On-Premises IM Using Cisco Jabber

TECHNOLOGY DESIGN GUIDE

August 2013

Table of Contents

Preface

Cisco Validated Designs (CVDs) provide the framework for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Cisco engineers have comprehensively tested and documented each CVD in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested and validated design and deployment details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate or reference existing CVDs, but also include product features and functionality across Cisco products and may include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems using their own setup and configuration.

How to Read Commands

Many CVD guides tell you how to use a command-line interface (CLI) to configure network devices. This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands at a CLI or script prompt appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
police rate 10000 pps burst 10000 packets conform-action set-discard-class-
transmit 48 exceed-action transmit
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the feedback form.

For the most recent CVD guides, see the following site:

http://www.cisco.com/go/cvd

CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

Use Cases

This guide addresses the following technology use cases:

- On-Premises IM and Presence with Jabber—Organizations are challenged by the difficulty of getting their employees to connect with the right people at the right time, and the new workforce prefers immediate communication, which is easier than email and voicemail but less intrusive than a phone call or web-based meeting.

For more information, see the "Use Cases" section in this guide.

Scope

This guide covers the following areas of technology and products:

- Unified communications applications, such as IP telephony, voicemail, instant messaging (IM), and presence
- Telephony call agent
- Voicemail server
- IM and presence server
- Virtualized servers
- Windows, iPad, and iPhone software clients
- Lightweight Directory Access Protocol integration
- Integration of the above with LAN and data-center switching infrastructure

For more information, see the "Design Overview" section in this guide.

Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- CCNP Voice—3 to 5 years designing, installing, and troubleshooting voice and unified communications applications, devices, and networks
- VCP VMware—At least 6 months installing, deploying, scaling, and managing VMware vSphere environments

Related CVD Guides

Telephony Using Cisco UCM Technology Design Guide

To view the related CVD guides,
click the titles or visit the following site:
http://www.cisco.com/go/cvd

Introduction

The ability to collaborate efficiently and effectively in a fast-growing enterprise is challenging for many organizations because they want their employees to work anywhere, anytime, and from any device. They want to lower their IT support requirements, but not stifle the ability of their employees to remain mobile. They also want to establish a common platform for communication inside and outside their organization, irrespective of geography or distance.

Technology Use Case

Organizations are challenged by the difficulty of getting their employees to connect with the right people at the right time and the significantly increasing modes of communications. Most knowledge workers use several devices on a day-to-day basis to communicate, including traditional desk phones, smart phones, tablets, laptops, and desktop computers. The modes to communicate are time-consuming to learn because each device is different from the rest. This always-on and always-connected mentality is permeated by the youngest members of the workforce who have grown accustomed to using technology to give them more flexibility in how and where they work. The new workforce prefers immediate communication, which is easier than email and voicemail but less intrusive than a phone call or web-based meeting.

Use Case: On-Premises IM and Presence with Jabber

Organizations need an application for laptops, desktops, Macs, tablets, and smartphones that allows them to be more productive, from anywhere, on any device. They want to find the right people, see if and how they are available, and collaborate using their preferred method of communication. They need an on-premises solution that is fast to deploy and easy to manage from a central location, without replicating costly features at their remote sites.

This design guide enables the following capabilities:

- **Use a centralized design**—Each remote site connects to the headquarters site through a WAN and they receive IM and presence features from the headquarters location. This makes the on-premises solution simpler to deploy and easier to manage from a centralized site, while saving on infrastructure components.
- **Reduce communication delays with presence and contact information**—The Cisco Jabber application enables you to see the availability of co-workers and colleagues within and outside your organization. This capability helps reduce communication delays, which results in faster decision making and enhanced productivity.
- **Quickly communicate with instant messaging**—The Cisco Jabber application delivers instant messaging capabilities that are integrated with other communication capabilities, so you can simply move between chats, audio conversations, and web conferences.
- **Bring IP telephony and video to the desktop**—Cisco Jabber for Windows delivers voice and video to your desktop as a soft phone with wideband and high-fidelity audio, standards-based high-definition video (720p), and desk-phone control features. These features mean that high-quality and high-availability voice and video telephony is available at all locations.
- **Accelerate team performance with multiparty conferencing and collaboration**—The Cisco Jabber application provides for smooth escalation to desktop sharing or Cisco WebEx Conferencing.
- **Collaborate from common business applications**—You can access the capabilities of the Cisco Jabber application from common desktop applications such as Microsoft Outlook, including lighting presence bubbles and click-to-communicate.

Design Overview

Cisco Jabber for Windows streamlines communications and enhances productivity by unifying presence, instant messaging, video, voice, voice messaging, desktop sharing, and conferencing capabilities securely into one desktop client. It offers flexible deployment models and integrates with commonly used applications. Cisco Jabber for Windows can also be deployed in virtual environments. In a virtual environment, it supports presence, instant messaging, and desk-phone control.

Cisco Jabber for iPad provides instant messaging, video and voice calling, corporate directory search, availability, and voicemail. Cisco Jabber for iPad uses video rate adaptation in order to negotiate optimal video quality based on your network conditions. Video rate adaptation dynamically scales video quality when video transmission begins, based on the available bandwidth.

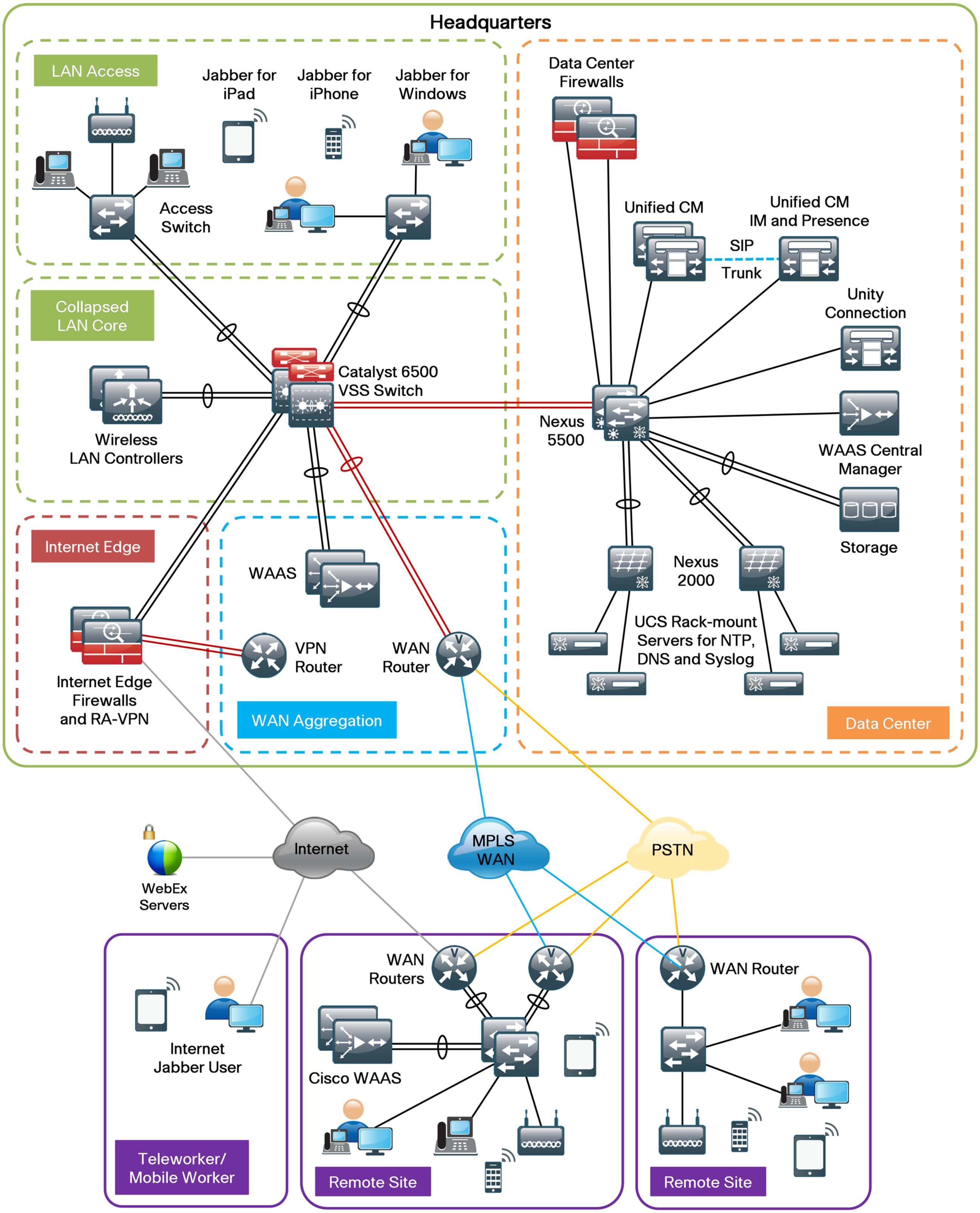
Cisco Jabber IM for iPhone lets you reduce communication delays by knowing a person's availability with rich presence status. You can use the application to connect quickly over IM and, if necessary, escalate to a phone call, send an email or text message, start an instant web conference, or use Short Message Service (SMS). Cisco Jabber for iPhone also provides voice-over-IP (VoIP) capabilities.

Cisco Jabber can be deployed on-premises or by using a cloud-based service, offering IT departments the flexibility to choose the model that best suits their business.

The on-premises Jabber solution includes the following components (shown in Figure 1):

- Unified CM IM and Presence for instant messaging and presence
- Unified CM for audio and video call management, user and device configuration, and Jabber software phone and directory synchronization
- Unity Connection for voice mail
- Jabber for Windows, Jabber for iPad, and Jabber for iPhone
- MS Active Directory for client user information
- WebEx Meeting Center for hosted meetings
- Network Time Protocol (NTP) server for logging consistency
- Domain Name System (DNS) server for name-to-IP resolution
- Syslog server for logging events (optional)

Figure 1 - On-premises IM and presence using Cisco Jabber



This guide includes the following Cisco Jabber features:

- Communication integration–Use a single, intuitive interface for instant messaging with individuals and groups, IP telephony, visual voicemail, voice and web conferencing, desktop sharing, communication history, and integrated directories.
- Presence–View real-time availability of co-workers and colleagues within and outside the enterprise network.
- Enterprise instant messaging–Chat in real time by using instant messaging. Several chat modes are supported, ranging from:
    - Point-to-point chat with co-workers inside your network, or supported federated business and personal contacts
    - Group chat, which enables multiple colleagues to communicate and collaborate in a single discussion
    - Personal instant messaging history for your reference
- Predictive search–Provides suggestions to you as you type in a search query and is capable of indexing your Cisco Jabber contact list, recent contacts, Microsoft Active Directory, or LDAP directory.
- Media escalation–Escalate from a chat to an audio call, video call, desktop share, or web meeting. Media escalations are as easy as clicking a button.
- Desktop share–Share what is on your desktop with Cisco Jabber users, as well as Cisco and other standards-based video endpoints.
- Integrated voice and video telephony–A coordinated video display on the screen and voice conversation with a dedicated soft phone.
    - Make, receive, and control your phone calls whether you are in or out of the office.
    - Business-quality video communication up to high-definition (720p) and high-fidelity wideband audio is supported.
    - You can use voice, video, and even desktop share when interacting with telepresence endpoints and room-based and multipoint videoconferencing systems.
    - Many call-control options are available, including mute, call transfer, call forwarding, and ad-hoc conferencing.
    - The reliability and failover features of Cisco Unified Communications Manager are supported.
- Visual voice message access–Access and manage your voice messages.
    - View, play back, and delete voice messages from Cisco Unity Connection.
    - Secure messaging is provided, with support for private and encrypted voice messages.

Deployment Details

The procedures for configuring a basic Cisco Unified Communications Manager (Unified CM) cluster with LDAP and Cisco Unity Connection are documented in the Telephony Using Cisco UCM Design Guide, so the concepts are not covered again in this guide.

This guide covers the details for installing Cisco Jabber for Windows, Cisco Jabber for iPad, and Cisco Jabber for iPhone. The first three processes have to be completed by all users of this guide. However, the remaining processes can be done together or on an individual basis, depending on the type of Cisco Jabber clients you are planning to deploy.

PROCESS

Preparing the Platform for Cisco Unified CM IM and Presence

1. Configure platform connectivity to the LAN
2. Prepare the server for IM and Presence

The on-premises design requires a server running the Cisco Unified Communications Manager Instant Messaging and Presence Service. It runs on the same Linux operating systems as several other unified communications platforms from Cisco. You install the operating system with the application by using the standard installation DVD or ISO file.

