Have up to two VoIP calls (call waiting, add new call, swap between active calls).
- Use many of the standard in-call features that Cisco Unified Communications Manager provides, including hold, transfer, and conference.
- Transfer an active Cisco Jabber VoIP call to your mobile network.
- Transfer an active Cisco Jabber VoIP call from your device to your desk phone.
- Search the corporate directory.
- See a message indicator for new voice messages that are left at the office phone number.
- Access voicemail from the home screen; or from the status bar if a new message exists.
- Receive calls to your work phone number while Cisco Jabber for Android runs in the background. Cisco Jabber for Android automatically registers to Cisco Unified Communications Manager when available.

Limitations and restrictions

Cisco Jabber for Android includes the following limitations and restrictions:

- Platform support and compatibility:
    - ◦ Telephony integration

      Cisco Unified Communications Manager Versions 7.1.5, 8.0.3, 8.5, and 8.6

      Note Cisco Unified Communications Manager 8.6 is supported with Cisco Jabber for Android 8.6.1 or later. See the *Release Notes* located at http://www.cisco.com/en/US/partner/products/ps11678/prod_release_notes_list.html for exact versions. For more information, see the “Cisco Unified Mobility” section of the *Cisco Unified Communications Manager Features and Services Guide* for limitations located at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

    - ◦ Voicemail (optional)

      Cisco Unity Connection Versions 7.1, 8.0, 8.5, and 8.6.1

    - ◦ Lightweight Directory Access Protocol (LDAP) integration (optional)

      Microsoft Active Directory 2003 and 2008, or Open LDAP. Required only to support corporate directory search.

    - ◦ Secure connect (optional)

      Cisco Adaptive Security Appliance (ASA):

        - ◦ For certificate-based authentication: ASA Version 8.4.1 or later
        - ◦ For AAA authentication: ASA Version 8.0 or later

      Certificate Authority (CA) if using certificate-based authentication: Cisco IOS Certificate Server or Microsoft Windows Server 2008 Certificate Authority

- Cisco Jabber supports G.711u, G.729a, and G.729b codecs.
- You can run Cisco Jabber for Android on the following devices:
    - Samsung Galaxy S International (GT-I9000) with Android operating system (OS) Version 2.2.1 or 2.3
    - Samsung Galaxy Tab International (GT-P1000) with Android 2.2.1 or 2.3
    - Samsung Galaxy S II (AT&T) with Android 2.3
    - Samsung Galaxy S 4G (T-Mobile) with Android 2.2.1

  To use Cisco Jabber for Android on the Samsung Galaxy S device, it is important that you upgrade your handset OS to Android Version 2.2.1 or 2.3. See the manufacturer/carrier site for more information about how to update the OS on your device. Minor voice quality issues may be experienced depending on the device used.

- Although not officially supported, Cisco Jabber for Android runs on many Android Version 2.2 and 2.3 devices with various limitations depending on the device. For information about running Cisco Jabber on unsupported devices, see the Cisco Support Forums at http://supportforums.cisco.com.
- To obtain the best possible experience when using Cisco Jabber over Wi-Fi, we recommend that:
    - Wi-Fi networks should be designed to minimize occurrences of layer 3 roams when IP addresses change, resulting in long latency or roam times, dropped calls, or dropped voice packets.
    - All access points have the same Service Set Identifier (SSID). Roaming can be slow if the SSIDs do not match.
    - Access points should broadcast their SSID (otherwise Cisco Jabber may disconnect from the Wi-Fi network when roaming to the next access point and interrupt calls).

Related documents

The following documentation includes information related to Cisco Jabber:

- Cisco Jabber documentation for users is available from http://www.cisco.com/en/US/partner/products/ps11678/products_user_guide_list.html.
- Technical information specific to this product is available in the Solutions Reference Network Design (SRND): http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guides_list.html.
- Cisco Unified Communications Manager documentation for administrators is available at http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html.

CHAPTER 2

Before you begin

Deploy Cisco Jabber

The following general steps describe how to deploy Cisco Jabber.

Procedure

Step 1 Verify system requirements, including network requirements for optimal voice quality and call maintenance. Release notes for this product are located at http://www.cisco.com/en/US/partner/products/ps11678/prod_release_notes_list.html.

Step 2 Review the list of necessary files. You can collect these files now, or collect them as you need them for the procedures in this document. See Required files, on page 6.

Step 3 Set up the system. See Before you begin, on page 5.

Step 4 Add a test device. See Administration, on page 17.

Step 5 Set up required features.

a) Verify that all prerequisites are met.

b) Set up the system-level settings for the features and functionality that you will deploy.

c) Set up the required user-level settings.

d) Set up the device in Cisco Unified Communications Manager.

e) Test your setup for each feature.

Instructions for each feature are listed in Feature setup, on page 23.

Step 6 Use your working setup as a template for setting up devices for your users.
See Bulk configuration, on page 21.

Step 7 Send an email message with the information that users need to set up Cisco Jabber.

The settings you entered on the device page in Cisco Unified Communications Manager are automatically entered into the application on the device. Users will enter passwords as applicable. Documentation for users is located at http://www.cisco.com/en/US/partner/products/ps11678/products_user_guide_list.html.

Required files

You need the following files to set up and use Cisco Jabber. You can collect them all now, or obtain them when you are ready to use them.

File	To obtain this file, see
For Cisco Unified Communications Manager Release 8.5 and earlier	
Cisco Options Package (COP) file required to make Application Dial Rules available to Cisco Jabber	Cisco Jabber for Android uses the same COP file as Cisco UC Integration for Microsoft Office Communicator to make Application Dial Rules available. 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.
For all Cisco Unified Communications Manager releases	
Device COP file	Go to the software download site: http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=281001428. Locate and download `cmterm-android_8.6.2v17.cop.sgn`.
Cisco Jabber application for your device	Use the Android Market application on your device to obtain the Cisco Jabber for Android application. Search for Jabber on the Google Android Market. When you search for Cisco Jabber, be sure to distinguish Cisco Jabber from Cisco Jabber IM.
For Cisco Adaptive Security Appliance releases (if deploying secure connect feature)	
Cisco AnyConnect VPN client software package	To set up the ASA for Cisco Jabber for Android with secure connect, you need the LINUX (3.0.x or later, 32-bit version) package. To verify the current package, on the ASA, in the left pane, choose **Network (Client)** > **AnyConnect Client Settings**.

File	To obtain this file, see
	If the package is absent or out of date, download the latest Cisco AnyConnect VPN client software package from http://www.cisco.com/cisco/software/navigator.html.

Related Topics

Install Cisco Options Package file for devices, on page 7
Verify device COP file version, on page 8
Obtain Cisco Options Package file for dial rules, on page 10

Install Cisco Options Package file for devices

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

Note To upgrade your Cisco Unified Communications Manager to Release 8.6, you must first install the latest COP file to your earlier release of Cisco Unified Communications Manager. To verify if you have the correct COP file, see Verify device COP file version.

After you upgrade your Unified CM, you may need to re-install the COP file.

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

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.

Procedure

Step 1 Download the device COP file.

a) Locate the device COP file.
See Required files, on page 6.
b) Click **Download Now**.
c) Note the MD5 checksum.
You will need this later.
d) Click **Proceed With Download** and follow the instructions.

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

Step 3 Install this COP file on the Publisher server in your Unified CM cluster:

a) From the Navigation list box in the top-right corner of the Cisco Unified Communications Manager Administration portal, choose Cisco Unified OS Administration and 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 Cisco Unified Communications Manager at a time of low usage.
j) Restart the Cisco Tomcat service on the Cisco Unified Communications Manager server.
This step is required for the device icon to display properly on the device list page in Cisco Unified Communications Manager. This step clears the Tomcat image cache.

k) Enter the following command from the CLI:

```
utils service restart Cisco Tomcat
```

l) Let the system fully return to service.

Note To avoid interruptions in service, make sure 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 used for the Publisher, including rebooting the server.

Verify device COP file version

Use this procedure to verify if the correct version of the device COP file is already installed on your release of Unified CM.

Procedure

Step 1 Sign in to Cisco Unified Communications Manager Administration.

Step 2 Choose **Device** > **Phone**.

Step 3 Click **Add New**.

Step 4 From the Phone Type drop-down list, choose **Cisco Dual Mode for Android**.

Step 5 Scroll down to the Product Specific Configuration Layout area, and verify that you can see the Enable Secure Connect setting.
If you can see the Enable Secure Connect setting, the COP file is already installed on your system.

