Configure Softphone

Create Softphones Workflow

Procedure

	Command or Action	Purpose
Step 1	Create and Configure Cisco Jabber Devices, on page 1	Create at least one device for every user who accesses Cisco Jabber. Generate an authentication string to provide to users.
Step 2	Add a directory number to the device, on page 5	For each device you create, add a directory number.
Step 3	Associate Users with Devices, on page 5	Associate users with devices.
Step 4	Create Mobile SIP Profiles, on page 6.	Complete this task if you have Cisco Unified Communications Manager release 9 and plan to configure devices for mobile clients.
Step 5	Configure the Phone Security Profile, on page 7	Complete this task to set up secure phone capabilities for all devices.

Create and Configure Cisco Jabber Devices

Create at least one device for every user that accesses Cisco Jabber. A user can have multiple devices.

Note Users can only remove participants from a conference call when using the softphone (CSF) device for calls.

Before you begin

- Install COP files.
- Create SIP profiles if you have Cisco Unified Communications Manager release 9 or earlier and plan to configure devices for mobile clients.
- Create the Phone Security Profile if you plan to set up secure phone capabilities for all devices.
- If you are using CAPF enrollment, for Cisco Unified Communications Manager release 10 or later, ensure that the Cisco Certificate Authority Proxy Function (CAPF) service parameters value for **Certificate Issuer to Endpoint** is **Cisco Certificate Authority Proxy Function**. This is the only option supported by Cisco Jabber. For information on configuring the CAPF service parameter see the *Update CAPF Service Parameters* topic in the Cisco Unified Communications Manager Security Guides.
- Before you create TCT devices, BOT devices, or TAB devices for Cisco Jabber for mobile users, specify the organization top domain name to support registration between Cisco Jabber and the Cisco Unified Communications Manager. In Unified CM Administration interface, select **System** > **Enterprise Parameters**. Under the Clusterwide Domain Configuration section, enter the organization top domain name. For example, cisco.com. This top domain name is used by Jabber as the DNS domain of the Cisco Unified Communications Manager servers for phone registration. For example, CUCMServer1@cisco.com.

Step 1 Log in to the **Cisco Unified CM Administration** interface.

Step 2 Select **Device** > **Phone**.
Find and List Phones window opens.

Step 3 Select **Add New**.

Step 4 From the **Phone Type** drop-down list, select the option that is applicable to the device type you are configuring and then select **Next**.

For Jabber users, you can only create one type of device per user although you can create multiple devices for each user. For example, you can create one tablet device and one CSF device but not two CSF devices.

- **Cisco Unified Client Services Framework**—Select this option to create a CSF device for Cisco Jabber for Mac or Cisco Jabber for Windows.
- **Cisco Dual Mode for iPhone**—Select this option to create a TCT device for an iPhone.
- **Cisco Jabber for Tablet**—Select this option to create a TAB device for an iPad or an Android tablet or for Chromebooks.
- **Cisco Dual Mode for Android**—Select this option to create a BOT device for an Android device.

Step 5 From the **Owner User ID** drop-down list, select the user for whom you want to create the device.

For the **Cisco Unified Client Services Framework** option in a Phone mode deployment, ensure that **User** is selected.

Step 6 In the **Device Name** field, use the applicable format to specify a name for the device:

If You Select	Required Format
Cisco Unified Client Services Framework	• Valid characters: a–z, A–Z, 0–9. • 15-character limit.

If You Select	Required Format
Cisco Dual Mode for iPhone	• The device name must begin with *TCT*. For example, if you create a TCT device for user, Tanya Adams, whose username is tadams, enter **TCTTADAMS**. • Must be uppercase. • Valid characters: A–Z, 0–9, period (.), underscore (_), hyphen (-). • 15-character limit.
Cisco Jabber for Tablet	• The device name must begin with *TAB*. For example, if you create a TAB device for user, Tanya Adams, whose username is tadams, enter **TABTADAMS**. • Must be uppercase. • Valid characters: A–Z, 0–9, period (.), underscore (_), hyphen (-). • 15-character limit.
Cisco Dual Mode for Android	• The device name must begin with *BOT*. For example, if you create a BOT device for user, Tanya Adams, whose username is tadams, enter **BOTTADAMS**. • Must be uppercase. • Valid characters: A–Z, 0–9, period (.), underscore (_), hyphen (-). • 15-character limit.