For a quick and easy installation experience, it is essential to know up-front what information you will need. For Cisco Unified CM Instant Messaging and Presence, make sure you have completed the following steps before you start:

- Download the Open Virtualization Archive (OVA) file from the Cisco website at: http://www.cisco.com/cisco/software/release.html?mdfid=284330176&flowid=33722&softwareid=283757588&release=9.0&relind=AVAILABLE&rellifecycle=&reltype=latest
- Check the Cisco website to determine if there is a patch for your version of Cisco Unified CM IM and Presence: http://software.cisco.com/download/release.html?mdfid=284510549&flowid=37582&softwareid=282074312&release=9.1(1)&relind=AVAILABLE&rellifecycle=&reltype=latest

Procedure 1 Configure platform connectivity to the LAN

The Cisco Unified CM IM and Presence server can be connected to a Cisco Nexus switch in the data center or a Cisco Catalyst switch in the server room. In both cases, quality of service (QoS) policies are added to the ports in order to maintain voice and data quality. Please choose the option that is appropriate for your environment.

Option 1: Connect the Cisco Unified CM IM and Presence server to a Cisco Nexus 2248UP switch

Step 1: Login to the Cisco Nexus switch with a username that has the ability to make configuration changes.

Step 2: If there is a previous configuration on the switch port where the Cisco Unified CM IM and Presence server is connected, remove the individual commands by issuing a **no** in front of each one. This brings the port back to its default state.

Step 3: Configure the port as an access port and apply the QoS policy.

```
interface Ethernet107/1/14
 description Unified CM IM and Presence
 switchport access vlan 148
 spanning-tree port type edge
 service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
```

Tech Tip

When deploying a dual-homed Cisco Nexus 2248 switch, you must apply this configuration to both Nexus 5548 switches.

Option 2: Connect the Cisco Unified CM IM and Presence server to a Cisco Catalyst 3750-X Series switch

To ensure that signaling traffic is prioritized appropriately, you must configure the Cisco Catalyst access switch port where the Cisco Unified CM IM and Presence server is connected to trust the differentiated services code point (DSCP) markings. The easiest way to do this is to clear the interface of any previous configuration and then, apply the egress QoS macro that was defined in the access-switch platform configuration of the Campus Wired LAN Design Guide.

Step 1: Login to the Cisco Catalyst switch with a username that has the ability to make configuration changes.

Step 2: Clear the interface's configuration on the switch port where the Cisco Unified CM IM and Presence server is connected.

```
default interface GigabitEthernet1/0/16
```

Step 3: Configure the port as an access port and apply the egress QoS policy.

```
interface GigabitEthernet1/0/16
 description Unified CM IM and Presence
 switchport access vlan 148
 switchport host
 macro apply EgressQoS
```

Procedure 2 Prepare the server for IM and Presence

The following table describes the scaling options for Cisco Unified CM IM and Presence:

Table 1 - Cisco Unified CM IM and Presence virtual machine scaling options

	5000 full UC users	**15000 full UC users**
Virtual CPUs	2	4
CPU speed	2500 MHz	8000 MHz
RAM	4 GB	6 GB
Hard disk	80 GB (2)	80 GB (2)
VMware ESXi	4.0, 4.1, 5.0	4.0, 4.1, 5.0
OS support	RHE Linux 5 (32-bit)	RHE Linux 5 (32-bit)
Total users	5000 or fewer	5000 to 10,000

Follow the steps below to deploy an OVA file in order to define the virtual machine requirements. You use the Open Virtualization Format (OVF) support of VMware in order to import and deploy the OVA file.

Step 1: In VMware vSphere Client, choose **File > Deploy OVF Template**.

Step 2: In the Deploy OVF Template wizard, enter the following information, and then click **Finish**:

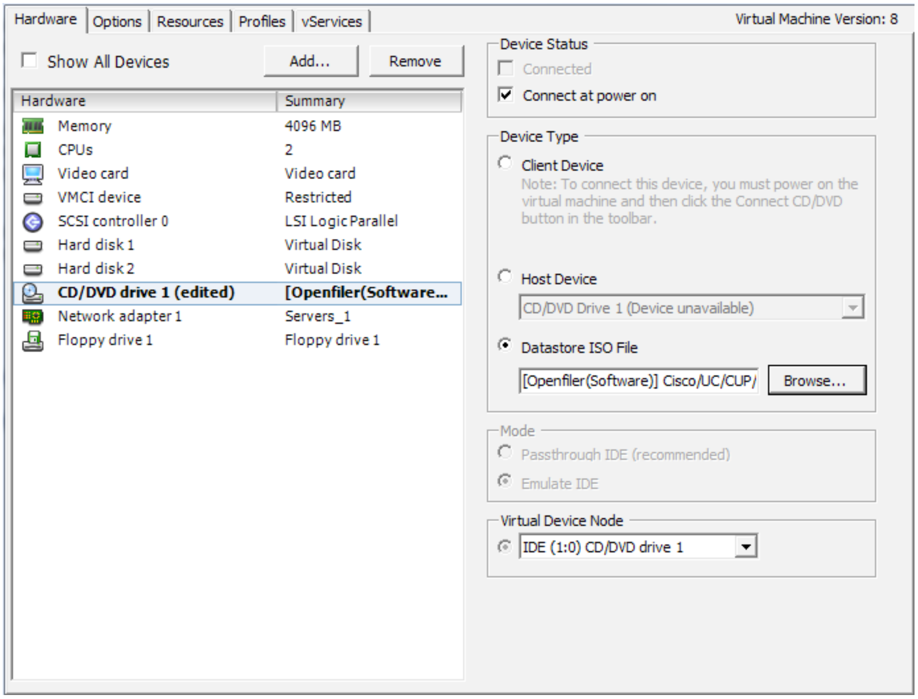
- On the **Source** page, next to the **Deploy from a file or URL** box, click **Browse**, navigate to the location of the OVA file that you downloaded from Cisco, and then click **Next**.
- On the **OVF Template Details** page, verify the information, and then click **Next**:
- On the Name and Location page, in the **Name** box, enter the virtual machine name **CUCM-IMP1**, and then click **Next**.
- On the Deployment Configuration page, select one of the following options for the number of Cisco UC users, and then click **Next**:
    - **5000 full UC users**–For a cluster of less than 5000 Cisco UC users
    - **15000 full UC users**–For a cluster of more than 5000 Cisco UC users
- On the Storage page, choose the location to store the VM files, and then click **Next**.
- On the Disk Format page, select **Thick Provision Eager Zeroed**, and then click **Next**.
- On the Ready to Complete page, verify the settings, and then click **Finish**.

Step 3: In the message window, click **Close**.

Step 4: After the virtual machine is created, click on the server name (Example: CUCM-IMP1), navigate to the **Getting Started** tab, and then click **Edit virtual machine settings**.

Step 5: On the Hardware tab, select **CD/DVD Drive 1**, and then select **Connect at power on**.

Step 6: Select **Datastore ISO File**, click **Browse**, and then navigate to the location of the Cisco Unified CM IM and Presence bootable installation file. After selecting the correct ISO image, click **OK**.



Virtual Machine Version: 8

□ Show All Devices

Hardware	Summary
Memory	4096 MB
CPUs	2
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
CD/DVD drive 1 (edited)	**[Openfiler(Software...**
Network adapter 1	Servers_1
Floppy drive 1	Floppy drive 1

Device Status

□ Connected

☑ Connect at power on

Device Type

○ Client Device

Note: To connect this device, you must power on the virtual machine and then click the Connect CD/DVD button in the toolbar.

○ Host Device

CD/DVD Drive 1 (Device unavailable)

● Datastore ISO File

[Openfiler(Software)] Cisco/UC/CUP/

Mode

○ Passthrough IDE (recommended)

● Emulate IDE

Virtual Device Node

IDE (1:0) CD/DVD drive 1

Step 7: On the Getting Started tab, click **Power on the virtual machine**.

Step 8: Click the **Console** tab, and then watch the server boot.

The virtual machine is prepared for installation.

PROCESS

Installing Cisco Unified CM IM and Presence

1. Install Cisco Unified CM IM and Presence
2. Configure Unified CM IM and Presence

Make sure you have the following information:

- Time zone for the server
- Host name, IP address, network mask, and default gateway
- Domain Name System (DNS) server IP addresses
- Administrator ID and password
- Organization, unit, location, state, and country
- Network Time Protocol (NTP) server IP addresses
- Security password
- Application username and password

Complete the tasks listed below before you start the installation:

- In DNS, configure the Cisco Unified CM IM and Presence host name: **CUCM-IMP1**
- Obtain license files from the Cisco licensing system

Procedure 1 Install Cisco Unified CM IM and Presence

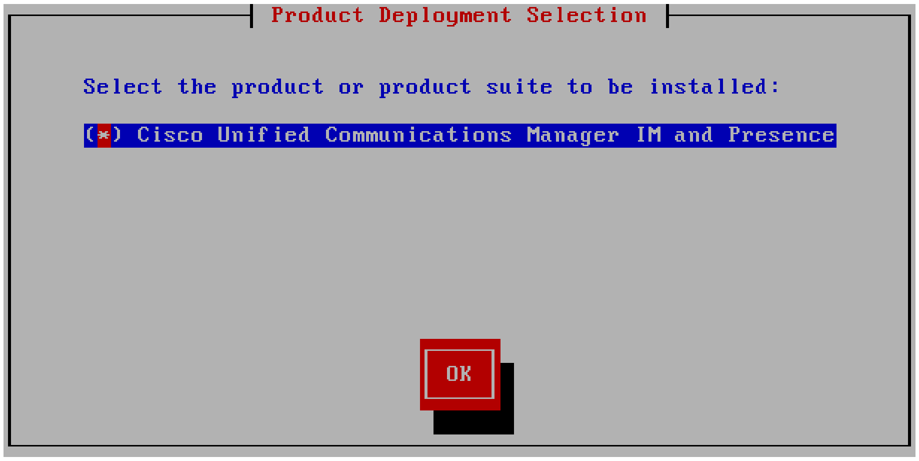
After the ISO/DVD loads, continue the installation on the server console.

Step 1: On the DVD Found page, choose Yes.

Step 2: If the media check is successful, choose OK.

If the media check does not pass, contact Cisco Technical Assistance Center or your local representative in order to replace the media, and then repeat Step 1.

Step 3: On the Product Deployment Selection page, verify the product is Cisco Unified Communications Manager IM and Presence, and then choose **OK**.



```
Product Deployment Selection

Select the product or product suite to be installed:

(*) Cisco Unified Communications Manager IM and Presence
```

Step 4: On the Proceed with Install page, verify that the version is correct, and then choose **Yes**.

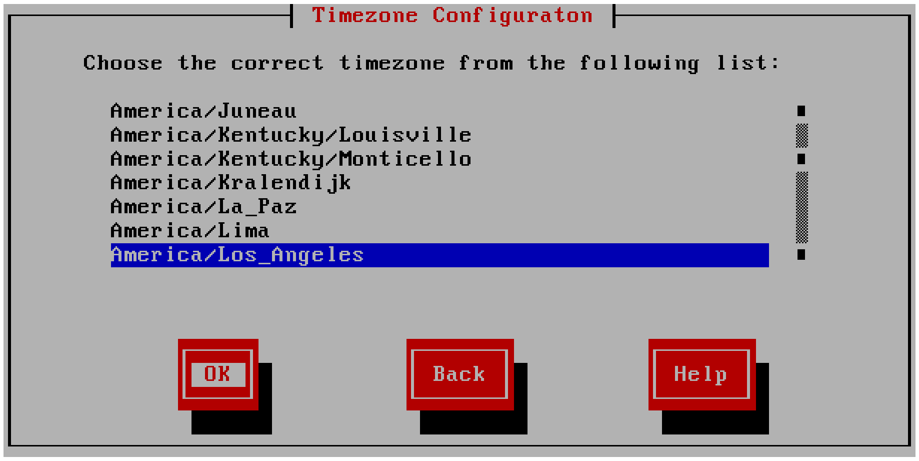
Step 5: On the Platform Installation Wizard page, choose **Proceed**.

Step 6: If no upgrade patch exists for the version you are installing, on the Apply Patch page, choose **No**.

If an upgrade patch does exist, on the Apply Patch page, choose **Yes**, and then follow the instructions on the pages to complete the process.

Step 7: On the Basic Install page, choose **Continue**.