Dial rules setup

Application Dial Rules

Because people are accustomed to dialing numbers differently from a mobile device than from a desk phone, consider setting up Unified CM to accommodate the different number patterns that mobile device users will 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 only to users of Cisco Jabber or so that different rules apply to devices in different countries or area codes.

For example, users may dial numbers as follows:

- 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 than the desk phone number, users may dial area codes when using their mobile device when they would not include the area code when dialing from office 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 that are dialed to the type of numbers above.

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 Cisco Jabber and not to all applications that use the XML files to access dial rules, you can enter them manually as XML text directly into the file that makes the rules available to Cisco Jabber. You will generate this file in a procedure later in this section.

Use of dial rules with Cisco Jabber

Perform this series of procedures to make all of your existing dial rules available to Cisco Jabber.

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

You will use a Cisco Options Package (COP) file that is also used for this purpose for other Cisco products.

Note This COP file is different from the device COP file that is described elsewhere in this document.

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 Cisco Jabber than you need for other clients that use this file, use the optional procedure to copy and modify the XML file to create a dedicated file for Cisco Jabber.

If you have deployed other Cisco telephony clients and integrations, you may have performed this series of procedures already.

Note Every time you update the dial rules on Unified CM, you must repeat this series of procedures to make the changes available to clients, including Cisco Jabber.

Perform the following procedures in order

1 Obtain Cisco Options Package file for dial rules, on page 10

2 Copy dial rules, on page 10

3 Locate copy of dial rules, on page 11

4 Modify dial rules, on page 11

5 Restart TFTP service, on page 13

Obtain Cisco Options Package file for dial rules

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

You will use a Cisco Options Package (COP) file that is also used for this purpose for other Cisco products.

Note The COP file described in this procedure is different from the device COP file that is used to install the Jabber application.

Procedure

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.

Note Cisco Jabber for Android uses the same COP file as Cisco UC Integration for Microsoft Office Communicator to make Application Dial Rules available.

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 Click **Download Now**.

Step 5 Follow 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.

Copy dial rules

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

Create copies of dial rules in the Unified CM application with the following steps:

Procedure

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

Step 2 In the top-right corner of the **Unified CM Administration** portal, choose Cisco Unified OS Administration and select **Go**.

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

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

Step 5 Select **Next**.

Step 6 From 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 a TFTP server.

Locate copy of dial rules

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

Procedure

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

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

Step 3 Verify that the dial rules are present.

Example:

- `AppDialRules.xml`

Modify dial rules

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

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

- You may require rules that are unique to Cisco Jabber and are not used for other clients.
- You may need to create multiple files and assign different rules to the Cisco Jabber 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

- Using the guidelines in Application Dial Rules, on page 8, determine the Application Dial Rules you need.
- 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*.

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

Procedure

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.

Example:

Using the built-in TFTP client on a PC or Mac, enter the following commands:

```
tftp server-name
get CUPC/AppDialRules.xml
```

Step 3 Rename the file as needed.

Example:

For 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.

Important Note the path and filename. You will need this information later.

a) From the drop-down list at the top-right of the window, select **Cisco Unified OS Administration**.

b) Select **Software Upgrade** > **TFTP File Management**.

c) Select the file on your hard drive.

d) Specify the folder on the TFTP server.
For example, ciscojabber.

e) Select **Upload**.

Step 8 Repeat for any other rules files that you need 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 earlier and you want Cisco Jabber 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.

Restart 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.

Procedure

Step 1 In the top-right corner of the Unified CM Administration portal, choose **Cisco Unified Serviceability** and select **Go**.

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

Step 3 Choose 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.

Increase SIP Dual Mode Alert Timer Value

Increase the SIP Dual Mode Alert Timer to ensure that calls to the Cisco Jabber extension are not prematurely routed to the mobile-network phone number.

Before You Begin

Cisco Jabber must be running to receive VoIP calls.

Procedure

Step 1 Sign in to Cisco Unified Communications Manager Administration.

Step 2 Select **System** > **Service Parameters**.

Step 3 Select the server.

Step 4 Select the **Cisco CallManager (Active)** service.

Step 5 Scroll to the **Clusterwide Parameters (System - Mobility)** section.

Step 6 Increase the SIP Dual Mode Alert Timer to 4500 milliseconds.

Step 7 Select **Save**.

Note If after you increase the SIP Dual Mode Alert Timer, incoming calls still arrive in Cisco Jabber, and are terminated and diverted using Mobile Connect, you can increase the SIP Dual Mode Alert Timer value. The 4500 millisecond value is the lowest recommended value.

Create dedicated SIP Profile

Create a dedicated SIP Profile that allows Cisco Jabber to stay connected to Cisco Unified Communications Manager while Cisco Jabber is running in the background.

Procedure

Step 1 In Cisco Unified Communications Manager, select **Device** > **Device Settings** > **SIP Profile**.

Step 2 Create a new SIP profile, or copy an existing SIP profile.

Step 3 In the new SIP profile, set the following values:

- **Timer Register Delta** to 30
- **Timer Register Expires** to 660
- **Timer Keep Alive Expires** to 660
- **Timer Subscribe Expires** to 660
- **Timer Subscribe Delta** to 15

Step 4 Save the changes.

Step 5 Navigate to **Device** > **Phone** and select the device that you want to configure.

Step 6 In the **Protocol Specific Information** section, change the SIP profile to the profile you just created.

Step 7 Select **Save** and then **Apply**.

Step 8 Click **OK**.

What to Do Next

Select this SIP Profile for all Cisco Dual-Mode for Android devices that are running Cisco Jabber.

System-level prerequisites

Make sure your system meets the following prerequisites:

- Standard SIP and phone features such as the following are set up and working independently of Cisco Jabber:
  - Music on hold
  - Music for network hold
- Midcall features including:
  - Hold/resume
  - Call waiting
  - Add a call

  - Conference call
  - Transfer
  - The ability to handle RFC 2833, Key Press Markup Language (KPML), and dual-tone multifrequency (DTMF) tones for IVR call routing allowing users to use the keypad to route to the correct extension or department.

- Conferencing calls using software-based conference bridges requires G.711 for all participating endpoints. Hardware-based conference bridges that use digital signal processing (DSP) on a Cisco router allow for G.729 conference participants without the use of a transcoder.

Usage and error tracking

Cisco Jabber 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. This functionality is not currently available as a reporting tool for administrators.

You can enable or disable usage reporting for each user when you set up each Cisco Jabber 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 Cisco Jabber (for example, how often users view their list of voice messages) • Feature activity (for example, how often users add a contact) • IP address of the TFTP server to which Cisco Jabber connects • Approximate geographic location, based on mobile service provider activity
Detailed	• Same information collected when “Enabled” is selected.
Disabled	None

The first time users launch Cisco Jabber, they see an agreement that describes the data that Cisco collects. Users must accept this agreement to use the application, whether or not the usage tracking feature is currently enabled.

For more information about the reporting tool, see:

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

CHAPTER 3

Administration

Set up Cisco Jabber

Perform this series of procedures to set up all your Cisco Jabber features on your Unified CM, and then provide users with instructions for setting up Cisco Jabber on their devices.

Perform the following procedures in order

1. Add a test device with basic telephony features.

   See Add user device.

2. Set up any additional features on your test device. These features are optional.

   See Feature setup.

3. After you verify that all features work on your test device, set up individual users and devices in bulk.

   See Bulk configuration.

4. Provide users with instructions for setting up their Cisco Jabber clients.

   See User instructions.

Add user device

Before You Begin

- Set up and test voicemail for the extension you will assign to this device, following standard procedures for any device. Make sure you set up the voicemail number as a regular phone number so users can call in to the voicemail system using an Enterprise VoIP or mobile call.
- Verify that the Device Pool that you will assign to the Cisco Jabber device is associated with a region that includes support for the G.711 codec.
- Determine whether you want to enable or disable usage and error tracking for each user. For information, see Usage and error tracking, on page 15.

Procedure

Step 1 Sign in to Cisco Unified Communications Manager Administration.

Step 2 Add a new phone device with Cisco Dual Mode for Android as the Phone Type.

Step 3 Enter settings for **Device-Specific Information**.
Restrictions and requirements that are not specific to Cisco Jabber may apply to these values. If you require additional information about any option on the device configuration page, see the online help in Cisco Unified Communications Manager.

a) Enter the Device Name
The Device Name:

- Must start with BOT
- Must be uppercase
- Can contain up to 15 characters
- Can include only the following characters: A to Z, 0 to 9, dash (-), or underscore (_)

We recommend that the device name include the username of the user so it is easily remembered.