Step 7 If you are using CAPF enrollment, complete the following steps to generate an authentication string:

a. Users can use the authentication string that you can provide to access their devices and securely register to Cisco Unified Communications Manager, navigate to the **Certification Authority Proxy Function (CAPF) Information** section.

b. From the **Certificate Operation** drop-down list, select **Install/Upgrade**.

c. From the **Authentication Mode** drop-down list, select **By Authentication String** or **By Null String**. Using the CAPF Authentication mode **By Null String** with JVDI and Jabber for Windows CSF devices is not supported. It causes Jabber registration with Cisco Unified Communications Manager to fail.

d. Click **Generate String**. The Authentication String autopopulates with a string value. This is the string that you will provide to end users.

e. From the **Key Size (Bits)** drop-down list, select the same key size that you set in the phone security profile.

f. In the **Operation Completes By** fields, specify an expiration value for the authentication string or leave as default.

g. If you are using a group configuration file, specify it in the **Cisco Support Field** of the **Desktop Client Settings.** Cisco Jabber does not use any other settings that are available on the **Desktop Client Settings**.

Step 8 Select **Save**.

Step 9 Click **Apply Config**.

What to do next

Add a Directory Number to the device.

Provide Users with Authentication Strings

If you are using CAPF enrollment to configure secure phones, then you must provide users with authentication strings. Users must specify the authentication string in the client interface to access their devices and securely register with Cisco Unified Communications Manager.

When users enter the authentication string in the client interface, the CAPF enrollment process begins.

Note The time it takes for the enrollment process to complete can vary depending on the user's computer or mobile device and the current load for Cisco Unified Communications Manager. It can take up to one minute for the client to complete the CAPF enrollment process.

The client displays an error if:

- Users enter an incorrect authentication string.

  Users can attempt to enter authentication strings again to complete the CAPF enrollment. However, if a user continually enters an incorrect authentication string, the client might reject any string the user enters, even if the string is correct. In this case, you must generate a new authentication string on the user's device and then provide it to the user.

- Users do not enter the authentication string before the expiration time you set in the **Operation Completes By** field.

  In this case, you must generate a new authentication string on the user's device. The user must then enter that authentication string before the expiration time.

Important When you configure the end users in Cisco Unified Communications Manager, you must add them to the following user groups:

- **Standard CCM End Users**
- **Standard CTI Enabled**

Users must not belong to the Standard CTI Secure Connection user group.

Add a directory number to the device

After you create and configure each device, you must add a directory number to the device. This topic provides instructions on adding directory numbers using the **Device** > **Phone** menu option.

Before you begin

Create a device.

Step 1 Locate the **Association Information** section on the **Phone Configuration** window.
Step 2 Click **Add a new DN**.
Step 3 In the **Directory Number** field, specify a directory number.
Step 4 In the **Users Associated with Line** section, click **Associate End Users**.
Step 5 In the **Find User where** field, specify the appropriate filters and then click **Find**.
Step 6 From the list that appears, select the applicable users and click **Add Selected**.
Step 7 Specify all other required configuration settings as appropriate.
Step 8 Select **Apply Config**.
Step 9 Select **Save**.

Associate Users with Devices

On Cisco Unified Communications Manager version 9.x only, when the client attempts to retrieve the service profile for the user, it first gets the device configuration file from Cisco Unified Communications Manager. The client can then use the device configuration to get the service profile that you applied to the user.

For example, you provision Adam McKenzie with a CSF device named `CSFAKenzi`. The client retrieves `CSFAKenzi.cnf.xml` from Cisco Unified Communications Manager when Adam signs in. The client then looks for the following in `CSFAKenzi.cnf.xml`:

```
<userId  serviceProfileFile="identifier.cnf.xml">amckenzi</userId>
```

For this reason, if you are using Cisco Unified Communications Manager version 9.x, you should do the following to ensure that the client can successfully retrieve the service profiles that you apply to users:

- Associate users with devices.
- Set the **User Owner ID** field in the device configuration to the appropriate user. The client will retrieve the Default Service Profile if this value is not set.

Before you begin

Note Do not associate a CSF to multiple users if you intend to use different service profiles for these users.

Step 1 Associate users with devices.

a) Open the **Unified CM Administration** interface.
b) Select **User Management** > **End User**.
c) Find and select the appropriate user.
The **End User Configuration** window opens.
d) Select **Device Association** in the **Device Information** section.
e) Associate the user with devices as appropriate.
f) Return to the **End User Configuration** window and then select **Save**.

Step 2 Set the **User Owner ID** field in the device configuration.

a) Select **Device** > **Phone**.
b) Find and select the appropriate device.
The **Phone Configuration** window opens.
c) Locate the **Device Information** section.
d) Select **User** as the value for the **Owner** field.
e) Select the appropriate user ID from the **Owner User ID** field.
f) Select **Save**.

Create Mobile SIP Profiles

This procedure is required only when you use Cisco Unified Communication Manager release 9 and are configuring devices for mobile clients. Use the default SIP profile provided for desktop clients. Before you create and configure devices for mobile clients, you must create a SIP profile that allows Cisco Jabber to stay connected to Cisco Unified Communication Manager while Cisco Jabber runs in the background.

If you use Cisco Unified Communication Manager Release 10, choose the **Standard SIP Profile for Mobile Device** default profile when you create and configure devices for mobile clients.

Step 1 Open the **Cisco Unified CM Administration** interface.