Step 8: On the Timezone Configuration page, select the correct time zone for the server location, and then choose **OK**.



```
Timezone Configuraton

Choose the correct timezone from the following list:

  America/Juneau
  America/Kentucky/Louisville
  America/Kentucky/Monticello
  America/Kralendijk
  America/La_Paz
  America/Lima
  America/Los_Angeles
```

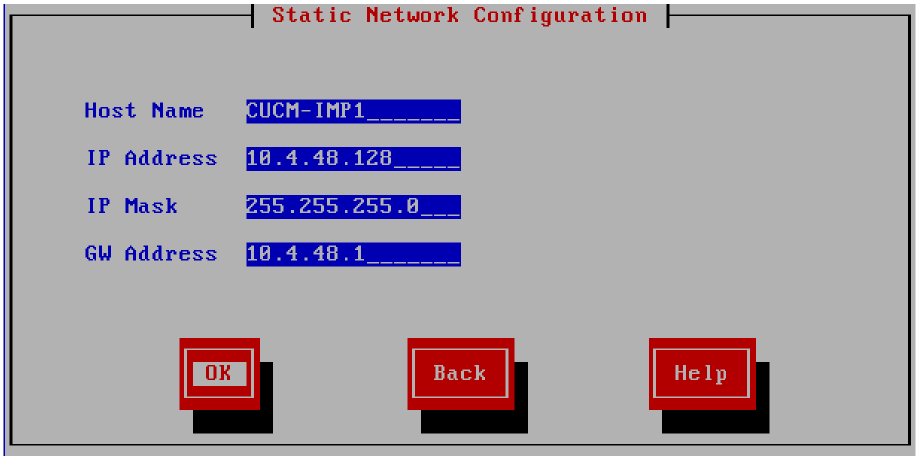
Step 9: On the Auto Negotiation Configuration page, choose **Continue**.

Step 10: On the MTU Configuration page, choose **No**.

Step 11: On the DHCP Configuration page, choose **No**.

Step 12: On the Static Network Configuration page, enter the following information, and then choose **OK**:

- Host Name—**CUCM-IMP1**
- IP Address—**10.4.48.128**
- IP Mask—**255.255.255.0**
- GW Address—**10.4.48.1**

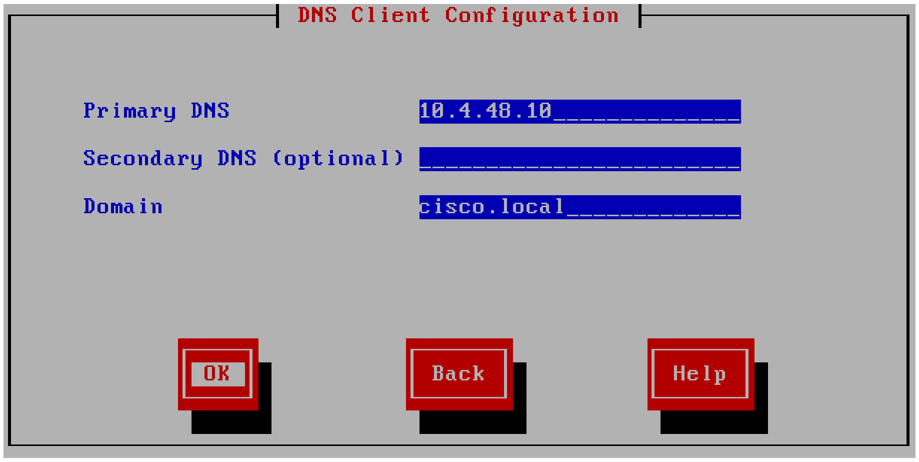


```
Static Network Configuration

Host Name     CUCM-IMP1______
IP Address    10.4.48.128_____
IP Mask       255.255.255.0___
GW Address    10.4.48.1_______
```

Step 13: On the first DNS Client Configuration page, choose **Yes**.

Step 14: On the second DNS Client Configuration page, enter the following information, and then choose **OK**:

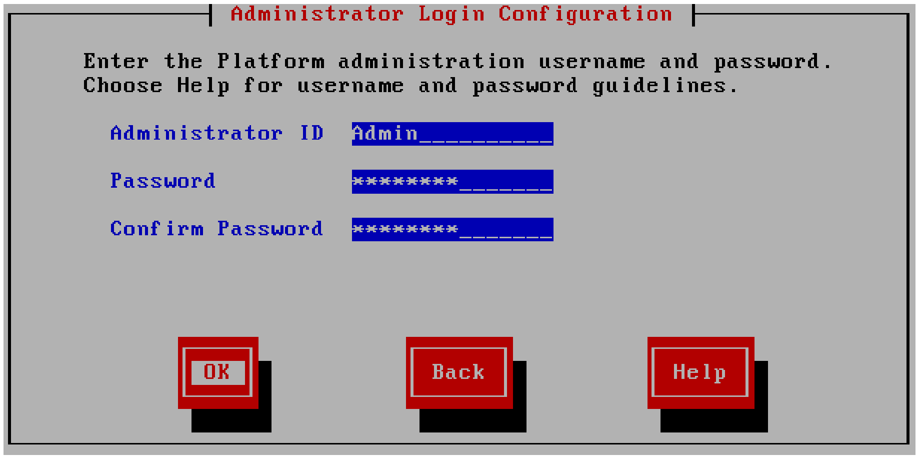
- Primary DNS—**10.4.48.10**
- Domain—**cisco.local**



```
DNS Client Configuration

Primary DNS                 10.4.48.10______________
Secondary DNS (optional)    ________________________
Domain                      cisco.local_____________
```

Step 15: On the Administrator Login Configuration page, enter the following information, and then choose **OK**:

- Administrator ID—**Admin**
- Password—**[password]**
- Confirm Password—**[password]**



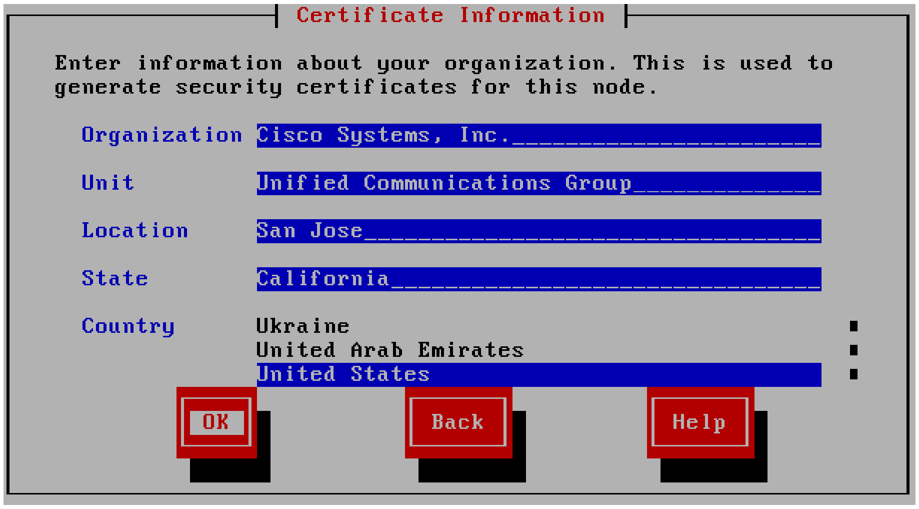
```
Administrator Login Configuration

Enter the Platform administration username and password.
Choose Help for username and password guidelines.

Administrator ID    Admin__________
Password            *********_______
Confirm Password    *********_______
```

Step 16: On the Certificate Information page, enter the information that will be used to generate security certificates, and then choose **OK**:

- Organization—**Cisco Systems, Inc.**
- Unit—**Unified Communications Group**
- Location—**San Jose**
- State—**California**
- Country—**United States**

Tech Tip

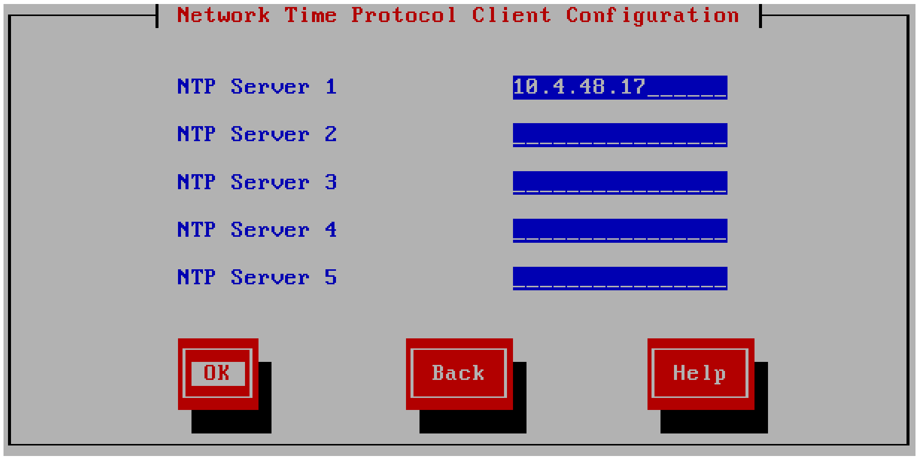
These fields must match the information submitted to Cisco, or the licenses will not be valid.



```
Certificate Information

Enter information about your organization. This is used to
generate security certificates for this node.

Organization  Cisco Systems, Inc.________________________
Unit          Unified Communications Group______________
Location      San Jose__________________________________
State         California________________________________
Country       Ukraine
              United Arab Emirates
              United States
```

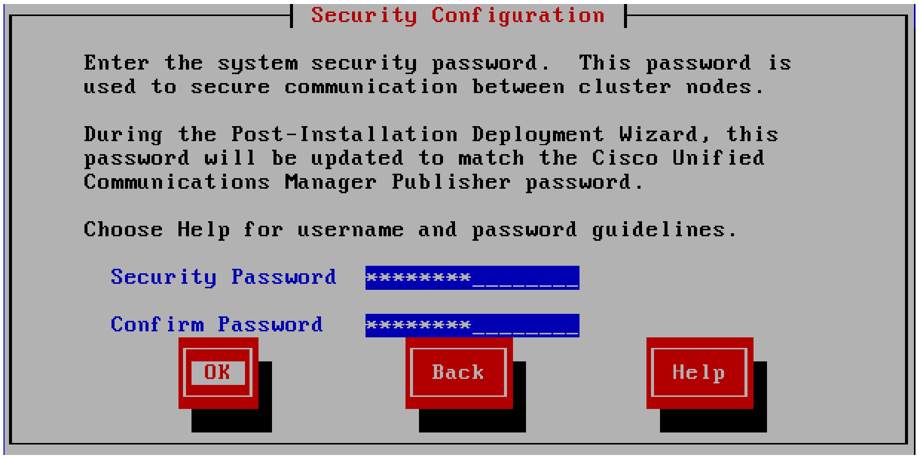
Step 17: On the First Node Configuration page, choose **Yes**.

Step 18: On the Network Time Protocol Client Configuration page, in the **NTP Server 1** box, enter **10.4.48.17**, and then choose **OK**.



```
Network Time Protocol Client Configuration

NTP Server 1          10.4.48.17______
NTP Server 2          ________________
NTP Server 3          ________________
NTP Server 4          ________________
NTP Server 5          ________________
```

Step 19: On the Security Configuration page, enter the password for server-to-server communication, and then choose **OK**.

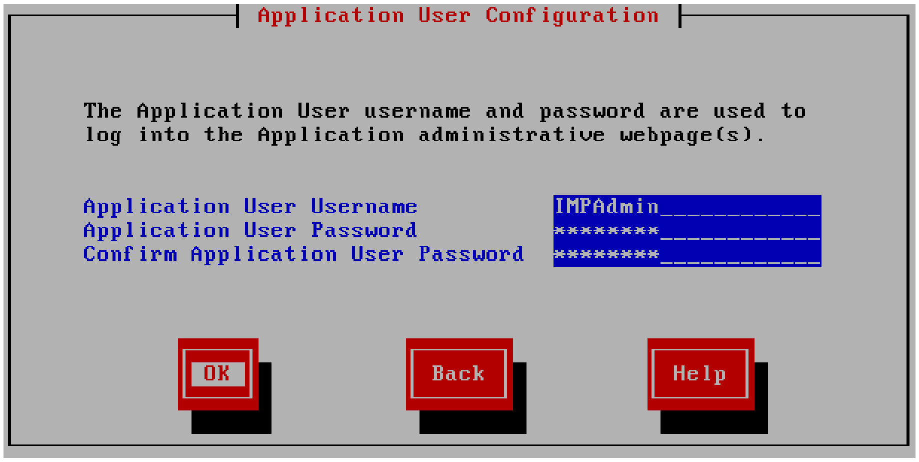


```
Security Configuration

Enter the system security password.  This password is
used to secure communication between cluster nodes.

During the Post-Installation Deployment Wizard, this
password will be updated to match the Cisco Unified
Communications Manager Publisher password.

Choose Help for username and password guidelines.

  Security Password    ********_________
  Confirm Password     ********_________
```

Step 20: On the SMTP Host Configuration page, choose **No**.

Step 21: On the Application User Configuration page, enter the following information, and then choose **OK**:

- Application User Username—**IMPAdmin**
- Password—**[password]**
- Confirm Password—**[password]**



```
Application User Configuration

The Application User username and password are used to
log into the Application administrative webpage(s).

Application User Username          IMPAdmin____________
Application User Password          ********____________
Confirm Application User Password  ********____________
```

Step 22: On the Platform Configuration Confirmation page, choose **OK**.

