Configure Softphone

Configure 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 that will access Cisco Jabber.
Step 2	Configure a SIP Trunk, on page 6	From Release 11.5(3), you must create a SIP trunk between Cisco Unified Communications Manager and IM and Presence Service it you want users to see phone presence from Cisco Jabber.
Step 3	Configure User Associations	
Step 4	Create Mobile SIP Profiles, on page 10.	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 12	Complete this task to set up secure phone capabilities for all devices.
Step 6	Provide Users with Authentication Strings, on page 13	

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.
- Enable mobility for each user for whom you plan to assign to a CTI remote device.
- 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.
- 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.

Procedure

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.
- **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 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
CTI Remote Device	• When you select **Owner User ID**, the device name field populates with *CTIRD<owner user ID>*. You can change this value. The device name does not have to begin with *CTIRD*. • Valid characters: a–z, A–Z, 0–9, period (.), underscore (_), hyphen (-). • 15-character limit.
Cisco Unified Client Services Framework	• Valid characters: a–z, A–Z, 0–9. • 15-character limit.
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.

If You Select	Required Format
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 creating a CTI Remote Device, in the **Protocol Specific Information** section, select an appropriate option from the **Rerouting Calling Search Space** drop-down list.
The Rerouting Calling Search Space defines the calling search space for rerouting and ensures that users can send and receive calls from the CTI remote device.

Step 8 To generate an authentication string that you can provide to end users to access their devices and securely register to Cisco Unified Communications Manager, navigate to the **Certification Authority Proxy Function (CAPF) Information** section.

Step 9 From the **Certificate Operation** drop-down list, select **Install/Upgrade**.

Step 10 From the **Authentication Mode** drop-down list, select **By Authentication String** or **By Null String**.

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

Step 11 Click **Generate String**.
The Authentication String autopopulates with a string value. This is the string that you will provide to end users.

Step 12 From the **Key Size (Bits)** drop-down list, select the same key size that you set in the phone security profile.

Step 13 In the **Operation Completes By** fields, specify an expiration value for the authentication string or leave as default.

Step 14 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 15 Select **Save**.

Step 16 Click **Apply Config**.

What to Do Next

Add a Directory Number to the device.

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.

Procedure

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**.

Add a Remote Destination

Remote destinations represent the CTI controllable devices that are available to users.

You should add a remote destination through the **Cisco Unified CM Administration** interface if you plan to provision users with dedicated CTI remote devices. This task ensures that users can automatically control their phones and place calls when they start the client.

If you plan to provision users with CTI remote devices along with software phone devices and desk phone devices, you should not add a remote destination through the **Cisco Unified CM Administration** interface. Users can enter remote destinations through the client interface.

Note

- You should create only one remote destination per user. Do not add two or more remote destinations for a user.
- Cisco Unified Communications Manager does not verify if it can route remote destinations that you add through the **Cisco Unified CM Administration** interface. For this reason, you must ensure that Cisco Unified Communications Manager can route the remote destinations you add.
- Cisco Unified Communications Manager automatically applies application dial rules to all remote destination numbers for CTI remote devices.

Procedure

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

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

The **Find and List Phones** window opens.

Step 3 Specify the appropriate filters in the **Find Phone where** field to and then select **Find** to retrieve a list of phones.

Step 4 Select the CTI remote device from the list.
The **Phone Configuration** window opens.

Step 5 Locate the **Associated Remote Destinations** section.

Step 6 Select **Add a New Remote Destination**.
The **Remote Destination Information** window opens.

Step 7 Specify JabberRD in the **Name** field.

Restriction You must specify JabberRD in the **Name** field. The client uses only the JabberRD remote destination. If you specify a name other than JabberRD, users cannot access that remote destination.

The client automatically sets the JabberRD name when users add remote destinations through the client interface.

Step 8 Enter the destination number in the **Destination Number** field.

Step 9 Specify all other values as appropriate.

Step 10 Select **Save**.

What to Do Next

Complete the following steps to verify the remote destination and apply the configuration to the CTI remote device:

1. Repeat the steps to open the **Phone Configuration** window for the CTI remote device.
2. Locate the **Associated Remote Destinations** section.
3. Verify the remote destination is available.
4. Select **Apply Config**.

Note The **Device Information** section on the **Phone Configuration** window contains a **Active Remote Destination** field.

When users select a remote destination in the client, it displays as the value of **Active Remote Destination**.

none displays as the value of **Active Remote Destination** if:

- Users do not select a remote destination in the client.
- Users exit or are not signed in to the client.

Configure a SIP Trunk

From Release 11.5(3), you must configure a SIP trunk between Cisco Unified Communications Manager and IM and Presence Service if you want users to see phone presence.

Configure a SIP Trunk Security Profile for IM and Presence Service

Procedure

Step 1 From Cisco Unified CM Administration choose **System** > **Security** > **SIP Trunk Security Profile**.

Step 2 Click **Find**.

Step 3 Click **Non Secure SIP Trunk Profile**.

Step 4 Click **Copy** and enter a name for the SIP trunk profile in the **Name** field.

Step 5 Verify the following settings:

- Device Security Mode = Non Secure
- Incoming Transport Type = TCP + UDP
- Outgoing Transport Type = TCP

Step 6 Check to enable the following items:

- Accept presence subscription
- Accept out-of-dialog refer
- Accept unsolicited notification
- Accept replaces header

Step 7 Click **Save**.