Example:
For example the device name of user jsmith would be BOTJSMITH.

b) Choose Standard Dual Mode for Android for the Phone Button Template.

c) Configure the following settings to prevent confusion for the person the user calls.

- Media Resource Group List
- User Hold MOH Audio Source
- Network Hold MOH Audio Source

These settings are not specific to this device. For information, see the Cisco Unified Communications Manager documentation.

d) Choose desk phone as the Primary Phone if the user has a desk phone.

Step 4 Enter settings for **Protocol Specific Information**.

a) In the **Device Security Profile** drop-down list, select **Cisco Dual Mode for Android - Standard SIP Non-Secure Profile**.

b) In the **SIP Profile** drop-down list, select the appropriate SIP profile.
See Create dedicated SIP Profile.

Values that are not described in this document are not specific to Cisco Jabber but may need to be entered for the device to work properly.

Step 5 Enter settings for the Product Specific Configuration Layout section.

a) Select the appropriate level of usage tracking in the Cisco Usage and Error Tracking drop-down list.
See Usage and error tracking, on page 15.

b) In the Application Dial Rules URL field:

- For Cisco Unified Communications Manager Release 8.6 and later, leave this field blank.
- If you are using Cisco Unified Communications Manager Release 8.5 or earlier and you want Cisco Jabber devices to apply Application Dial Rules, you must specify the path to these dial rules files, including the filenames.

  Use the following format: `tftp://`*`ip address of TFTP server/pathname to the XML file/XML filename`*

c) If your directory server requires authentication, enter LDAP username and password; otherwise leave these fields blank.
These credentials can be for a single read-only account for all users. These credentials are sent to the client in clear text in the TFTP file. Therefore, we strongly recommend that LDAP directory administrators generate a directory query account that has no other rights. Create this account with a value that is low enough to ensure that its credentials are semi-public (available to anyone on the local network).

d) Enter any designated emergency numbers in the Emergency Numbers field.
You can enter a comma-separated list of additional emergency numbers that will always be dialed direct for this user. These numbers must contain only numerical digits. No spaces, dashes, or other characters are permitted.

Emergency numbers as defined on the device are always dialed direct using the mobile network (never dialed using Enterprise VoIP) to allow the location of the caller to be sent automatically to emergency services personnel where this service is available. Direct-dial numbers can be useful for users who frequently travel to countries other than the country of their mobile network provider, if the emergency number differs depending on the users' location, or if your company has a dedicated security number.

e) Enter your domain in the Domain Name field if the Cisco Unified Communications Manager setting in **System** > **Server** is a hostname that does not include the domain name.

Example:

```
cisco.com
```

f) Enter a list of up to three SSIDs separated by forward slashes (/) in the Preset Wi-Fi Networks field.
Cisco Jabber attempts to connect to Cisco Unified Communications Manager only after the mobile device is connected to an SSID that you list here, or one that the user selects in the client. Cisco Jabber must be able to reach Cisco Unified Communications Manager when it is connected to these SSIDs. Typically, these are your corporate Wi-Fi SSIDs. SSIDs can be up to 32 characters long and are case-sensitive.

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.
This can be a new DN; a desk phone with the same DN is not required.

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

a) Forward Unregistered Internal
b) Forward Unregistered External

For more information about these settings, see the online help in Cisco Unified Communications Manager for the Forward All and other settings.

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

Step 12 Select **Save**.

Step 13 Navigate to the **End User** page for the user.

Step 14 Associate the Cisco Dual Mode for Android device that you just created for this user.
The device should now appear in the Controlled Devices box in either the Device Information or Device Associations section (depending on your release of Unified CM).

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 that your configuration works:

- Make sure the mobile device is connected to the corporate network. Verify that you can access a web page on your corporate intranet using the browser on your device.
- Launch Cisco Jabber and complete the setup wizard. Enter the IP address of your TFTP server (generally the IP address of your Cisco Unified Communications Manager server) and the Device Name (BOTXXXX) of the device you just added.
- Wait for a notice that the device is registered. The Cisco Jabber icon in the status bar turns black when the device is connected to Cisco Unified Communications Manager.
- Test basic telephony features in Cisco Jabber, such as the ability to make, hold, and transfer calls.

Changes to user device

If you change settings on the Cisco Unified CM Administration pages (for example, LDAP, call control, dial plan), Cisco Jabber reregisters after you click Save and then click Apply Config. The application reregisters again 30 seconds later. If the user is on a call when the application reregisters, the call drops and the application restarts automatically.

If the device is out of coverage at the time you apply the changes, it is updated when it reregisters to Cisco Unified Communications Manager.

If you delete the device from Cisco Unified Communications Manager, Cisco Jabber drops any active calls and after several reregister attempts the user receives an error message that it cannot connect. Client information is not erased from the device. To remove all client information (for example, if the employee leaves the company), use the appropriate device management solution, such as Active Sync.

To delete a device, see the "Deleting a Phone" topic in the *Cisco Unified Communications Manager Administration Guide* for your release at

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

Bulk configuration

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

Note The settings in the Product Specific Configuration Layout section of the device configuration page are not handled as individual columns in the exported spreadsheet. Instead, all of those settings, and the information they contain, appear as XML code in a single cell for each device. If you edit user-specific information in this cell, do so cautiously.

User instructions

After you finish setting up devices in Cisco Unified Communications Manager, give your users the following information:

- Instructions for connecting the mobile device to the corporate Wi-Fi. This process is independent of Cisco Jabber.
- User documentation with instructions for setting up Cisco Jabber, available from http://www.cisco.com/en/US/partner/products/ps11678/products_user_guide_list.html.

  Note Users must perform the initial setup of Cisco Jabber for Android within the corporate network.

- Direction to download and install Cisco Jabber from the Android Market.
- The device name of their Cisco Dual Mode for Android device, for example BOTJSMITH.
- The IP address of the TFTP server.
- The email address to which users should send problem reports (troubleshooting logs).
- (If applicable) Credentials required to access the corporate directory. The username should be in the format userid@company.com or the full DN format, cn=userid,ou=organization,dc=company,dc=com.

- (If applicable) Information required to access the corporate network remotely, using the secure connect feature. This information includes information such as the gateway address, group names, user ID, and if applicable, user password.

CHAPTER 4

Feature setup

Add Mobile Connect and Mobile Identity

Mobile Connect, formerly known as Single Number Reach (SNR), allows the native mobile phone number to ring when someone calls the office number while Cisco Jabber is not available.

When Cisco Jabber is running and connected to the corporate network, and thus available to receive VoIP calls, Mobile Connect is automatically inactivated.

A Mobile Identity is required to transfer calls from VoIP in Cisco Jabber to the mobile network.

Procedure

Step 1 Sign in to Cisco Unified Communications Manager Administration.

Step 2 Search for and delete any existing Remote Destination or Mobile Identity that is already set up with the mobile phone number.

Step 3 Navigate to the **End User** page for the user.

a) Check the **Enable Mobility** check box.

b) Specify the Primary User Device.

c) Select **Save**.

Step 4 Navigate to the device page for the Cisco Dual Mode mobile device settings.

a) Enter information:

Example:

Setting	Information
Softkey Template	Choose a softkey template that includes the Mobility button.
Mobility User ID	Select the user.
Owner User ID	Select the user. The value should match the Mobility User ID.
Rerouting Calling Search Space	If your Unified CM has custom partitions and multiple calling search spaces, select a Rerouting Calling Search Space that includes the partition that applies to the mobile phone number, which you will enter as a Mobile Identity.

b) Select **Save**.

Step 5 Add a new Mobile Identity for the mobile phone number:

a) Navigate to the device page for the Cisco Dual Mode mobile device settings.

b) Select **Add a New Mobile Identity**.

c) Enter the mobile phone number as the Destination Number.
This number must be routable to an outbound gateway. Generally, it will be the full E.164 number.

d) Enter initial values for call timers.
These values ensure that calls are not routed to the native device voicemail before they ring in the client on the mobile device.

For more information, see the online help in Unified CM.

Example:

Setting	Suggested initial value
Answer Too Soon Timer	3000
Answer Too Late Timer	20000
Delay Before Ringing Timer	0 This value accommodates the relatively long call-setup times that are characteristic of mobile calls.

e) Check the **Enable Mobile Connect** check box.

f) Set up the schedule for routing calls to the mobile number.

g) Select **Save**.