The system finishes the rest of the installation process without user input. The system reboots a few times during installation. The process can take 60 minutes or more, depending on your server hardware.

After the software has finished installing, the login prompt appears on the console.

Step 23: In the vSphere Client, navigate to the virtual machine's **Getting Started** tab, and then click **Edit virtual machine settings**.

Step 24: On the Hardware tab, select **CD/DVD Drive 1**.

Step 25: Clear **Connect at power on**, and then click **OK**.

Procedure 2 Configure Unified CM IM and Presence

After the software is installed, use the web interface in order to complete the rest of the procedures.

Step 1: In a web browser, access the IP address or hostname of the Cisco Unified CM IM and Presence server, and then in the center of the page under Administrative Applications, click **Cisco Unified Communications Manager IM and Presence**.

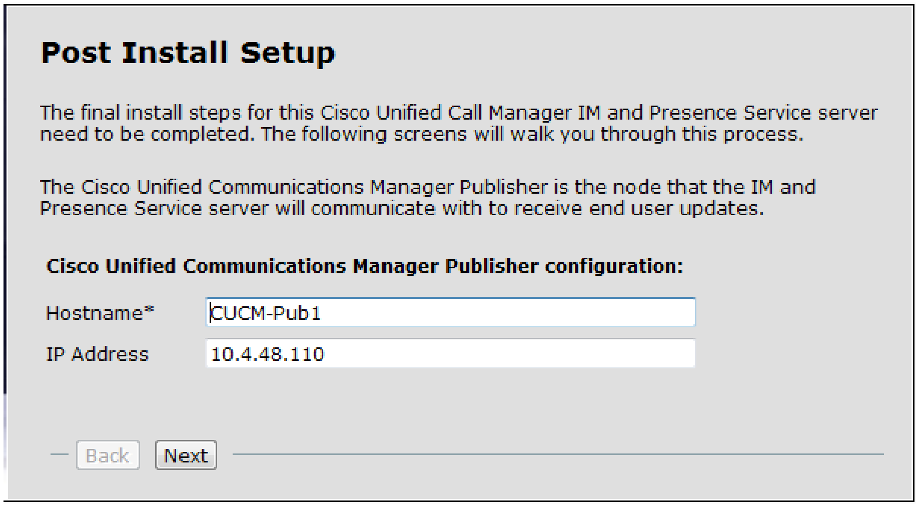
Tech Tip

If you receive a message about the website's security certificate, ignore it and continue to the page.

Step 2: Enter the name and password you entered on the Application User Configuration page in Step 21 of Procedure 1 "Install Cisco Unified CM IM and Presence," and then click **Login**.

Step 3: On the Post Install Setup page, enter the following information, and then click **Next**:

- Hostname—**CUCM-Pub1**
- IP Address—**10.4.48.110**



Post Install Setup

The final install steps for this Cisco Unified Call Manager IM and Presence Service server need to be completed. The following screens will walk you through this process.

The Cisco Unified Communications Manager Publisher is the node that the IM and Presence Service server will communicate with to receive end user updates.

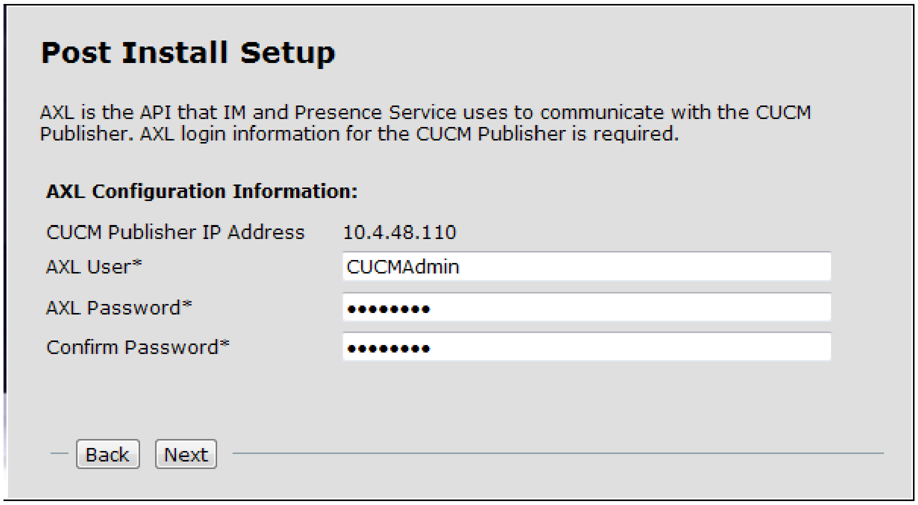
Cisco Unified Communications Manager Publisher configuration:

Hostname* CUCM-Pub1

IP Address 10.4.48.110

Step 4: On the next page, enter the following information, and then click **Next**:

- AXL User—**CUCMAdmin**
- AXL Password—**[password]** (must match the password on Cisco Unified CM)
- Confirm Password—**[password]**



Post Install Setup

AXL is the API that IM and Presence Service uses to communicate with the CUCM Publisher. AXL login information for the CUCM Publisher is required.

AXL Configuration Information:

CUCM Publisher IP Address 10.4.48.110

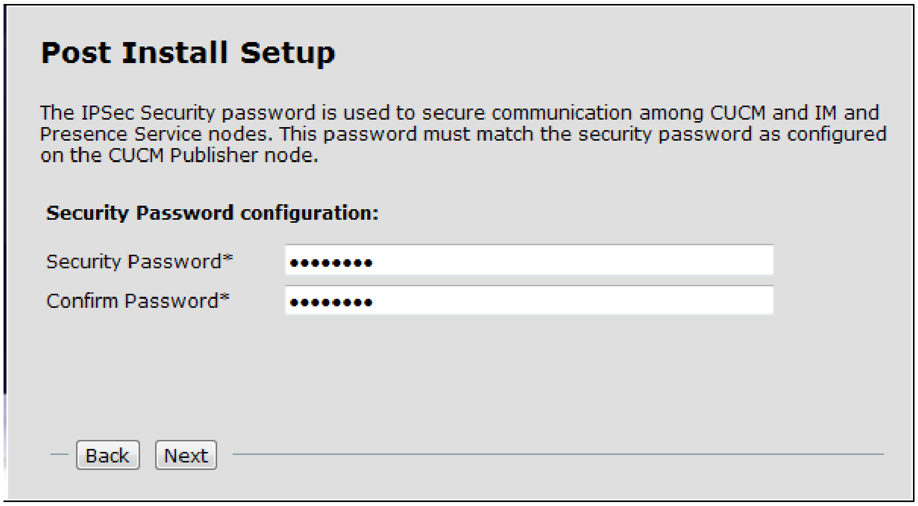
AXL User* CUCMAdmin

AXL Password* ••••••••

Confirm Password* ••••••••

Step 5: On the next page, enter the following information, and then click **Next**:

- Security Password—**[password]** (must match the password on Cisco Unified CM)
- Confirm Password—**[password]**



Post Install Setup

The IPSec Security password is used to secure communication among CUCM and IM and Presence Service nodes. This password must match the security password as configured on the CUCM Publisher node.

Security Password configuration:

Security Password* ••••••••

Confirm Password* ••••••••

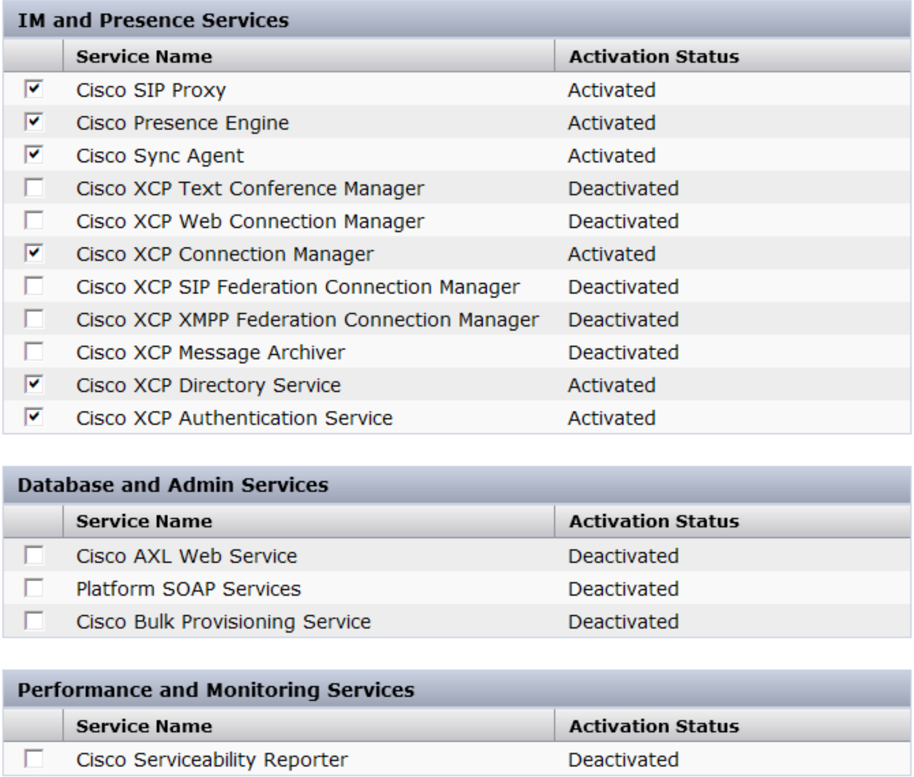
Step 6: On the next page, verify the information, and then click **Confirm**.

Step 7: On the next page, click **Home**.

Step 8: In the **Navigation** list at the top right of the page, choose **Cisco Unified IM and Presence Serviceability**, and then click **Go**.

Step 9: Navigate to Tools > Service Activation, enter the following information, and then click Save:

- Cisco SIP Proxy—**Select**
- Cisco Presence Engine—**Select**
- Cisco Sync Agent—**Select**
- Cisco XCP Connection Manager—**Select**
- Cisco XCP Directory Service—**Select**
- Cisco XCP Authentication Service—**Select**



IM and Presence Services

	Service Name	Activation Status
☑	Cisco SIP Proxy	Activated
☑	Cisco Presence Engine	Activated
☑	Cisco Sync Agent	Activated
□	Cisco XCP Text Conference Manager	Deactivated
□	Cisco XCP Web Connection Manager	Deactivated
☑	Cisco XCP Connection Manager	Activated
□	Cisco XCP SIP Federation Connection Manager	Deactivated
□	Cisco XCP XMPP Federation Connection Manager	Deactivated
□	Cisco XCP Message Archiver	Deactivated
☑	Cisco XCP Directory Service	Activated
☑	Cisco XCP Authentication Service	Activated

Database and Admin Services

	Service Name	Activation Status
□	Cisco AXL Web Service	Deactivated
□	Platform SOAP Services	Deactivated
□	Cisco Bulk Provisioning Service	Deactivated

Performance and Monitoring Services

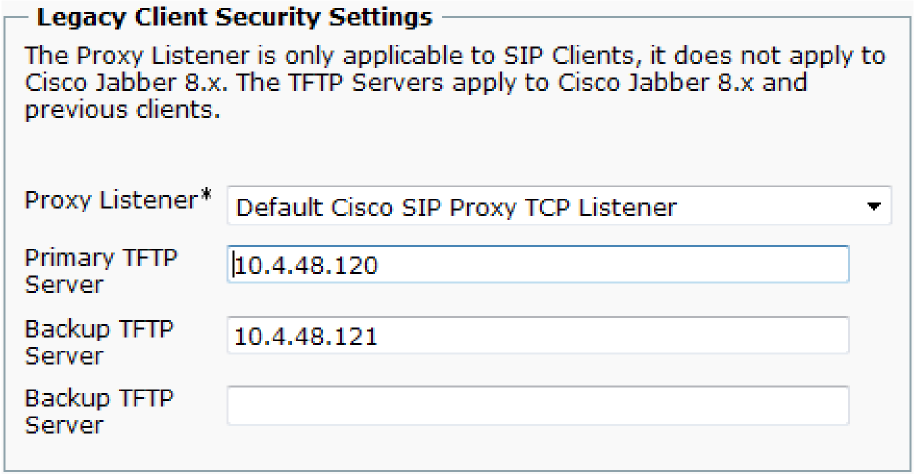
	Service Name	Activation Status
□	Cisco Serviceability Reporter	Deactivated

Step 10: In the message window, click OK.

Step 11: In the Navigation list at the top right of the page, choose Cisco Unified CM IM and Presence Administration, and then click Go.