What to Do Next

Configure a SIP Trunk for IM and Presence Service, on page 7

Configure a SIP Trunk for IM and Presence Service

You only configure one SIP trunk between a Cisco Unified Communications Manager cluster and an IM and Presence Service cluster. After you configure the SIP trunk, you must assign that SIP trunk as the IM and Presence PUBLISH Trunk on Cisco Unified Communications Manager.

In the **Destination Address** field, enter a value using one of the following formats:

- dotted IP address
- fully qualified domain name (FQDN)
- DNS SRV

If high availability is configured for the IM and Presence cluster, multiple entries should be entered in the dotted IP address or FQDN to identify the various nodes in the cluster. DNS SRV cannot be used for an IM and Presence cluster if high availability is configured.

Before You Begin

Configure a SIP Trunk Security Profile for IM and Presence Service, on page 7

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Trunk**.

Step 2 Click **Add New**.

Step 3 Choose **SIP Trunk** from the Trunk Type menu.

Step 4 Choose **SIP** from the Device Protocol menu.

Step 5 Choose **None** for the Trunk Service Type.

Step 6 Click **Next**.

Step 7 Enter **CUPS-SIP-Trunk** for the Device Name.

Step 8 Choose a device pool from the Device Pool menu.

Step 9 In the SIP Information section at the bottom of the window, configure the following values:

a) In the Destination Address field, enter the Dotted IP Address, or the FQDN, which can be resolved by DNS and must match the SRV Cluster Name configured on the IM and Presence node.

b) Check the **Destination Address is an SRV** if you are configuring a multinode deployment.
In this scenario, Cisco Unified Communications Manager performs a DNS SRV record query to resolve the name, for example *_sip._tcp.hostname.tld*. If you are configuring a single-node deployment, leave this checkbox unchecked and Cisco Unified Communications Manager will perform a DNS A record query to resolve the name, for example *hostname.tld*.

Cisco recommends that you use the IM and Presence Service default domain as the destination address of the DNS SRV record.

Note You can specify any domain value as the destination address of the DNS SRV record. No users need to be assigned to the domain that is specified. If the domain value that you enter differs from the IM and Presence Service default domain, you must ensure that the SIP Proxy Service Parameter called SRV Cluster Name on IM and Presence Service matches the domain value that you specify in the DNS SRV record. If you use the default domain, then no changes are required to the SRV Cluster Name parameter.

In both scenarios, the Cisco Unified Communications SIP trunk Destination Address must resolve by DNS and match the SRV Cluster Name configured on the IM and Presence node.

c) Enter 5060 for the Destination Port.

d) Choose **Non Secure SIP Trunk Profile** from the SIP Trunk Security Profile menu.

e) Choose **Standard SIP Profile** from the SIP Profile menu.

Step 10 Click **Save**.
Troubleshooting Tip

If you modify the DNS entry of the Publish SIP Trunk SRV record by changing the port number or IP address, you must restart all devices that previously published to that address and ensure each device points to the correct IM and Presence Service contact.

What to Do Next

Configure SIP Publish Trunk, on page 9

Configure SIP Publish Trunk

Complete this procedure to enable Cisco Unified Communications Manager to publish phone presence for all line appearances that are associated with users licenses on Cisco Unified Communications Manager for IM and Presence Service.

Before You Begin

Configure a SIP Trunk for IM and Presence Service, on page 7

Procedure

Step 1 From Cisco Unified CM IM and Presence Administration choose **Presence** > **Settings** > **Standard Configuration**.

Step 2 From the **CUCM SIP Publish Trunk** drop-down list, choose a SIP trunk.

Step 3 Click **Save**.

Configure User Associations

When you associate a user with a device, you provision that device to the user.

Before You Begin

Create and configure Cisco Jabber devices.

Procedure

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

Step 2 Select **User Management** > **End User**.
The **Find and List Users** window opens.

Step 3 Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.

Step 4 Select the appropriate user from the list.
The **End User Configuration** window opens.

Step 5 Locate the **Service Settings** section.

Step 6 Select **Home Cluster**.

Step 7 Select the appropriate service profile for the user from the **UC Service Profile** drop-down list.

Step 8 Locate the **Device Information** section.

Step 9 Select **Device Association**.

The **User Device Association** window opens.

Step 10 Select the devices to which you want to associate the user. Jabber only supports a single softphone association per device type. For example, only one TCT, BOT, CSF, and TAB device can be associated with a user.

Step 11 Select **Save Selected/Changes**.

Step 12 Select **User Management** > **End User** and return to the **Find and List Users** window.

Step 13 Find and select the same user from the list.
The **End User Configuration** window opens.

Step 14 Locate the **Permissions Information** section.

Step 15 Select **Add to Access Control Group**.
The **Find and List Access Control Groups** dialog box opens.

Step 16 Select the access control groups to which you want to assign the user.
At a minimum you should assign the user to the following access control groups:

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

Remember If you are provisioning users with secure phone capabilities, do not assign the users to the **Standard CTI Secure Connection** group.

Certain phone models require additional control groups, as follows:

- Cisco Unified IP Phone 9900, 8900, or 8800 series or DX series, select **Standard CTI Allow Control of Phones supporting Connected Xfer and conf**.
- Cisco Unified IP Phone 6900 series, select **Standard CTI Allow Control of Phones supporting Rollover Mode**.

Step 17 Select **Add Selected**.
The **Find and List Access Control Groups** window closes.

Step 18 Select **Save** on the **End User Configuration** window.

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.

Procedure

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.

Procedure

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.

Procedure

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.
- **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 VXME and Jabber for Windows CSF devices is not supported. It causes Jabber registration with Cisco Unified Communications Manager (CUCM) 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**.

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.