What to Do Next

Test your settings:

- Exit Cisco Jabber on the mobile device. For instructions, see the *FAQs* for users at http://www.cisco.com/en/US/partner/products/ps11678/products_user_guide_list.html.

- Call the Cisco Jabber extension from another phone.

The native mobile network phone number should ring and the call should connect when you answer it.

Enable active call transfer from VoIP to mobile network

Users can transfer an active VoIP call from Cisco Jabber to their mobile phone number on the mobile network. This feature is useful when a user on a call leaves the Wi-Fi (for example, leaving the building to walk out to the car), or if there are voice quality issues over the Wi-Fi. This Cisco Jabber feature is called Use mobile network.

- For system-level settings, check that the Mobility softkey appears when the phone is in the connected and on-hook call states.
  a) Sign in to Cisco Unified Communications Manager Administration.
  b) Select **Device** > **Device Settings** > **Softkey Template**.
  c) Select the softkey template that you selected when you configured the device for Mobile Connect.
  d) In the **Related Links** drop-down list at the upper right, choose **Configure Softkey Layout** and select **Go**.
  e) In the call state drop-down list, select the Connected state and verify that the Mobility key is in the list of selected softkeys, and then do the same for the On Hook state.
- For the per-user and per-device settings in Cisco Unified Communications Manager, set the specific device to use the Mobility softkey when transferring calls to the mobile voice network. Ensure that you have set up both Mobile Identity and Mobile Connect for the mobile device. After the transfer feature is working, users can enable and disable Mobile Connect at their convenience without affecting the feature.
  a) Sign in to Cisco Unified Communications Manager Administration.
  b) Select the Owner User ID on the **Phone Configuration** screen for your Cisco Dual Mode for Android device.
  c) Select the Mobility User ID.
     The value should match that of the Owner User ID.
  d) In the Product Specific Configuration Layout section, in the **Transfer to Mobile Network** drop-down list, choose **Use Mobility Softkey**.

What to Do Next

Test your settings: transfer an active call from VoIP to the mobile network.

Related Topics

Add Mobile Connect and Mobile Identity, on page 23

Add user device, on page 18

Enable active call transfer from desk phone to mobile device

Before You Begin

- Ensure that you configured the desk phone and the Cisco Dual Mode for Android (BOTXXXX) device.

- Ensure that you configured the Mobile Connect feature on the BOTXXXX device. See Add Mobile Connect and Mobile Identity.

Procedure

Step 1 Sign in to Cisco Unified Communications Manager Administration.

Step 2 Navigate to the **Phone Configuration** screen for the BOTXXXX device.

Step 3 In the Device Information section, note the value of the Mobility User ID.

Step 4 Navigate to the **Phone Configuration** screen for the associated desk phone.

Step 5 In the Device Information section, ensure that the value of the Owner User ID of the desk phone matches the value for the Mobility User ID of the BOTXXXX device.

Step 6 In the Device Information section, from the **Softkey Template** drop-down list, choose **Mobility**.

Note If you do not see the Mobility option, you must configure the Mobility softkey. See the “Mobility Softkey Configuration” section in the “Cisco Unified Mobility” chapter of *Cisco Unified Communications Manager Features and Services Guide, Release 7.0* at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/7_0_1/ccmfeat/fsmobmgr.html#wp1124994.

What to Do Next

Test your settings. The procedure for moving the call to your mobile device may vary depending on your desk phone model. A sample procedure is as follows:

1. Press the **Mobility** softkey on your desk phone.
   You may need to press **More** a few times before you see the **Mobility** softkey.
2. Select **Send call to Mobile**.
3. Answer your call on your mobile device.

Related Topics

Add Mobile Connect and Mobile Identity, on page 23
Add user device, on page 18

Set up secure connect

Secure connect is a feature that allows Cisco Jabber to securely connect to your corporate network from a remote location, using Wi-Fi or mobile data networks.

Note Cisco does not guarantee the voice quality on non-corporate Wi-Fi networks or mobile data networks.

Set up secure connect with the following procedures:

1. Install and set up the Cisco Adaptive Security Appliance (ASA). See Install and set up the Cisco Adaptive Security Appliance.
2. Set up the ASA for secure connect. See Set up the ASA for secure connect.

3 Set up the Unified CM for secure connect. See Set up Unified CM to use secure connect.

Install and set up the Cisco Adaptive Security Appliance

You must install and set up a Cisco Adaptive Security Appliance (ASA).

For supported Cisco Adaptive Security Appliance models, see the Release Notes at http://www.cisco.com/en/US/products/ps11678/prod_release_notes_list.html.

Install and set up your Cisco ASA using one of the following methods:

- For instructions for using Cisco Adaptive Security Device Manager (ASDM) software utility, see http://www.cisco.com/en/US/docs/security/asa/asa84/asdm64/configuration_guide/access_certs.html.
- For CLI instructions, see http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/access_certs.html#wp1125252.

Note To support secure connect, you must have an ASA license with the AnyConnect feature enabled.

Set up the ASA for secure connect

The following procedures describe one method for setting up the ASA for secure connect. This information is provided as a reference; the setup in your organization may be different.

1 Create an identity certificate. See Create an identity certificate.

2 Set up the system for the authentication required by your organization.

For certificate-based authentication, see Set up the system for secure connect using certificate-based authentication.

For password-based authentication using AAA (authentication, authorization, and accounting), see Set up the ASA for secure connect using AAA authentication.

Create an identity certificate

Use this procedure to create an identity certificate on the ASA that allows users to use SSL VPN.

Procedure

Step 1 On the ASDM, in the left pane, choose **Certificate Management > Identify Certificates**.

Step 2 Click **Add**.

Step 3 In the **Trustpoint Name** field, enter a name for the trustpoint.

Step 4 Select the **Add a new identity certificate** radio button.

Step 5 In the **Certificate Subject DN** field, enter CN=<*fully qualified domain name*>.

Step 6 (Optional) Check the **Generate self-signed certificate** check box.

You can also use a certificate that is signed by an external CA instead of a self-signed certificate. For more information about using certificates that are signed by an external CA, see the “Configuring Digital Certificates” chapter at http://www.cisco.com/en/US/docs/security/asa/asa84/asdm64/configuration_guide/access_certs.html.

Step 7 (Optional) Check the **Act as local certificate authority and issue dynamic certificates to TLS-Proxy** check box.

Step 8 Click **Add Certificate**.

Step 9 Click **OK**.

Set up the system for secure connect using certificate-based authentication

Perform the following procedures to set up the system for Cisco Jabber with secure connect using certificate-based authentication.

1. Install and set up a certificate authority.
2. Set up the ASA for secure connect and certificate-based authentication.

Install and set up a certificate authority

If your organization requires certificate-based authentication, you must set up a Certificate Authority (CA) to provide the certificates that the system uses for authentication.

We recommend that you create a root CA and then create subordinate CAs. Start with a self-signed certificate.

Cisco Jabber supports Cisco IOS Certificate Server and Microsoft Windows Server 2008 Enterprise Certificate Authority.

For Certificate Authority requirements, see the Release Notes at http://www.cisco.com/en/US/products/ps11678/prod_release_notes_list.html.

Cisco IOS certificate server

To set up a Cisco IOS Certificate Authority Server, see http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_ioscs.html.

Microsoft Windows Server 2008 Enterprise Certificate Authority

Use this procedure to create a Microsoft Windows Server 2008 Enterprise Certificate Authority that is customized for Cisco Jabber with secure connect using certificate-based authentication.

Procedure

Step 1 See the Microsoft documentation to install and set up the Certificate Authority.

Step 2 Create the SCEP template.

Step 3 Set the default template.

Step 4 Disable the SCEP challenge password.

Create the SCEP template

Use this procedure to add a new certificate template that supports both IPsec and SSL.

The default certificate for Microsoft Windows Server 2008 Enterprise Certificate Authority supports only IPsec because of the limited Extended Key Usage. You must modify this certificate template to ensure that the system can issue certificates for both IPsec and SSL.

Procedure

Step 1 On the Microsoft Windows Server 2008 server, choose **Start** > **Administrative Tools** > **Server Manager**.

Step 2 In the Server Manager window, in the left pane, navigate to Roles\Certificate Services\<*Name of your Certificate Authority*> OR Roles\Active Directory Certificate Services\<*Name of your Certificate Authority*>.