Step 12: Navigate to **Application > Legacy Clients > Settings**, enter the following information, and then click **Save**:

- Primary TFTP Server—**10.4.48.120**
- Backup TFTP Server—**10.4.48.121**



Legacy Client Security Settings

The Proxy Listener is only applicable to SIP Clients, it does not apply to Cisco Jabber 8.x. The TFTP Servers apply to Cisco Jabber 8.x and previous clients.

Proxy Listener*	Default Cisco SIP Proxy TCP Listener
Primary TFTP Server	10.4.48.120
Backup TFTP Server	10.4.48.121
Backup TFTP Server	

The initial application administration setup is now complete.

PROCESS

Configuring Services for Cisco Jabber IM and Cisco UC

1. Configure Cisco Unified CM for Jabber IM
2. Configure Unity Connection for Jabber
3. Configure IM and Presence services
4. Configure users for IM and Presence

The next several procedures will create the specific services on Cisco Unified CM, Cisco Unity Connection and the Unified CM IM and Presence servers for Cisco Jabber IM and Cisco UC installations.

Procedure 1 Configure Cisco Unified CM for Jabber IM

When you integrate Cisco Unified Communications Manager and Cisco Unified Communications IM and Presence, you must configure the required services in order to enable communication between the servers. This communication includes a Session Initiation Protocol (SIP) publish trunk in order to enable synchronization of availability status between Cisco Unified Communications Manager and Cisco Unified Communications IM and Presence.

You also create several Cisco UC service profiles and apply them to a service profile for all Cisco Jabber users.

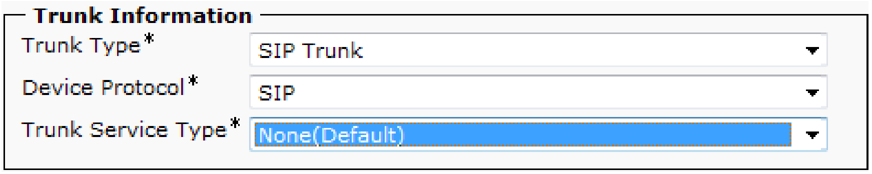
Step 1: In a web browser, access the IP address or hostname of the Cisco Unified CM publisher, and then in the center of the page, under Installed Applications, click **Cisco Unified Communications Manager**.

Step 2: Enter the application username and password, and then click **Login**.

Step 3: Navigate to **Device > Trunk**, and then click **Add New**.

Step 4: On the Trunk Configuration page, enter the following values, and then click **Next**:

- Trunk Type—**SIP Trunk**
- Device Protocol—**SIP**
- Trunk Service Type—**None (Default)**

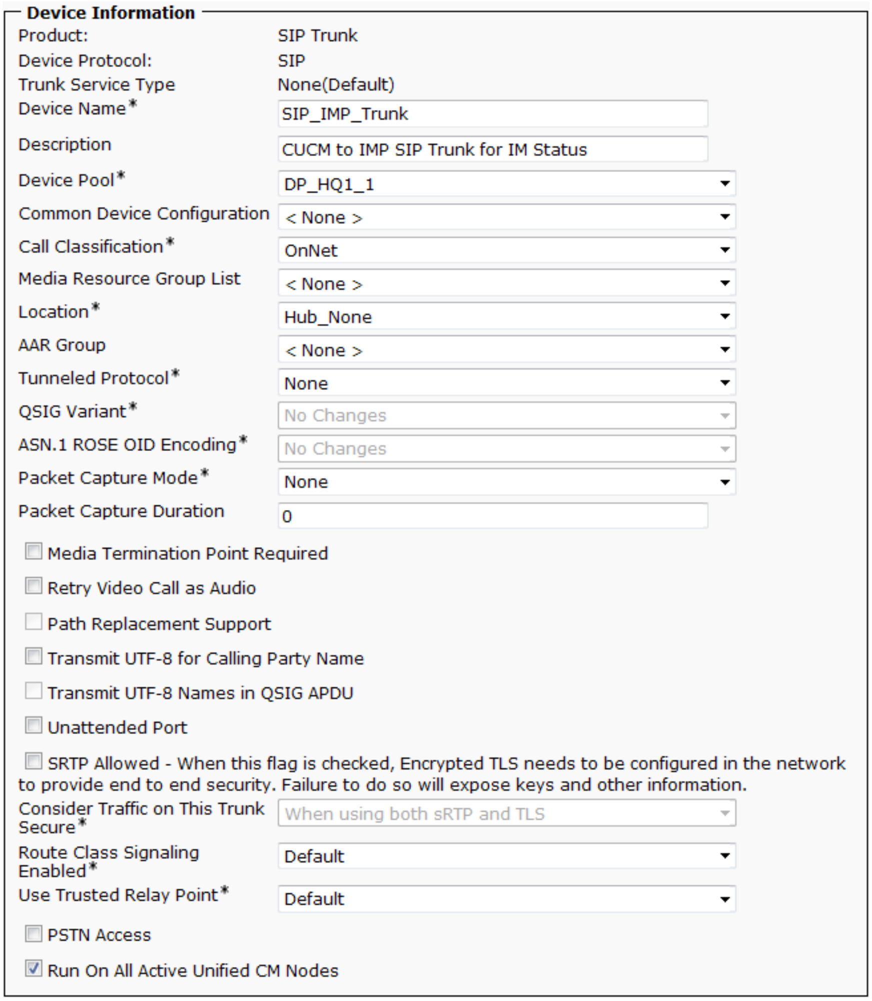


Trunk Information

Trunk Type*	SIP Trunk
Device Protocol*	SIP
Trunk Service Type*	None(Default)

Step 5: On the next page, in the Device Information section, enter the following values:

- Device Name—**SIP_IMP_Trunk**
- Description—**CUCM to IMP SIP Trunk for IM Status**
- Device Pool—**DP_HQ1_1**
- Call Classification—**OnNet**
- Location—**Hub_None**
- Run On All Active Unified CM Nodes—**Select**



Device Information

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	SIP_IMP_Trunk
Description	CUCM to IMP SIP Trunk for IM Status
Device Pool*	DP_HQ1_1
Common Device Configuration	< None >
Call Classification*	OnNet
Media Resource Group List	< None >
Location*	Hub_None
AAR Group	< None >
Tunneled Protocol*	None
QSIG Variant*	No Changes
ASN.1 ROSE OID Encoding*	No Changes
Packet Capture Mode*	None
Packet Capture Duration	0

☐ Media Termination Point Required

☐ Retry Video Call as Audio

☐ Path Replacement Support

☐ Transmit UTF-8 for Calling Party Name

☐ Transmit UTF-8 Names in QSIG APDU

☐ Unattended Port

☐ SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.

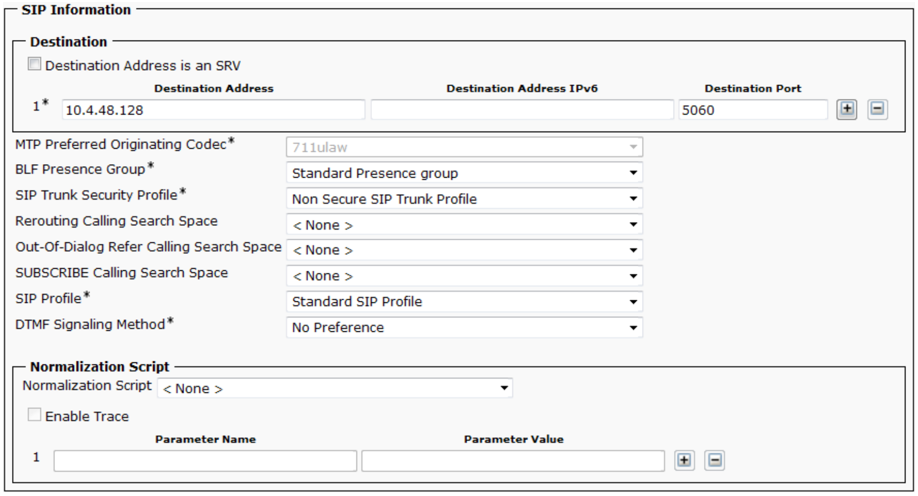
Consider Traffic on This Trunk Secure*	When using both sRTP and TLS
Route Class Signaling Enabled*	Default
Use Trusted Relay Point*	Default

☐ PSTN Access

☑ Run On All Active Unified CM Nodes

Step 6: In the SIP Information section, enter the following values, and then click **Save**:

- Destination Address 1—**10.4.48.128**
- Destination Port 1—**5060**
- SIP Trunk Security Profile—**Non Secure SIP Trunk Profile**
- SIP Profile—**Standard SIP Profile**



SIP Information

Destination

□ Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.4.48.128		5060

MTP Preferred Originating Codec*	711ulaw
BLF Presence Group*	Standard Presence group
SIP Trunk Security Profile*	Non Secure SIP Trunk Profile
Rerouting Calling Search Space	< None >
Out-Of-Dialog Refer Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile
DTMF Signaling Method*	No Preference

Normalization Script

Normalization Script < None >

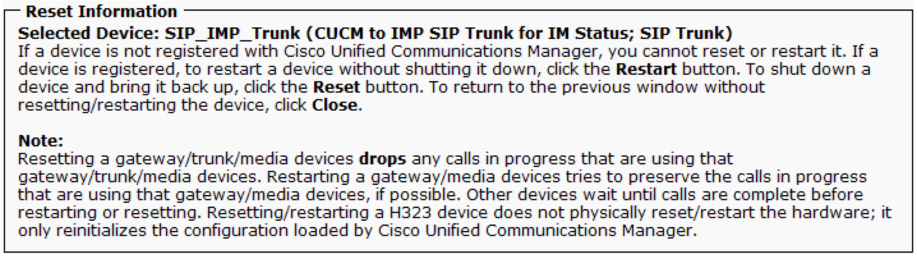
□ Enable Trace

	Parameter Name	Parameter Value
1		

Step 7: In the Message window, click **OK**.

Step 8: On the Trunk Configuration page, click **Reset**.

Step 9: On the Device Reset page, click **Reset**, and then click **Close**.



Reset Information

Selected Device: SIP_IMP_Trunk (CUCM to IMP SIP Trunk for IM Status; SIP Trunk)

If a device is not registered with Cisco Unified Communications Manager, you cannot reset or restart it. If a device is registered, to restart a device without shutting it down, click the **Restart** button. To shut down a device and bring it back up, click the **Reset** button. To return to the previous window without resetting/restarting the device, click **Close**.

Note:

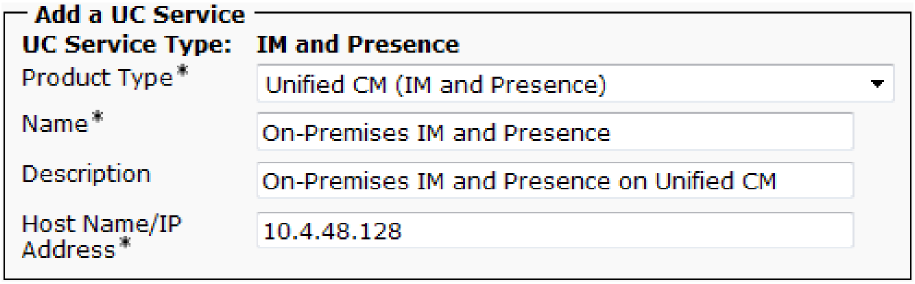
Resetting a gateway/trunk/media devices **drops** any calls in progress that are using that gateway/trunk/media devices. Restarting a gateway/media devices tries to preserve the calls in progress that are using that gateway/media devices, if possible. Other devices wait until calls are complete before restarting or resetting. Resetting/restarting a H323 device does not physically reset/restart the hardware; it only reinitializes the configuration loaded by Cisco Unified Communications Manager.

Step 10: Navigate to **User Management > User Settings > UC Service**, and then click **Add New**.

Step 11: On the UC Service Configuration page, in the UC Service Type list, select **IM and Presence**, and then click **Next**.

Step 12: In the Add a UC Service section, enter the following information, and then click **Save**:

- Product Type—**Unified CM (IM and Presence)**
- Name—**On-Premises IM and Presence**
- Description—**On-Premises IM and Presence on Unified CM**
- Host Name/IP Address—**10.4.48.128**



Add a UC Service

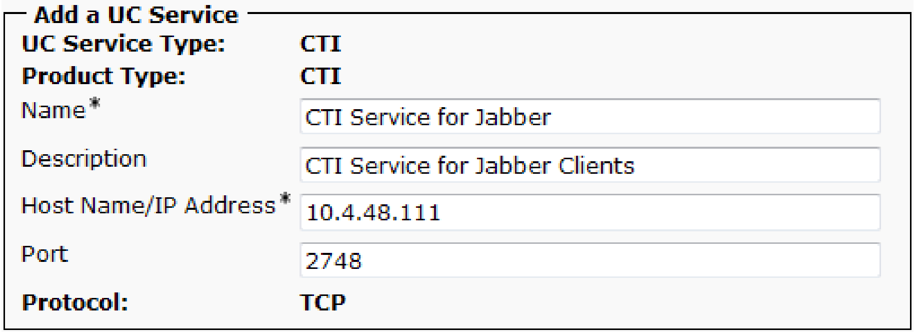
UC Service Type:	**IM and Presence**
Product Type*	Unified CM (IM and Presence)
Name*	On-Premises IM and Presence
Description	On-Premises IM and Presence on Unified CM
Host Name/IP Address*	10.4.48.128

Step 13: Navigate to **User Management > User Settings > UC Service**, and then click **Add New**.

