Configuration

Configuration Files

For each Cisco Unified Client Services Framework (CSF) device that you add to the system, Cisco Unified Communications Manager creates a configuration (CNF.xml) file. The CNF file contains the device specifications for the associated user.

When users sign in to Cisco Jabber, Cisco Jabber Softphone for VDI starts the download of the associated CNF file to the thin client. To ensure the successful transfer of the file, open the relevant ports in all firewall applications to allow the thin client to access the ports. For more information about how to open ports, see the documentation for the firewall software.

Important Download of the CNF.xml file follows the system setting for HTTP proxy. Ensure that the proxy does not route the HTTP request from the thin client outside of the corporate network.

Set up Users on the Cisco Unified Communications Manager Workflow

Step 1 Create a CSF Device and a Directory Number for Each User, on page 2.

Step 2 Associate New Devices with a User, on page 4.

Step 3 Enable the CTI Protocol for Users, on page 4.

Step 4 Configure Cisco Unified Communications Features for Users, on page 5.

Enable the Unified Communications Manager IM and Presence Service. See the documentation for your version of Cisco Unified Communications Manager.

Create a CSF Device and a Directory Number for Each User

You can use the same Cisco Unified Client Services Framework (CSF) devices for the virtual environment, as you do for the nonvirtual environment. We recommend that you create only one CSF device for each virtual user. If multiple devices exist for a virtual user, virtual Jabber automatically selects the first device in the list.

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 2 Select **Add New**.

Step 3 From the **Phone Type** drop-down list, choose **Cisco Unified Client Services Framework**, and then select **Next**.

Step 4 In the **Phone Configuration** window, enter the applicable information for the phone as follows:

Option	Description
Device Name	Enter a name to identify the Cisco Unified Client Services Framework device. The name can contain 1 to 15 characters, including alphanumeric characters. Periods, hyphens, and underscores are not supported. Typically the device name format is CSF<username>; however, including the user ID is optional. Example: CSFjohndoe.
Description	Enter a descriptive name for the phone. For example, enter *Richard-phone-on-computer*.
Device Pool	Choose **Default** or another profile that was previously created. The device pool defines sets of common characteristics for devices. These characteristics include the region, the date and time group, the softkey template, and Multilevel Precedence and Preemption (MLPP) information.
Phone Button Template	Choose **Standard Client Services Framework**. The phone button template determines the configuration of buttons on a phone and identifies which feature (such as line or speed dial) is used for each button. This option is required.
Owner User ID	To use an adjunct license with this device, choose the user ID from the list.
Primary Phone	To use an adjunct license with this device, choose the device name of the Cisco Unified IP Phone to associate with the client application.
Allow Control of Device from CTI	Always check this option in a virtual environment.
Presence Group	Choose **Standard Presence Group**.
Device Security Profile	Choose **Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile**.
SIP Profile	Choose **Standard SIP Profile** or another profile that was previously created. SIP profiles provide specific SIP information for the phone, such as registration and keepalive timers, media ports, and Do Not Disturb control.

Option	Description
	Important If you choose **Secure Phone Profile**, do not specify the Certificate Authority Proxy Function (CAPF) authentication mode **By Null string**. Use of this setting with Cisco Jabber Softphone for VDI causes Jabber registration with Cisco Unified Communications Manager to fail.

Step 5 Scroll down to the **Product Specific Configuration Layout** section, and set **Video Calling** to **Enabled**.

Step 6 Select **Save**.

Step 7 Select **Apply Config** if this button is available, and then confirm when prompted.

Step 8 Select **Add a new DN** in the **Association Information** section that appears on the left side of the window.

Step 9 Enter information for the directory number on the **Directory Number Configuration** window.

Option	Description
Directory Number	Enter the directory number (line) to assign to the device.
Route Partition	Enter the route partition. Partitions divide the route plan into logical subsets. These subsets include organization, location, and type of call.
Display (Internal Caller ID)	Enter the Caller ID. This entry is optional. The actual display depends on this entry and the configuration for the other party. For example, Cisco IP Phones display the Caller ID, but Cisco Jabber does not.
Maximum Number of Calls	Specify the maximum number of calls that can be presented to the application. This number includes all calls placed on hold plus the active call, regardless of which party initiated the calls.
Busy Trigger	Specify the number of calls (active and on hold). Incoming calls, above this limit receive a busy signal or are redirected to the Forward Busy Internal/External target (if the target is configured).