Step 3 Right-click the **Certificate Templates** folder and choose **Manage.**

Step 4 In the Certificate Templates Console window, right-click the **User** template and then choose **Duplicate Template**.

Step 5 In the Duplicate Template dialog box, click the **Windows Server 2008, Enterprise Edition** radio button.

Step 6 Click **OK**.

Step 7 In the Properties of New Template dialog box, in the General tab, in Template display name field, enter a descriptive name for the template (for example: `NDES-IPsec-SSL`).

Step 8 In the Validity period fields, enter a validity period for the template.
We recommend a validity period that is greater than three years to ensure that the certificate does not expire.

Step 9 Click the **Cryptography** tab.

Step 10 In the Minimum key size field, enter 512.

Step 11 Click the **Subject Name** tab.

Step 12 Click the **Supply in Request** radio button.

Step 13 If the application displays a warning, click **OK**.

Step 14 Click the **Extensions** tab.

Step 15 To make the certificates valid for both SSL and IPsec, in the Extensions included in this template section, click **Application Policies**.

Step 16 In the Description of Application Policies section, verify that the list includes the following policies at a minimum:

- Client Authentication
- IP security IKE intermediate
- IP security tunnel termination
- IP security user

Step 17 If you need to add policies:

a) Click **Application Policies** > **Edit**.
b) Click **Add**.
c) In the Add Application Policy dialog box, in the Application policies section, right-click the application policies you want to add.
d) Click **OK**.

e) In the Edit Application Policies Extension dialog box, verify your application policies and click **OK**.

Step 18 In the Properties of New Template dialog box, click **Apply**.

Step 19 Click **OK**.

Step 20 Close the Certificate Templates Console window.

Step 21 In the Server Manager window, right-click the **Certificate Templates** folder and choose **New** > **Certificate Template to Issue**.

Step 22 To enable the CA to use your new template, in the Enable Certificate Templates window, click the name of the new template that you created in the previous steps, and then click **OK**.

Set the default template

Use this procedure to set the certificate template that supports either IPsec or SSL as the default template.

Procedure

Step 1 On the Microsoft Windows Server 2008 server, choose **Start** > **Run**.

Step 2 In the **Open** field, enter **regedit**.

Step 3 Click **OK**.

Step 4 In the Registry Editor window, in the left pane, navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP.

Step 5 In the right pane, double-click the EncryptionTemplate key.

Step 6 In the **Value data** field, enter the name of the new certificate template you created in Step 7 of Create the SCEP template.

Step 7 Click **OK**.

Step 8 Repeat Steps 5 to 7 for both the GeneralPurposeTemplate and SignatureTemplate keys.

Step 9 Save and reboot the CA.

Disable the SCEP challenge password

Use this procedure to disable the SCEP challenge password so clients are not required to obtain the out-of-band password before SCEP enrollment.

Procedure

Step 1 On the Microsoft Windows Server 2008 server, choose **Start** > **Run**.

Step 2 In the **Open** field, enter **regedit**.

Step 3 Click **OK**.

Step 4 In the Registry Editor window, in the left pane, navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword.

Step 5 If you do not see the EnforcePassword key, right-click in the right pane, choose **New** > **DWORD (32-bit) Value**, and name the key EnforcePassword.

Step 6 In the right pane, click the EnforcePassword key.

Step 7 In the Edit DWORD dialog box, in the **Value data** field, enter **0** to disable the SCEP challenge password.

Step 8 Click **OK**.

Step 9 Exit regedit.

Step 10 Save and reboot the CA.

Set up the ASA for secure connect and certificate-based authentication

We recommend that you use this authentication method with the SCEP certificate enrollment scheme because it provides strong security and usability. Deployment for this method requires a Cisco ASA 5500 Series Adaptive Security Appliance (ASA) and a Certificate Authority (CA).

After you set up the CA, perform the following tasks on the ASA:

1. Set up an AnyConnect connection profile for SCEP enrollment
2. Add the certificate authority to the trustpoint
3. Set up the Dynamic Access Policy
4. Set up the AnyConnect client profile
5. Set up an AnyConnect connection profile for certificate authentication

Before You Begin

- Make sure your ASA software is Version 8.4.1 or later.
- Verify that the LINUX (3.0.x or later, 32-bit version) package is present by selecting **Network (Client)** > **AnyConnect Client Settings**.

  Look for a package that uses the following format: anyconnect-linux-3.0.xxxx-k9.pkg.

  If the package is absent or out of date, download the latest Cisco AnyConnect VPN client software package from http://www.cisco.com/cisco/software/navigator.html. Search for “AnyConnect Secure Mobility Client.”
- Verify that you have appropriate licenses before enabling secure connect on devices. The secure connect feature requires either AnyConnect Essentials licenses (minimum requirement) or AnyConnect Premium licenses.

Set up an AnyConnect connection profile for SCEP enrollment

Use this procedure to set up an AnyConnect connection profile (tunnel group) for Simple Certificate Enrollment Process (SCEP).

SCEP enrollment provides a scalable and secure means for Cisco Jabber users to create and download a personal or user certificate to use with secure connect. The certificate is a credential for authenticating secure connect sessions. Administrators can enter enrollment and secure connect values in the TFTP file to simplify the user experience when initiating certificate enrollment.

Procedure

Step 1 On the ASDM, in the left pane, choose **Network (Client) Access** > **AnyConnect Connection Profiles**.

Step 2 In the Connection Profiles section, add or choose the profile you want to set up as the SCEP group.

Step 3 Click **Edit** to open the Edit AnyConnect Connection Profile window for the selected profile.

Step 4 Choose the **Both** radio button for Authentication Method.

Step 5 In the **AAA Server Group** drop-down list, choose the server on which the user information is stored.

Step 6 In the Client Address Assignment section, choose the **None** radio button.

Step 7 In the Client Address Pools field, enter the pool you have associated with the profile.

Step 8 In the Default Group Policy section, enter a name for the Group Policy, and check the **Enable SSL VPN client protocol** check box.

Step 9 In the DNS Servers field, enter the IP address for the DNS server you want to use.

Step 10 In the Domain Name field, enter the domain name you want to use. For example, company.com.

Step 11 In the left pane, choose **Advanced** > **General**.

Step 12 Choose **Enable Simple Certificate Enrollment Protocol (SCEP)** for this Connection Profile.

Step 13 Choose **Network (Client) Access** > **Group Policies**.

Step 14 Choose the group policy you created.

Step 15 Click **Edit**.

Step 16 Ensure that **Inherit** is selected for Banner, Address Pools, and IPv6 Address Pools.

Step 17 In the SCEP forwarding URL, ensure that **Inherit** is not selected, and enter the address for the Certificate Authority.

Add the certificate authority to the trustpoint

Use this procedure to add the certificate authority to the trustpoint. Trustpoints let you manage and track CAs and certificates. A trustpoint is a representation of a CA or identity pair. A trustpoint includes the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate.

For automatic enrollment, a trustpoint must be configured with an enrollment URL, and the CA that the trustpoint represents must be available on the network and must support SCEP.

Procedure

Step 1 On the ASDM, choose **Certificate Management** > **CA Certificates**.

Step 2 Click **Add**.

Step 3 In the **Trustpoint Name** field, enter a name for the trustpoint.

Step 4 Choose the **Use SCEP** radio button.

Step 5 In the **SCEP URL: http//** field, enter the full SCEP enrollment URL.

Example:

- For Microsoft CA: http://<*ca-ip-or-name*>/certsrv/mscep/mscep.dll
- For other CAs: http://<*ca-ip-or-name*>/cgi-bin/pkiclient.exe

Step 6 Click **Install Certificate**.

Set up the Dynamic Access Policy

Set up a Dynamic Access Policy to support the SCEP proxy.

The system uses dynamic access policies to enforce rules of eligibility to enroll for a certificate.

Procedure

Step 1 On the ASDM, choose **Network (Client) Access** > **Dynamic Access Policies**.

Step 2 On the Configure Dynamic Access Policies window, click **Add** to create a new Dynamic Access Policy. For more information, see http://www.cisco.com/en/US/docs/security/asa/asa84/asdm64/configuration_guide/vpn_asdm_dap.html.

Step 3 In the AAA Attribute section, click **Add**.

Step 4 In the **AAA Attribute Type** drop-down list, select **Cisco**.

Step 5 Check the **SCEP Required** check box.

Step 6 Verify the operation and value drop-down lists are set to **= true**.