Step 14: On the UC Service Configuration page, in the UC Service Type list, select **CTI**, and then click **Next**.

Step 15: In the Add a UC Service section, enter the following information, and then click **Save**:

- Name—**CTI Service for Jabber**
- Description—**CTI Service for Jabber Clients**
- Host Name/IP Address—**10.4.48.111** (Subscriber 1)
- Port—**2748**



Add a UC Service

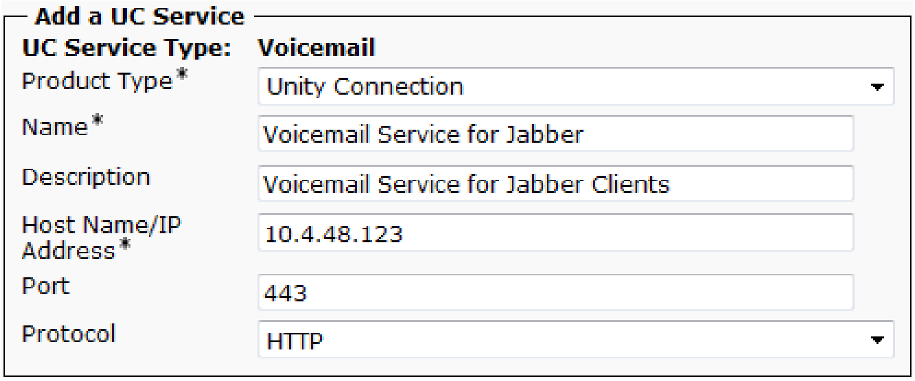
UC Service Type:	**CTI**
Product Type:	**CTI**
Name*	CTI Service for Jabber
Description	CTI Service for Jabber Clients
Host Name/IP Address*	10.4.48.111
Port	2748
Protocol:	**TCP**

Step 16: Navigate to **User Management > User Settings > UC Service**, and then click **Add New**.

Step 17: On the UC Service Configuration page, in the UC Service Type list, select **Voicemail**, and then click **Next**.

Step 18: In the Add a UC Service section, enter the following information, and then click **Save**:

- Product Type—**Unity Connection**
- Name—**Voicemail Service for Jabber**
- Description—**Voicemail Service for Jabber Clients**
- Host Name/IP Address—**10.4.48.123**
- Port—**443**
- Protocol—**HTTP**


Add a UC Service

UC Service Type:	**Voicemail**
Product Type*	Unity Connection
Name*	Voicemail Service for Jabber
Description	Voicemail Service for Jabber Clients
Host Name/IP Address*	10.4.48.123
Port	443
Protocol	HTTP

Step 19: Navigate to **User Management > User Settings > UC Service**, and then click **Add New**.

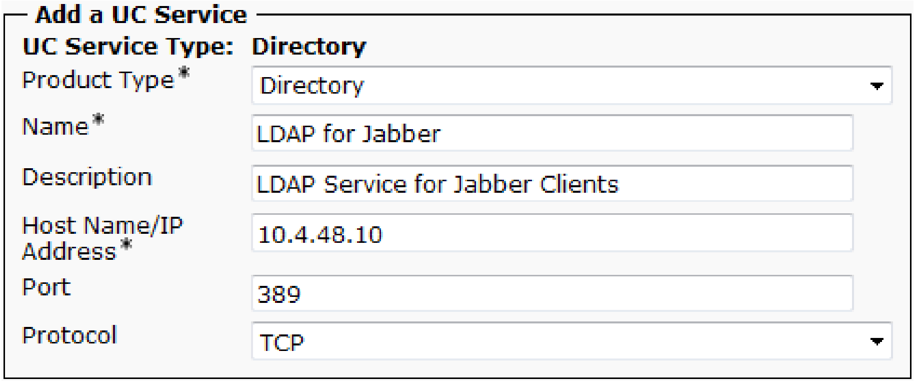
Step 20: On the UC Service Configuration page, in the UC Service Type list, select **Directory**, and then click **Next**.

Tech Tip

When using an LDAP directory service, the Cisco Jabber client's click-to-call the phone number that is listed in the Telephone Number attribute of LDAP. This may or may not be the same attribute that was used when you synchronized your users with Cisco Unified CM.

Step 21: In the Add a UC Service section, enter the following information, and then click **Save**:

- Product Type—**Directory**
- Name—**LDAP for Jabber**
- Description—**LDAP Service for Jabber Clients**
- Host Name/IP Address—**10.4.48.10**
- Port—**389**
- Protocol—**TCP**



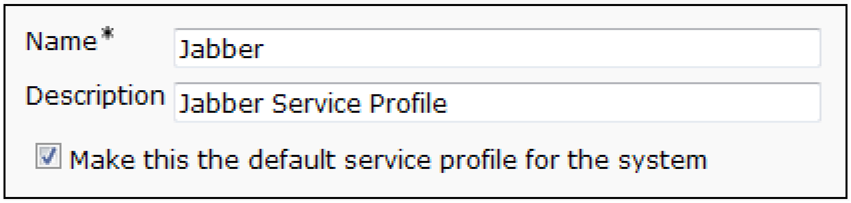
Add a UC Service

UC Service Type: Directory

Product Type*	Directory
Name*	LDAP for Jabber
Description	LDAP Service for Jabber Clients
Host Name/IP Address*	10.4.48.10
Port	389
Protocol	TCP

Step 22: Navigate to **User Management > User Settings > Service Profile**, click **Add New**, and then enter the following information:

- Name—**Jabber**
- Description—**Jabber Service Profile**
- Make this the default service profile for the system—**Select**

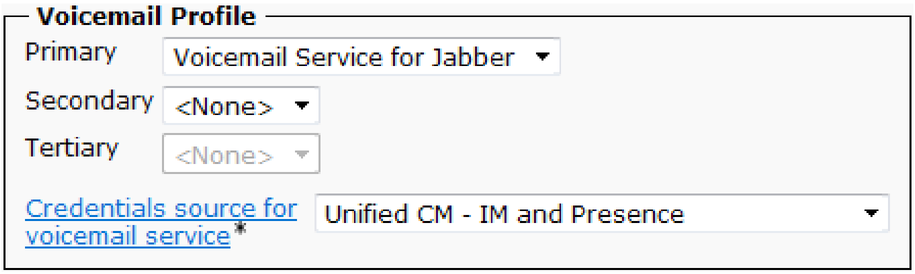


Name*	Jabber
Description	Jabber Service Profile

☑ Make this the default service profile for the system

Step 23: In the Voicemail Profile section, enter the following information:

- Primary—**Voicemail Service for Jabber**
- Credential source for voicemail service—**Unified CM - IM and Presence**

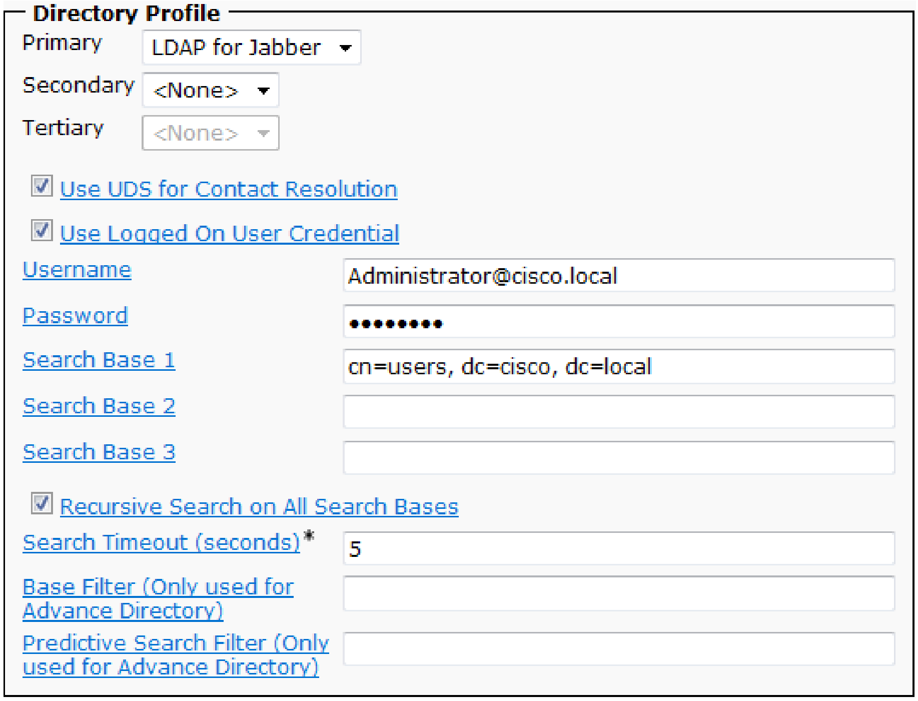


Voicemail Profile

Primary	Voicemail Service for Jabber
Secondary	<None>
Tertiary	<None>
Credentials source for voicemail service*	Unified CM - IM and Presence

Step 24: In the Directory Profile section, enter the following information:

- Primary—**LDAP for Jabber**
- Use UDS for Contact Resolution—**Select**
- Use Logged On User Credential—**Select**
- Username—**Administrator@cisco.local**
- Password—**[password]**
- Search Base 1—**cn=users, dc=cisco, dc=local**



Directory Profile

Primary	LDAP for Jabber
Secondary	<None>
Tertiary	<None>

☑ Use UDS for Contact Resolution

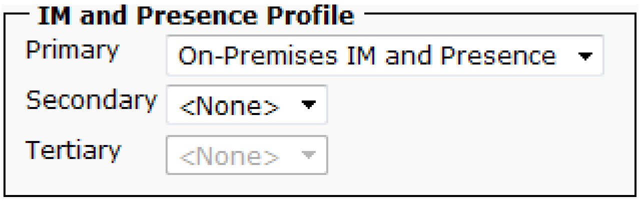
☑ Use Logged On User Credential

Username	Administrator@cisco.local
Password	••••••••
Search Base 1	cn=users, dc=cisco, dc=local
Search Base 2	
Search Base 3	

☑ Recursive Search on All Search Bases

Search Timeout (seconds)*	5
Base Filter (Only used for Advance Directory)	
Predictive Search Filter (Only used for Advance Directory)	

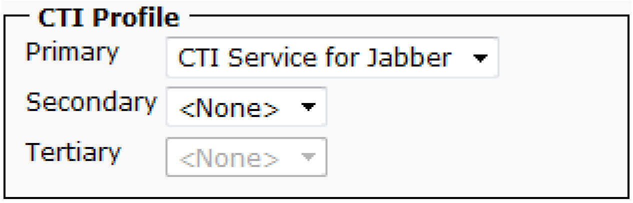
Step 25: In the IM and Presence Profile section, in the **Primary** list, choose **On-Premises IM and Presence**.



IM and Presence Profile

Primary	On-Premises IM and Presence
Secondary	<None>
Tertiary	<None>

Step 26: In the CTI Profile section, in the **Primary** list, choose **CTI Service for Jabber**, and then click **Save**.



CTI Profile

Primary	CTI Service for Jabber
Secondary	<None>
Tertiary	<None>

Procedure 2 Configure Unity Connection for Jabber

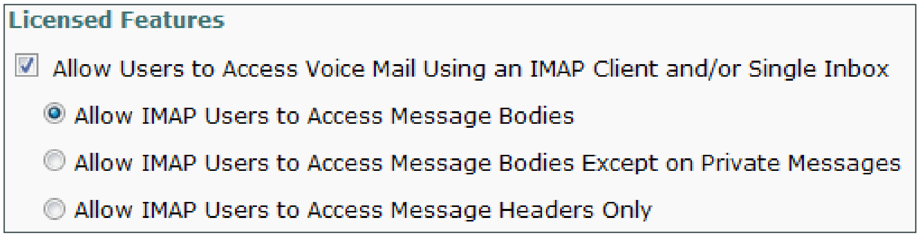
The next set of steps will configure Cisco Unity Connection for use with Jabber.

Step 1: In a web browser, access the Cisco Unity Connection administration interface, and then in the center of the page, under Installed Applications, click **Cisco Unity Connection**.