Step 10 Select **Save**.

Step 11 Select **Apply Config** if this button is available, and then confirm when prompted.

Step 12 Scroll to the bottom of the **Directory Number Configuration** window, and then select **Associate End Users**.

Step 13 In the **Find and List Users** window, use the search criteria to find the user who you want to associate with the directory number.

Step 14 Check the box next to that username, and then select **Add Selected**.

The user is now associated with the DN.

Step 15 In the **User Associated with Line** section of the window, select the username.

Step 16 In the **End User Configuration** window, scroll down to the **Direct Number Associations** section.

Step 17 From the **Primary Extension** drop-down list, choose the DN for the user.

Step 18 In the **End User Configuration** window, under **Permissions Information**, select **Add to User Group** or **Add to Access Control Group**, depending on your version of Cisco Unified Communications Manager.

Step 19 In the **Find and List User Groups** window, use the search criteria to find **Standard CCM End Users**.

Step 20 Check the box next to **Standard CCM End Users**, and then select **Add Selected**.

Step 21 In the **Find and List User Groups** window, use the search criteria to find **Standard CTI Enabled**.

Step 22 Check the box next to **Standard CTI Enabled**, and then select **Add Selected**.

Step 23 Select **Save**.

Cisco Unified Communications Manager reminds you that changes to line or directory number settings require a restart. However, you need only restart after you edit lines on Cisco Unified IP Phones that are running at the time of the modifications.

Associate New Devices with a User

Note Perform this task in Cisco Unified Communications Manager.

Step 1 From Cisco Unified Communications Manager Administration, choose > **User Management** > **End User**.

Step 2 Search for the user in the **Find and List Users** window.

Step 3 Select the user.

Step 4 Select **Device Association** in the **Device Information** section.

Step 5 Search for the devices that you require in the **User Device Association** window.

Step 6 Select the devices that you require.

For example, you can select a device whose type is Cisco Unified Client Services Framework, and a desk-phone device.

Step 7 Select **Save Selected/Changes**.

Step 8 Select **Back to User** from the menu in the **Related Links** navigation box at the top right of the window.

Step 9 Select **Go**.

Step 10 Verify that the devices are listed in the **Device Information** section in the **End User Configuration** window.

Enable the CTI Protocol for Users

Enable the computer-telephony integration (CTI) protocol for each Cisco Jabber Softphone for VDI user.

Step 1 In Cisco Unified Communications Manager Administration, click **User Management** > **End Users**.

Step 2 Search for the user in the **Find and List Users** window.

Step 3 Select the user.

Step 4 In the **End User Configuration** window, scroll down to Permissions Information.

Step 5 Click **Add to User Group**.

Step 6 Select the following required groups:

- Standard CCM End Users
- Standard CTI Allow Control of All Devices
- Standard CTI Enabled

Step 7 Select the following groups if want to configure selective call recording:

- Standard CTI Allow Call Recording
- Standard CTI Allow Call Monitoring

Step 8 Click **Save**.

What to do next

Enable the Unified Communications Manager IM and Presence Service. See the documentation for your version of Cisco Unified Communications Manager.

Configure Cisco Unified Communications Features for Users

For information about how to configure Cisco Unified Communications features for Cisco Jabber, see the deployment and installation guide for your release, available from http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html.

Change a User Password

Use this procedure to change the password for a user only if LDAP Authentication is not enabled. If LDAP Authentication is enabled, the passwords are stored on the LDAP Server. For Cisco Unified Communications Manager 9.0 or later, this procedure applies only to passwords for users created locally.

SUMMARY STEPS

1. From Cisco Unified Communications Manager Administration, choose **Cisco Unified Communications Manager Administration** > **User Management** > **End User**.
2. Search for the user in the **Find and List Users** window.
3. Select the user.
4. In the **End User Configuration** window, in the **Password** field, enter a new password for the user.
5. In the **Confirm Password** field, enter the new password for the user again.
6. Select **Save**.

DETAILED STEPS

Step 1 From Cisco Unified Communications Manager Administration, choose **Cisco Unified Communications Manager Administration** > **User Management** > **End User**.

Step 2 Search for the user in the **Find and List Users** window.

Step 3 Select the user.

Step 4 In the **End User Configuration** window, in the **Password** field, enter a new password for the user.

Step 5 In the **Confirm Password** field, enter the new password for the user again.

Step 6 Select **Save**.