Step 7 Click **OK**.

Step 8 In the Advanced section, choose the **AND** radio button.

Step 9 In the **Logical Expression** field, enter EVAL(endpoint.device.id , “NE”, aaa.cisco.username2, “caseless”).

Set up the AnyConnect client profile

Use this procedure to specify the VPN connection attributes for client-based connections.

Procedure

Step 1 Create an AnyConnect client profile. For more information, see http://www.cisco.com/en/US/docs/security/asa/asa84/asdm64/configuration_guide/vpn_asdm_setup.html#wp1119491.

Step 2 Choose **Network (Client) Access** > **AnyConnect Client Profiles**.

Step 3 Highlight the AnyConnect client profile you just created.

Step 4 Click **Edit**.

Step 5 In the left pane, choose **Certificate Enrollment**.

Step 6 Check the **Certificate Enrollment** check box.

Step 7 In the **CA URL** field, enter the address for the SCEP Certificate Authority server.

Step 8 In the Certificate Contents section, in the **Name (CN)** field, enter %USER%.

Step 9 In the **Company (O)** field, enter your company name.

Step 10 Ensure that the **Display Get Certificate Button** check box is checked.

Step 11 In the left pane, choose **Server List**.

Step 12 In the right pane, click **Add**.

Step 13 In the **Host Display Name (Required)** field, enter the fully qualified domain name of the ASA gateway.

Step 14 In the **Primary Protocol** drop-down list, choose **SSL**.

Step 15 Click **OK**.

Set up an AnyConnect connection profile for certificate authentication

Use this procedure to create a connection profile (tunnel group) that enables users to authenticate with the certificate they obtain with the SCEP connection profile.

Procedure

Step 1 On the ASDM, configure an AnyConnect SSL VPN connection profile, using the AnyConnect VPN Wizard. To start the wizard, choose **Wizards** > **VPN Wizards** > **AnyConnect VPN Wizard**. For more information, see http://www.cisco.com/en/US/docs/security/asa/asa84/asdm64/configuration_guide/wizard_vpn.html#wp1052383.

a) For **VPN Protocols**, check **SSL** check box.

b) In the **Device Certificate** field, choose the trustpoint created in Create an identity certificate.

Step 2 Choose **Network (Client) Access** > **AnyConnect Connection Profiles**.

Step 3 Highlight the AnyConnect connection profile you just created.

Step 4 Click **Edit**.

Step 5 In the Authentication section, select the **Certificate** radio button for the Method.

Step 6 Click **OK**.

Step 7 Choose **Advanced** > **AnyConnect** > **Client** > **Dead Peer Detection**.

Step 8 For Gateway Side Detection, check the **Inherit** check box.

Step 9 For Client Side Detection, check the **Inherit** check box.

Step 10 Click **OK**.

Step 11 Choose **Advanced** > **AnyConnect Client**.

Step 12 For **Datagram TLS**:

a) Uncheck the **Inherit** check box.

b) Select the **Enable** radio button.

Step 13 Click **OK**.

Set up the ASA for secure connect using AAA authentication

Use the following procedures to set up the ASA for Cisco Jabber with secure connect using authentication, authorization, and accounting (AAA) to provide password-based authentication. Deployment for this method requires an ASA. If you are using one time passwords, each user requires a password generator.

Note We recommend deploying Cisco Jabber with secure connect using certificate-based authentication. The next preferred method is password-based authentication using AAA on RADIUS servers.

Set up secure connect with the following procedures:

1. Add a AAA server group to the ASA
2. Set up an AnyConnect connection profile for AAA authentication

Before You Begin

- Make sure your ASA software is Version 8.0 or later.
- Verify that the LINUX (3.0.x or later, 32-bit version) package is present by selecting **Network (Client)** > **AnyConnect Client Settings**. If the package is absent or out of date, download the latest Cisco AnyConnect VPN client software package from http://www.cisco.com/cisco/software/navigator.html.
- Verify you have enough licenses before enabling secure connect on devices. The secure connect feature requires either AnyConnect Essentials licenses (minimum requirement) or AnyConnect Premium licenses.

Add a AAA server group to the ASA

Use this procedure to add a AAA server group to your ASA that allows users to authenticate with either a one-time or static password.

For information about adding the AAA server group, see the procedure called “Configuring AAA Server Groups” at http://www.cisco.com/en/US/docs/security/asa/asa84/asdm64/configuration_guide/access_fwaaa.html.

For one-time password authentication, point to a AAA server that supports one-time password authentication.

For static password authentication, point to a AAA server that supports static passwords (either the local user database or another server that supports static passwords).

For detailed information about how to set up AAA authentication for network access, see http://www.cisco.com/en/US/docs/security/asa/asa84/asdm64/configuration_guide/access_fwaaa.html.

Set up an AnyConnect connection profile for AAA authentication

Use this procedure to create a connection profile (tunnel group) that enables users to authenticate with AAA using a one-time or static password.

Procedure

Step 1 On the ASDM, configure an AnyConnect SSL VPN connection profile, using the AnyConnect VPN Wizard. To start the wizard, choose **Wizards** > **VPN Wizards** > **AnyConnect VPN Wizard**. For more information, see http://www.cisco.com/en/US/docs/security/asa/asa84/asdm64/configuration_guide/wizard_vpn.html#wp1052383.

Step 2 For **VPN Protocols**:

a) Check the **SSL** check box.

b) In the **Device Certificate** field, choose the trustpoint created in Create an identity certificate.

Step 3 For **Client Images**, choose the LINUX (3.0.x or later, 32-bit version) package.
If the package is absent or out of date, download the latest Cisco AnyConnect VPN client software package from http://www.cisco.com/cisco/software/navigator.html.

Step 4 For **Authentication Methods**, choose the AAA Server Group created in Add a AAA server group to the ASA.

Set up Unified CM to use secure connect

Use this procedure to set up the Unified CM device to use the secure connect feature.

Procedure

Step 1 Sign in to Cisco Unified Communications Manager Administration.

Step 2 Choose **Device** > **Phone** to open or add the device on which you want to set up secure connect.

Step 3 In the Preset Wi-Fi Networks field, enter the SSIDs for Wi-Fi networks (SSIDs) that are approved by your organization. Separate SSIDs with a forward slash (/). Devices do not connect to secure connect if they are connected to one of the entered Wi-Fi networks.

Step 4 In the **Enable Secure Connect** list box, select **Enabled**.

Step 5 In the Secure Connect Gateway Address field, enter the IP address or hostname for the ASA gateway on which you set up SCEP or passwords.

Step 6 If using certificate-based authentication, in the Secure Connect Certificate Enrollment Group (SCEP) field for certificate-based authentication, enter the group you created on the ASA. For AAA (password-based) authentication, leave this field blank. This field is case sensitive.

Step 7 If using certificate-based authentication, in the Secure Connect Authentication Group field, enter the secure VPN tunnel group name to which the user signs in.

Step 8 In the Secure Connect Username field, enter the SCEP username for certificate-based authentication. For AAA (password-based) authentication, enter the authentication username.

Step 9 Click **Save**.

Step 10 Click **Apply Config**.

Step 11 Click **Reset**.

What to Do Next

Verify that your configuration works:

- On the Android phone, clear the Cisco Jabber data.
- Make sure the mobile device is connected to the corporate network. Verify that you can access a web page on your corporate intranet using the browser on your device.
- Within the corporate Wi-Fi network, launch Cisco Jabber and complete the setup wizard.
- Wait for a notice that the device is registered. The Cisco Jabber icon in the status bar turns black when the device is connected to Cisco Unified Communications Manager.
- Test the device from a noncorporate Wi-Fi network or mobile data network. Confirm the following:
    - You can connect to the corporate network.
    - Secure connect is connected.

      To verify your connection, in Cisco Jabber for Android, tap **Menu** > **Settings** > **Accounts** > **Secure Connect**. When you are connected, Cisco Jabber for Android displays the following text: “Connected over secure connect.”
    - The device is registered.
    - You can use the basic telephony features in Cisco Jabber (for example, you can make, hold, and transfer calls).

Enable Enhanced Message Waiting Indicator

A Message Waiting Indicator alerts users to the presence of new voice messages. Enhanced Message Waiting Indicator provides a count of unheard messages on systems that support this feature. Users can call the voice messaging system to retrieve the messages.

Note To enable the basic Message Waiting Indicator, follow the instructions in the Cisco Unified Communications Manager documentation for your release. There are no unique configurations for this client.