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

The **Find and List SIP Profiles** window opens.

Step 3 Do one of the following to create a new SIP profile:

- Find the default SIP profile and create a copy that you can edit.
- Select **Add New** and create a new SIP profile.

Step 4 In the new SIP profile, set the following values:

- **Timer Register Delta** = 120
- **Timer Register Expires** = 720
- **Timer Keep Alive Expires** = 720
- **Timer Subscribe Expires** = 21600

- **Timer Subscribe Delta** = 15

Step 5 Select **Save**.

Setting up System SIP Parameters

If you are connected to a low-bandwidth network and finding it difficult to take an incoming call on your mobile device, you can set the system SIP parameters to improve the condition. Increase the SIP Dual Mode Alert Timer value to ensure that calls to the Cisco Jabber extension are not prematurely routed to the mobile-network phone number.

Before you begin

This configuration is only for mobile clients.

Cisco Jabber must be running to receive work calls.

Step 1 Open the **Cisco Unified CM Administration** interface.

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

Step 3 Select the node.

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** value to 10000 milliseconds.

Step 7 Select **Save**.

Note If, after you increase the SIP Dual Mode Alert Timer value, incoming calls that arrive in Cisco Jabber are still terminated and diverted using Mobile Connect, you can increase the SIP Dual Mode Alert Timer value again in increments of 500 milliseconds.

Configure the Phone Security Profile

You can optionally set up secure phone capabilities for all devices. Secure phone capabilities provide secure SIP signaling, secure media streams, and encrypted device configuration files.

If you enable secure phone capabilities for users, device connections to Cisco Unified Communications Manager are secure. However, calls with other devices are secure only if both devices have a secure connection.

Before you begin

- Configure the Cisco Unified Communications Manager security mode using the Cisco CTL Client. At minimum, select mixed mode security.

  For instructions on how to configure mixed mode with the Cisco CTL Client, see the Cisco Unified Communications Manager Security Guide.

- For conference calls, ensure that the conferencing bridge supports secure phone capabilities. If the conferencing bridge does not support secure phone capabilities, calls to that bridge are not secure. Likewise, all parties must support a common encryption algorithm for the client to encrypt media on conference calls.
- If your deployment uses Unified Communications Manager Release 12.5 or later, we recommend using SIP OAuth with Cisco Jabber. For details, see the chapter on SIP OAuth in the *Feature Configuration Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Step 1 In **Cisco Unified Communications Manager**, select **System** > **Security** > **Phone Security Profile**.

Step 2 Select **Add New**.

Step 3 From the **Phone Type** drop-down list, select the option that is applicable to the device type you are configuring and then select **Next**.

- **Cisco Unified Client Services Framework**—Select this option to create a CSF device for Cisco Jabber for Mac or Cisco Jabber for Windows.
- **Cisco Dual Mode for iPhone**—Select this option to create a TFT device for an iPhone.
- **Cisco Jabber for Tablet**—Select this option to create a TAB device for an iPad or an Android tablet or for Chromebooks.
- **Cisco Dual Mode for Android**—Select this option to create a BOT device for an Android device.
- **CTI Remote Device**—Select this option to create a CTI remote device.

  CTI remote devices are virtual devices that monitor and have call control over a user's remote destination.

Step 4 In the **Name** field of the **Phone Security Profile Configuration** window, specify a name for the phone security profile.

Step 5 For **Device Security Mode**, select one of the following options:

- **Authenticated**—The SIP connection is over TLS using NULL-SHA encryption.
- **Encrypted**—The SIP connection is over TLS using AES 128/SHA encryption. The client uses Secure Real-time Transport Protocol (SRTP) to offer encrypted media streams.

Step 6 For **Transport Type**, leave the default value of **TLS**.

Step 7 Select the **TFTP Encrypted Config** check box to encrypt the device configuration file that resides on the TFTP server.

Note For a TCT/BOT/Tablet device, do not select the TFTP Encrypted Config check box here. For Authentication Mode, select By Authentication String or Null String.

Step 8 For **Authentication Mode**, select **By Authentication String** or **By Null String**.

Note Using the CAPF Authentication mode **By Null String** with JVDI and Jabber for Windows CSF devices is not supported. It causes Jabber registration with Cisco Unified Communications Manager to fail.

Step 9 For **Key Size (Bits)**, select the appropriate key size for the certificate. Key size refers to the bit length of the public and private keys that the client generates during the CAPF enrollment process.

The Cisco Jabber clients were tested using authentication strings with 1024-bit length keys. The Cisco Jabber clients require more time to generate 2048-bit length keys than 1024-bit length keys. As a result, if you select 2048, expect it to take longer to complete the CAPF enrollment process.

Step 10 For **SIP Phone Port**, leave the default value.

The port that you specify in this field takes effect only if you select **Non Secure** as the value for **Device Security Mode**.

Step 11 Click **Save**.