Step 2: Enter the application administrator username and password, and then click **Login**.

Step 3: Navigate to **Class of Service > Class of Service** and then click **Voice Mail User COS**.

Step 4: On the Edit Class of Service (Voice Mail user COS) page, in the Licensed Features section, select **Allow users to Access Voice Mail Using IMPA Client and/or Single Inbox**, select **Allow IMAP Users to Access Message Bodies**, and then click **Save**.



Licensed Features

☑ Allow Users to Access Voice Mail Using an IMAP Client and/or Single Inbox

● Allow IMAP Users to Access Message Bodies

○ Allow IMAP Users to Access Message Bodies Except on Private Messages

○ Allow IMAP Users to Access Message Headers Only

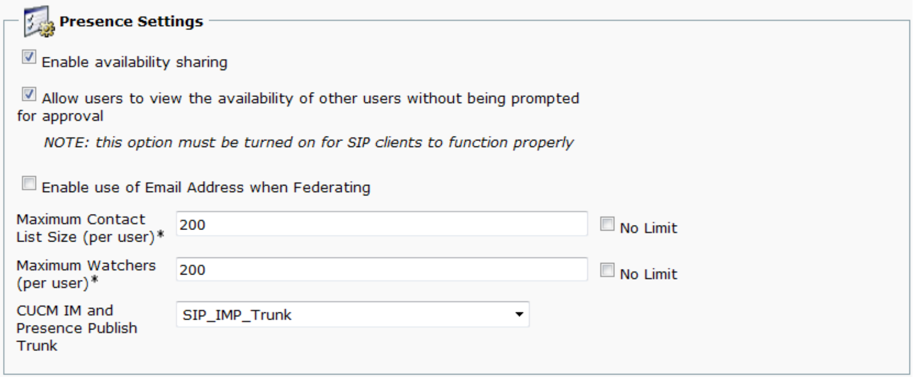
Procedure 3 Configure IM and Presence services

This procedure configures Cisco Unified CM IM and Presence with a publish trunk, presence gateway, and a Cisco Unified Communications Manager IP phone service profile.

Step 1: In a web browser, access the IP address or hostname of the Cisco Unified CM IM and Presence server, and then in the center of the page under Administrative Applications, click **Cisco Unified Communications Manager IM and Presence**.

Step 2: Enter the name and password you entered on the Application User Configuration page in Step 21 of Procedure 1 "Install Cisco Unified CM IM and Presence," and then click **Login**.

Step 3: Navigate to **Presence > Settings**, and in the CUCM IM and Presence Publish Trunk list, choose **SIP_IMP_Trunk**, and then click **Save**.



Presence Settings

☑ Enable availability sharing

☑ Allow users to view the availability of other users without being prompted for approval

NOTE: this option must be turned on for SIP clients to function properly

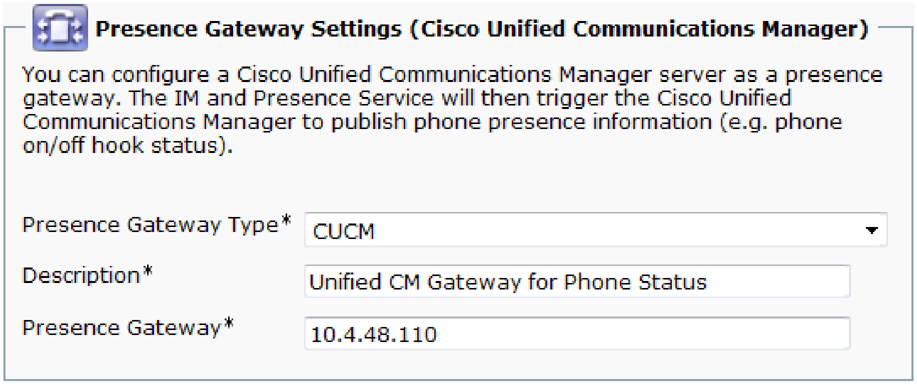
☐ Enable use of Email Address when Federating

Maximum Contact List Size (per user)*	200	☐ No Limit
Maximum Watchers (per user)*	200	☐ No Limit
CUCM IM and Presence Publish Trunk	SIP_IMP_Trunk	

Step 4: Navigate to Presence > Gateways, and then click Add New.

Step 5: On the Presence Gateway Configuration page, enter the following information, and then click Save:

- Presence Gateway Type—**CUCM**
- Description—**Unified CM Gateway for Phone Status**
- Presence Gateway—**10.4.48.110** (publisher)



Presence Gateway Settings (Cisco Unified Communications Manager)

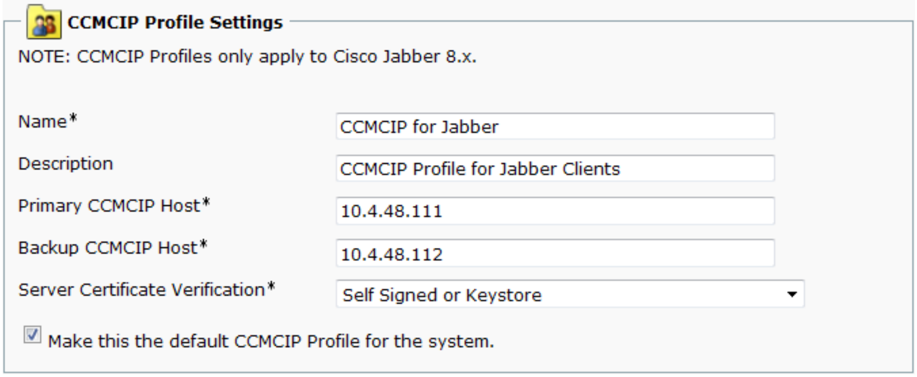
You can configure a Cisco Unified Communications Manager server as a presence gateway. The IM and Presence Service will then trigger the Cisco Unified Communications Manager to publish phone presence information (e.g. phone on/off hook status).

Presence Gateway Type*	CUCM
Description*	Unified CM Gateway for Phone Status
Presence Gateway*	10.4.48.110

Step 6: Navigate to Application > Legacy Clients > CCMCIP Profile, and then click Add New.

Step 7: On the CCMCIP Profile Configuration page, enter the following information, and then click Save:

- Name—**CCMCIP for Jabber**
- Description—**CCMCIP Profile for Jabber Clients**
- Primary CCMCIP Host—**10.4.48.111** (subscriber 1)
- Backup CCMCIP Host—**10.4.48.112** (subscriber 2)
- Server Certificate Verification—**Self Signed or Keystore**
- Make this the default CCMCIP Profile for the system—**Select**



CCMCIP Profile Settings

NOTE: CCMCIP Profiles only apply to Cisco Jabber 8.x.

Name*	CCMCIP for Jabber
Description	CCMCIP Profile for Jabber Clients
Primary CCMCIP Host*	10.4.48.111
Backup CCMCIP Host*	10.4.48.112
Server Certificate Verification*	Self Signed or Keystore

☑ Make this the default CCMCIP Profile for the system.

Step 8: In the message window, click OK.

Procedure 4 Configure users for IM and Presence

This procedure will configure Cisco Unified CM for Cisco Jabber for Windows, Jabber for iPad, and Jabber for iPhone users who require these capabilities.

Step 1: In a web browser, access the IP address or hostname of the Cisco Unified CM publisher, and then in the center of the page, under Installed Applications, click **Cisco Unified Communications Manager**.

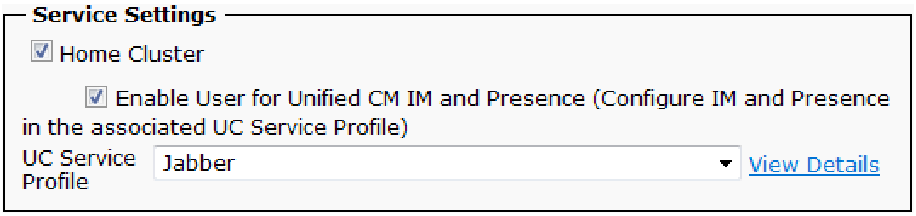
Step 2: Enter the Unified CM application username and password, and then click **Login**.

Step 3: Navigate to **User Management > End User**, and then click **Find**.

Step 4: Find the appropriate Cisco Jabber user, and then click the username.

Step 5: In the Service Settings section, enter the following information, and then click **Save**:

- Home Cluster—**Select**
- Enable User for Unified CM IM and Presence—**Select**
- UC Service Profile—**Jabber**



Service Settings

☑ Home Cluster

☑ Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)

UC Service Profile: Jabber

Step 6: In the Permissions Information section, select **Add to Access Control Group**.

Step 7: On the Find and List Access Control Groups page, click **Find**, and then select the following groups:

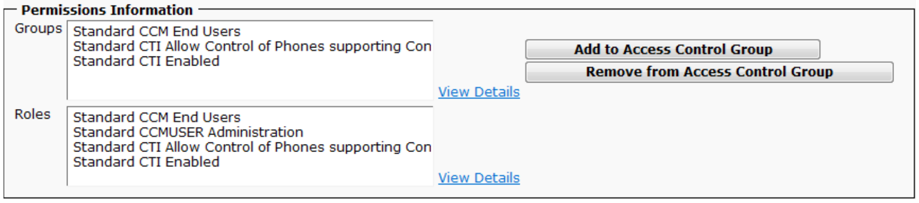
- Access Control Group—**Standard CCM End users** (existing)
- Access Control Group—**Standard CTI Enabled**

Step 8: If you are using one of the following phone models, select the appropriate additional control group:

- Cisco Unified IP Phone 9900 Series—**Standard CTI Allow Control of Phones supporting Connected Xfer and conf**
- Cisco Unified IP Phone 6900 Series—**Standard CTI Allow Control of Phones supporting Rollover Mode**

Step 9: Click **Add Selected**.

Step 10: On the End User Configuration page, click **Save**.



Permissions Information

Groups: Standard CCM End Users
Standard CTI Allow Control of Phones supporting Con
Standard CTI Enabled

Roles: Standard CCM End Users
Standard CCMUSER Administration
Standard CTI Allow Control of Phones supporting Con
Standard CTI Enabled

Step 11: Repeat Step 3 through Step 10 for each additional Cisco Jabber for Windows, Jabber for iPad, and Jabber for iPhone user.

PROCESS

Configuring Cisco Jabber for Windows

1. Configure Profiles in Unified CM
2. Configure Jabber for Windows softphones
3. Configure Jabber for Windows users
4. Download and install Jabber for Windows

This process is only necessary if you plan to deploy Cisco Jabber for Windows.

In this process, you configure Cisco Unified CM to enable unified communications on Cisco Jabber for Windows clients. You also download and install Cisco Jabber for Windows and the Cisco Media Services Interface software to a user's laptop or desktop computer.

Procedure 1 Configure Profiles in Unified CM

To enable unified communications with voice and video calling capabilities from Cisco Unified CM, a software phone device is required for each Cisco Jabber for Windows user.

The first stage in building a software phone device is to create a SIP profile enabling video desktop sharing. You cannot edit or configure the default SIP profile, so you create a new SIP profile from the default and modify the specific settings.

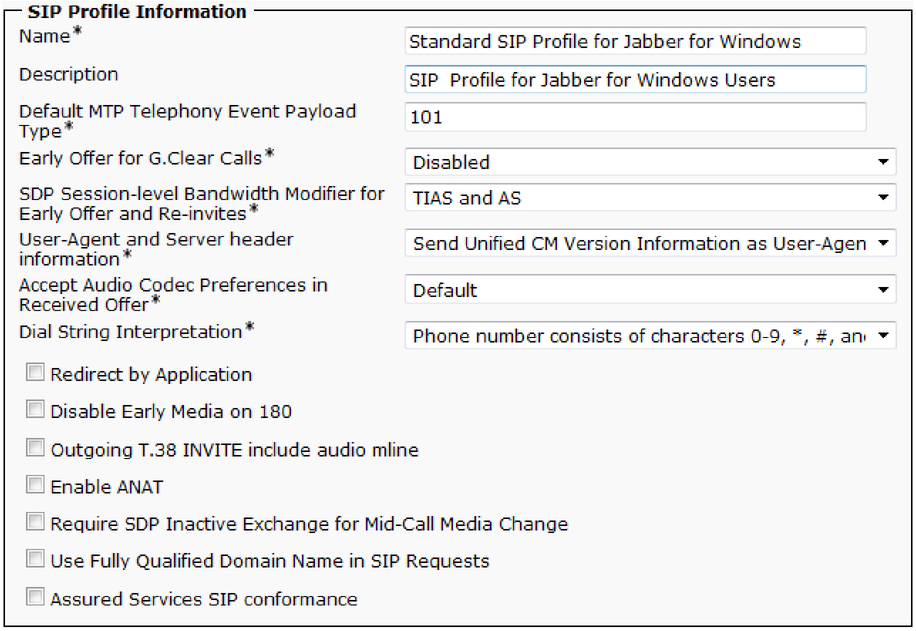
You also modify the default standard common phone profile in order to enable Real-time Transport Control Protocol (RTCP).