If your deployment supports Enhanced Message Waiting Indicator, enable this option in the **Cisco Unity Connection Administration** portal.

Procedure

Step 1 Sign in to Cisco Unified Communications Manager Administration.

Step 2 Select **Telephony Integrations**.

Step 3 Select **Phone System**.

Step 4 Select **Cisco Unified Communications Manager server**.

Step 5 Select **Send Message Counts**.

Specify directory search settings

Specify the settings that the client will use to connect to the directory server. When the user sets up the client, these settings will be automatically configured on the client.

Before You Begin

Identify attributes in your corporate directory schema that are different from, or additional to, the application defaults. You must map changed attributes later in this procedure.

Element	Element name	Default Active Directory attribute	Default attribute for all other LDAP servers	Your value, if different
Unique identifier	identifier	distinguishedName	distinguishedName	
Display name	displayName	displayName	cn	
Email address	emailAddress	mail	mail	
First name	firstName	givenName	givenName	
Last name	lastName	sn	sn	
User ID	userid	sAMAccountName	uid	

Element	Element name	Default Active Directory attribute	Default attribute for all other LDAP servers	Your value, if different
Main phone number	mainPhoneNumber	telephoneNumber	telephoneNumber	
Home phone number	homePhoneNumber			
Second home phone number	homePhoneNumber2			
Mobile phone number	mobilePhoneNumber			
Second mobile phone number	mobilePhoneNumber2			
Direct to voicemail phone number	voicemailPhoneNumber	voicemail		
Fax number	faxPhoneNumber	facsimileTelephoneNumber		
Other phone number	otherPhoneNumber			
Manager	manager	manager		
Direct reports	directReports	directReports		
Title	title	title		
Department	department	department		

Procedure

Step 1 Sign in to Cisco Unified Communications Manager Administration.

Step 2 Navigate to the Cisco Dual Mode device page for the user.

Step 3 Enter LDAP User Authentication settings.

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

Step 4 Enter LDAP server IP address or hostname.

- If you are not deploying Directory Search in Cisco Jabber, leave this field blank.

- Otherwise, enter the IP address or hostname, and port number of your directory server.

Use the format *YourDirectoryServer.YourCompany.com:portnumber*.

- If Global Catalog is enabled, use port 3269 for secure SSL connections and 3268 for nonsecure connections.
- If Global Catalog is not enabled, do not enter a port.

If you enter an IP address or hostname but do not enter a port, the client tries to connect to ports 389 or 636, depending on the SSL setting.

Step 5 Choose **Enabled** or **Disabled** as required by your directory server to enable LDAP SSL.

Step 6 Enter the LDAP Search Base using the format: *CN=users,DC=corp,DC=yourcompany,DC=com*.
By default, this application uses the search base 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.

Note 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 Enter the LDAP photo location. Enter the pathname to the image files on your HTTP server. Be sure to specify the correct graphics file type (for example, jpg or png). Use the variable %%*LDAP Attribute* %% to represent the LDAP attribute.

Example:

```
http://yourcompany.cisco.com/photo/std/%%userID%%.jpg
```

You must include the double percent symbols in the string.

Cisco Jabber will automatically resize the images as needed, but smaller images will be processed faster.

Your photos must be stored on an HTTP server, with filenames that are identical to the values in an LDAP directory attribute (excluding the filename extension).

By default, Cisco Jabber uses the attribute mapped to the **userid** element in the LDAP Field Mappings table that precedes this procedure. You can specify a different attribute in the LDAP Field Mappings field.

Example:
An image file from your directory is named `jsmith.jpg`, and the value in the cn attribute is jsmith. You have used the LDAP Field Mappings field to map the userid element to the cn attribute in your LDAP directory.

Step 9 Select **Save**.

Step 10 Restart Cisco Jabber.

What to Do Next

Test the directory search feature.

CHAPTER 5

Troubleshooting

The following list describes how to troubleshoot Cisco Jabber.

- For solutions that users can perform without administrator assistance, and for tips and tricks about how the application works, see the user *FAQs* at http://www.cisco.com/en/US/partner/products/ps11678/products_user_guide_list.html.
- See also the Release Notes for this product at http://www.cisco.com/en/US/partner/products/ps11678/prod_release_notes_list.html.
- Verify the status of the connection to each enterprise server directly from the mobile device.
- For features that are not unique to this product (for example, conferencing or transferring calls):
    - Test the feature on existing configured desk phones. If it works, compare the working device configuration to your Cisco Jabber device configuration.
    - Check the Cisco Unified Communications Manager documentation for troubleshooting tips. See http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_troubleshoot_and_alerts.html.
- Make sure you entered the correct IP addresses, ports, paths, usernames, and passwords. If you entered hostnames instead of IP addresses, enter the IP address instead.
- If users experience problems that you are unable to solve and you need to contact Cisco for support, have the users send you the client log files that capture the problem. See the following topic about obtaining logs from the client.

Verify connection status

Verify your connection status using your mobile device.

Procedure

Step 1 Tap Cisco Jabber icon to open application.

Step 2 Tap **Menu** > **Settings** > **Help** > **Troubleshooting** > **Connection Status**.

Connection status is displayed.

Connected	Feature is configured and connected properly.
Connecting	Feature is currently making a connection attempt.
Disconnected	Feature is configured but is not currently connected. You might not be properly connected to the Wi-Fi or the server might be down.
Error	Feature is not currently configured or connected. You might have entered an incorrect password.

Obtain logs from Cisco Jabber

Have the user follow this procedure to send you logs from Cisco Jabber.

We recommend that the email application be set up and working on the Android device.

Procedure

Step 1 Launch Cisco Jabber from your mobile device.

Step 2 Tap **Menu** > **Settings** > **Help** > **Troubleshooting**.

Step 3 Set Detailed Logging to On.

Step 4 Try to reproduce the problem to capture the details in the logs.

Step 5 Tap **Menu** > **Settings** > **Help** > **Troubleshooting** > **Problem Reporting**.

Step 6 Select Audio Engine Logs and Configuration Files.

Step 7 Tap **Email Problem Report**.
Your email application launches with a new message that contains a prepopulated subject line and message with the logs attached.

Step 8 Describe the problem in the body of the email message.

Step 9 Enter the email address that your administrator provided for problem reporting.

Step 10 Tap **Send**.

What to Do Next

Be sure the user sets Detailed Logging to Off when no longer needed.

Troubleshooting issues

Setup issues

Changes to dial rules do not take effect

Problem Changes to the Application Dial Rules or the Directory Lookup Rules in Unified CM are not taking effect.

Solution Run the COP file again to make the changes available to Cisco Jabber, and then restart the TFTP service. The updated rules will be available to Cisco Jabber the next time the user restarts the application. See Use of dial rules with Cisco Jabber, on page 9.

Cisco Jabber registration fails

Problem Cisco Jabber registration fails or times out.

Solution The following list describes different possible causes for and solutions to registration failure or timeout conditions:

- Have the user check the troubleshooting tips in the *FAQs* for users at http://www.cisco.com/en/US/partner/products/ps11678/products_user_guide_list.html.
- Verify that the mobile device can reach Cisco Unified Communications Manager: Try using the browser on the device to connect to the Cisco Unified Communications Manager Administration portal.
- If registration is rejected with error 503, go to the Cisco Dual Mode for Android device page in Cisco Unified Communications Manager and select Reset, and then try again.
- Make sure your DNS server can resolve the hostname of the Cisco Unified Communications Manager server that is used as the TFTP server address.
- Enter the IP address instead of the hostname of the Cisco Unified Communications Manager server into the TFTP Server Address setting in Cisco Jabber.
- If registration fails with the error message “Verification Timed Out,” you did not reboot all Cisco Unified Communications Manager servers in the cluster after you installed the device COP file. To resolve the error, reboot all Cisco Unified Communications Manager servers.
- Make sure you have enough licenses to accommodate your deployment.
- Have the user check that the device connects to the corporate Wi-Fi. If the Wi-Fi is a custom Wi-Fi and it is not checked on the Custom Wi-Fi Networks screen, Cisco Jabber will not try to register.
- If the value in **System** > **Server** in Cisco Unified Communications Manager is a hostname without a domain, enter your domain name in the **Domain Name** field in the **Cisco Dual Mode for Android** device page.
- If you set up your system with secure connect, see also Secure connect is not available.

Related Topics

Install Cisco Options Package file for devices, on page 7

Device icon is missing

Problem The device icon in the Unified CM Administration pages does not appear.

Solution Try the following:

1. Restart the Tomcat service as described in Install Cisco Options Package file for devices, on page 7.
2. Reload the device page in your browser.
3. Clear the browser cache if necessary.

Directory server handshake error

Problem When the client attempts to connect to the directory server, the connection fails with an SSL Handshake error.

Solution Change the Enable LDAP SSL setting on the device page in Cisco Unified Communications Manager and relaunch the application.

Unable to create Cisco Jabber device in Unified CM

Problem The user’s device type is not available as an option.

Solution Make sure that you uploaded the device COP file and restarted Unified CM. See Install Cisco Options Package file for devices, on page 7.

Device issues

Battery drains faster during Cisco Jabber calls

Problem The device battery seems to drain more quickly during Cisco Jabber calls than during standard mobile calls.

Solution VoIP calls may use slightly more battery power than standard mobile calls. For actions the user can take, see the FAQs for users at http://www.cisco.com/en/US/partner/products/ps11678/products_user_guide_list.html.

Cisco Jabber registration drops frequently

Problem Unified CM registration drops frequently when the user's device is idle.

Solution Verify the SIP Profile settings in Unified CM Administration. For more information, see Create dedicated SIP Profile.

Cannot complete calls

Problem Numbers that should be dialable cannot be connected. Users hear a network busy tone or error message.

Solution Try the following:

- If you made changes to the Application Dial Rules, make sure you ran the COP file to make the changes available to Cisco Jabber, and that you restarted the TFTP service.
- If you modified the dial rules and specified an alternate location for the dial rules in the Product Specific Configuration Layout section on the device page, make sure that you updated the custom file before you restarted the TFTP service.
- Make sure that you set the Call Forward Unregistered settings on the device page.

Calls incorrectly sent to voicemail

Problem Calls are routed directly to voicemail.

Solution In Unified CM, modify the call timer values on the Mobile Identity page. For more information see Add Mobile Connect and Mobile Identity, on page 23.

Calls are dropped or interrupted

Problem Calls are unexpectedly dropped or interrupted.

Solution Because network issues outside your enterprise are neither under the control of nor specific to Cisco Jabber, Cisco Technical Assistance Center (TAC) does not troubleshoot these issues. Try one of the following:

- For actions the user can take, see the FAQs for users at http://www.cisco.com/en/US/partner/products/ps11678/products_user_guide_list.html.
- If these problems are frequent, verify the SIP Profile settings in Unified CM Administration. For more information, see Create dedicated SIP Profile.
- If these problems are frequent while users are on the corporate premises, make sure your Wi-Fi meets the network requirements specified in the Release Notes at http://www.cisco.com/en/US/partner/products/ps11678/prod_release_notes_list.html.
- If you change settings on the Cisco Unified Communications Manager Administration pages and click **Save** and then click **Apply Config**, Cisco Jabber reregisters. The application reregisters again 30 seconds later. When Cisco Jabber reregisters, active calls are dropped and the application automatically restarts.

Related Topics

Changes to user device, on page 20

Limitations and restrictions, on page 2

Problems with voice quality

Problem Voice quality is poor.

Solution Voice quality cannot be guaranteed because of variable network conditions.

However:

- For actions the user can take, see the *FAQs* for users at http://www.cisco.com/en/US/partner/products/ps11678/products_user_guide_list.html.
- For general information about optimizing your corporate Wi-Fi network for voice transmission, see the "Network Requirements" section of the Release Notes for Cisco Jabber at http://www.cisco.com/en/US/partner/products/ps11678/prod_release_notes_list.html.

Note Because network issues outside your enterprise are neither under the control of nor specific to Cisco Jabber, the Cisco Technical Assistance Center (TAC) does not troubleshoot these issues.

Unable to move calls from the mobile network to Cisco Jabber

Problem User is unable to transfer a call from the mobile network to Cisco Jabber.

Solution Users can transfer calls to the mobile network from Cisco Jabber, but not in the other direction.

Unable to receive calls in Cisco Jabber

Problem An incoming call arrives briefly in Cisco Jabber while it is running, but then the call is terminated and diverted to the native mobile phone number using Mobile Connect instead.

Solution In Unified CM, set the SIP Dual Mode Alert Timer as described in Increase SIP Dual Mode Alert Timer Value, on page 13.

Unable to send calls to mobile device

Problem User cannot send an active call from Cisco Jabber to the mobile phone number.

Solution Try one of the following:

- Verify that Mobile Connect works by exiting Cisco Jabber and dialing the extension. If you hear a fast busy signal, make sure you entered the Mobility Identity phone number in a routable format.
- In Unified CM, adjust the call timers on the Mobile Identity page. See the online help in Unified CM for more information. Make sure that the No Answer Ring Duration on the Primary DN page is greater than the value you specified for Answer Too Late Timer on the Mobile Identity page.

Note The Answer Too Late Timer starts when Unified CM receives an acknowledgment from the mobile network that the call was accepted. Some mobile networks subsequently send a separate alert that the dialed number is ringing; in those cases, the Answer Too Late Timer restarts when Cisco Unified Communications Manager receives that alert.

To test this for a particular mobile device, dial the mobile phone number (the mobile network) from an office phone and track the amount of time that passes between the time you dial the last digit and the time the call goes to voicemail.

If you increase the No Answer Ring Duration, see related cautions for this setting in the online help in Unified CM.

Search issues

No directory search

Problem Directory search is not available.

Solution If you do not enter an IP address for a directory server in the device page in Cisco Unified Communications Manager, Cisco Jabber assumes your deployment does not include Directory Services. Enter this information, save and reset the device, and then relaunch Cisco Jabber.

Secure connect issues

Secure connect is not available

Problem User is performing initial setup of Cisco Jabber but cannot set up secure connect.

Solution Try one of the following:

- Make sure the user is located within the corporate Wi-Fi network during setup.
- Verify that you have proper AnyConnect licenses for the ASA. The secure connect feature requires either AnyConnect Essentials licenses (minimum requirement) or AnyConnect Premium licenses.
- Verify that you installed the correct Linux package on the ASA. To verify, open the Cisco Adaptive Security Device Manager (ADSM). In the left pane, choose **Network (Client)** > **AnyConnect Client Settings**, and confirm that you have the correct Linux package: 3.0.x or later, 32-bit version.
- If you set up the ASA to use SCEP, verify that the ASA software is Version 8.4.1 or later.
- In Cisco Unified CM Administration, check the Cisco Dual Mode device page to ensure that the Enable Secure Connect setting is enabled. If this setting is disabled, users do not see the secure connect feature.
- In Cisco Unified CM Administration, check the Cisco Dual Mode device page to ensure that you have entered the correct values in the secure connect settings. Ensure that you entered the correct address in the Secure Connect Server Address field.

Table 1: Unified CM secure connect settings

	For certificate-based authentication	For AAA authentication
Secure Connect Certificate Enrollment Group	required	empty
Secure Connect Authentication Group	required	required
Secure Connect Username	optional	optional

For more information about the secure connect settings, see Set up Unified CM to use secure connect.

Secure connect no longer connects

Problem User could previously connect to the corporate network using secure connect, but now cannot connect.

Solution Try one of the following:

- On the Cisco Jabber for Android device, verify that the user has set the correct group. If the user has a SCEP group, ensure that the user did not select the SCEP group instead of the authentication group.
- If the user is set up with one-time password authentication, ask the user to check whether the password is expired. When the password expires, the user sees an error message.
- If the user is set up with certificate-based authentication, check whether the certificate has expired.
- Check to see if the group name was changed. If so, the user should delete the previously configured connection and add a new connection. For information about deleting and adding a connection for secure connect, see http://www.cisco.com/en/US/products/ps7271/products_user_guide_list.html.
- Verify that the ASA license is still valid.
- Verify that the gateway is reachable.
- Verify that the user can connect to the corporate network.
- If the user performs initial setup of Cisco Jabber while the Android device is remotely connected to the corporate network using Cisco AnyConnect, Cisco Jabber adds the remote network to the Custom Wi-Fi Networks list. When your device is connected to a checked network on this list, secure connect does not launch. The user must uncheck the check box for the remote (non-corporate) network. To access the Custom Wi-Fi Networks list, go to the Cisco Jabber home screen and tap **Menu** > **Settings** > **General** > **Wi-Fi Networks** > **Custom Wi-Fi Networks**.