Step 1: Navigate to **Device > Device Settings > SIP Profile**, and then click **Find**.

Step 2: Locate **Standard SIP Profile**, and then on the right side of the page in line with the profile, click the **Copy** icon.

Step 3: On the SIP Profile Configuration page, in the SIP Profile Information section, enter the following information:

- Name—**Standard SIP Profile for Jabber for Windows**
- Description—**SIP Profile for Jabber for Windows Users**



SIP Profile Information

Name*	Standard SIP Profile for Jabber for Windows
Description	SIP Profile for Jabber for Windows Users
Default MTP Telephony Event Payload Type*	101
Early Offer for G.Clear Calls*	Disabled
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites*	TIAS and AS
User-Agent and Server header information*	Send Unified CM Version Information as User-Agen
Accept Audio Codec Preferences in Received Offer*	Default
Dial String Interpretation*	Phone number consists of characters 0-9, *, #, an

☐ Redirect by Application

☐ Disable Early Media on 180

☐ Outgoing T.38 INVITE include audio mline

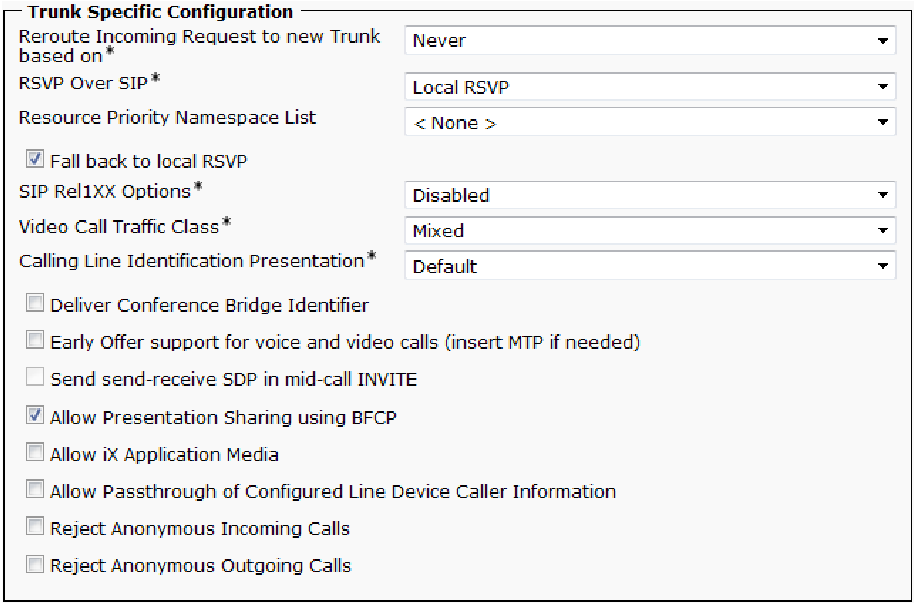
☐ Enable ANAT

☐ Require SDP Inactive Exchange for Mid-Call Media Change

☐ Use Fully Qualified Domain Name in SIP Requests

☐ Assured Services SIP conformance

Step 4: In the Trunk Specific Configuration section, select Allow Presentation Sharing using BFCP, and then click Save.



Trunk Specific Configuration

Reroute Incoming Request to new Trunk based on*	Never
RSVP Over SIP*	Local RSVP
Resource Priority Namespace List	< None >

☑ Fall back to local RSVP

SIP Rel1XX Options*	Disabled
Video Call Traffic Class*	Mixed
Calling Line Identification Presentation*	Default

☐ Deliver Conference Bridge Identifier

☐ Early Offer support for voice and video calls (insert MTP if needed)

☐ Send send-receive SDP in mid-call INVITE

☑ Allow Presentation Sharing using BFCP

☐ Allow iX Application Media

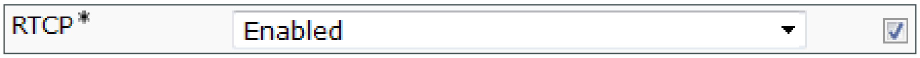
☐ Allow Passthrough of Configured Line Device Caller Information

☐ Reject Anonymous Incoming Calls

☐ Reject Anonymous Outgoing Calls

Step 5: Navigate to Device > Device Settings > Common Phone Profile, click Find, and then click Standard Common Phone Profile.

Step 6: In the Product Specific Configurations Layout section, in the **RTCP** list, choose **Enabled**, and then click **Save**.



RTCP*	Enabled	☑

Step 7: On the Common Phone Profile Configuration page, click **Reset**, and then on the Device Reset page, click **Reset**.

Step 8: Click **Close** to return to the previous page.

Procedure 2 Configure Jabber for Windows softphones

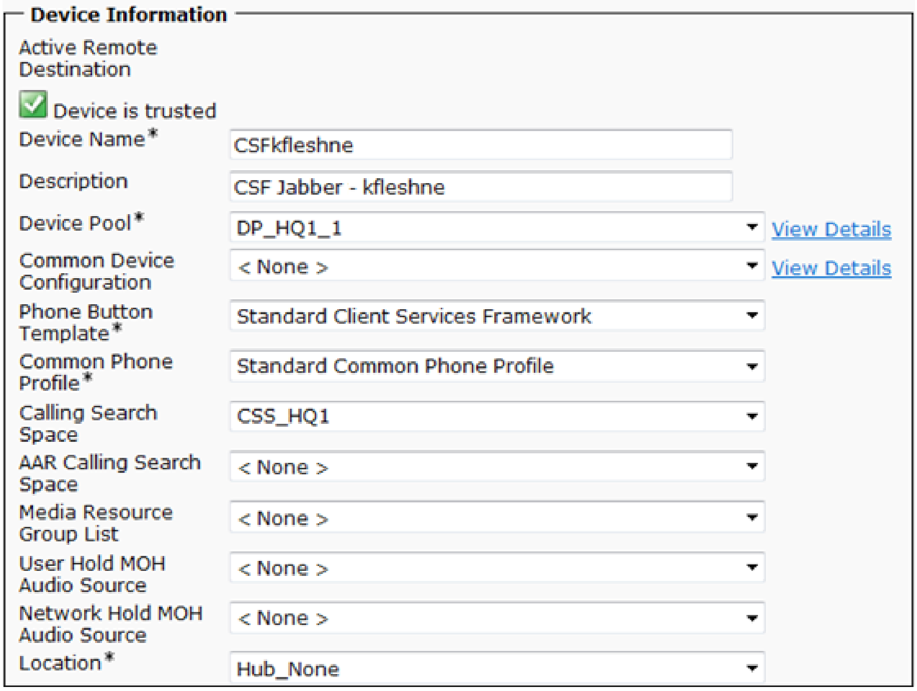
The Client Service Framework (CSF) phone type is used within Cisco Unified CM in order to deploy Cisco Jabber for Windows clients that require unified communications.

Step 1: Navigate to **Device > Phone**, and then click **Add New**.

Step 2: In the **Phone Type** list, choose **Cisco Unified Client Services Framework**, and then click **Next**.

Step 3: On the Phone Configuration page, in the Device Information section, enter the following information:

- Device Name—**CSFkfleshne** (uppercase CSF plus username)
- Description—**CSF Jabber - kfleshne**
- Device Pool—**DP_HQ1_1**
- Phone Button Template—**Standard Client Services Framework**
- Common Phone Profile—**Standard Common Phone Profile**
- Calling Search Space—**CSS_HQ1**
- Location—**Hub_None**



Device Information

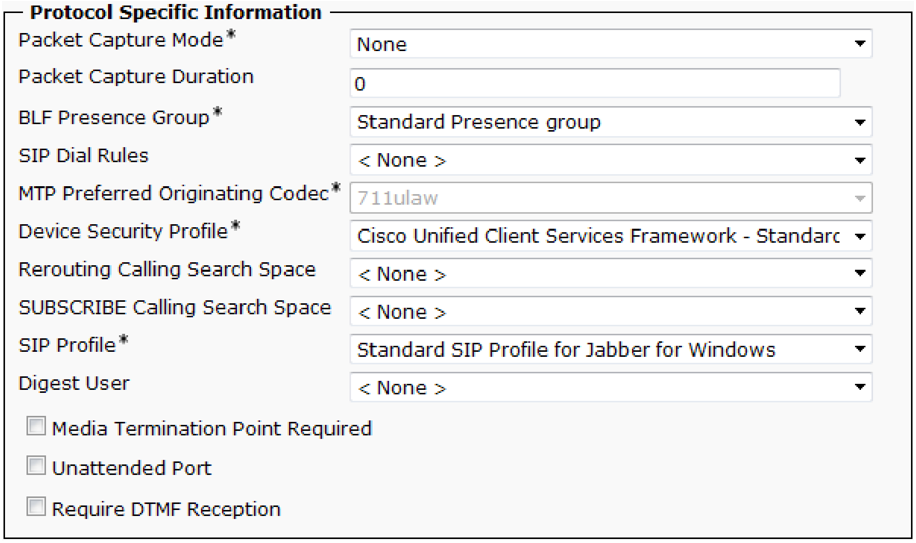
Active Remote Destination

☑ Device is trusted

Device Name*	CSFkfleshne	
Description	CSF Jabber - kfleshne	
Device Pool*	DP_HQ1_1	View Details
Common Device Configuration	< None >	View Details
Phone Button Template*	Standard Client Services Framework	
Common Phone Profile*	Standard Common Phone Profile	
Calling Search Space	CSS_HQ1	
AAR Calling Search Space	< None >	
Media Resource Group List	< None >	
User Hold MOH Audio Source	< None >	
Network Hold MOH Audio Source	< None >	
Location*	Hub_None	

Step 4: In the Protocol Specific Information section, enter the following information, and then click **Save**:

- Device Security Profile—**Cisco Unified Client Services Framework - Standard SIP Non-Secure**
- SIP Profile—**Standard SIP Profile for Jabber for Windows**



Protocol Specific Information

Packet Capture Mode*	None
Packet Capture Duration	0
BLF Presence Group*	Standard Presence group
SIP Dial Rules	< None >
MTP Preferred Originating Codec*	711ulaw
Device Security Profile*	Cisco Unified Client Services Framework - Standarc
Rerouting Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile for Jabber for Windows
Digest User	< None >

□ Media Termination Point Required

□ Unattended Port

□ Require DTMF Reception

Step 5: On the Phone Configuration page, in the Association Information section, click **Line [1] - Add a new DN**.

Tech Tip

When using an LDAP directory service, the Cisco Jabber client's click-to-call the phone number that is listed in the Telephone Number attribute of LDAP.

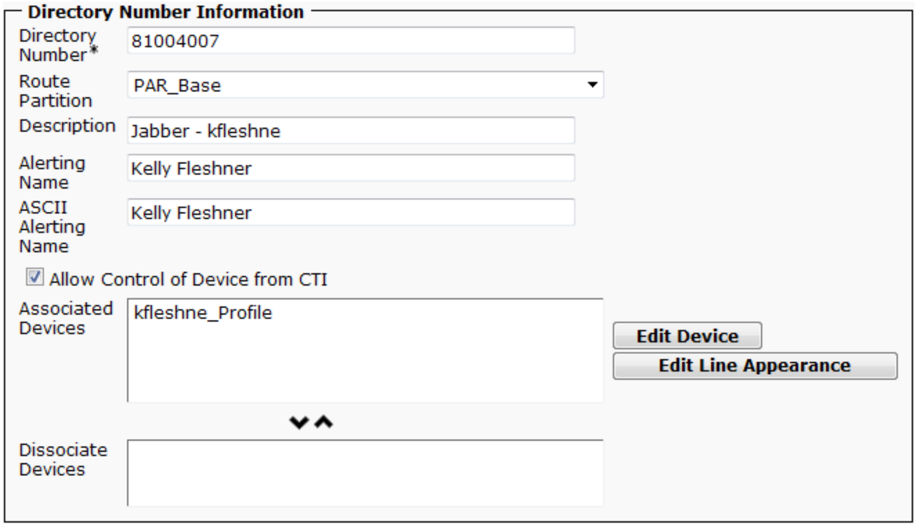
Confirm that the Telephone Number attribute in your LDAP implementation matches the Directory Number used in Cisco Unified CM for your Cisco Jabber client.

Figure 3 has an example of the LDAP General Information page in Microsoft Active Directory.

Step 6: On the Directory Number Configuration page, enter the following values:

- Directory Number—**81004007**
- Route Partition—**PAR_Base**
- Description—**Jabber - kfleshne**
- Alerting Name—**[Alerting name]**
- ASCII Alerting Name—**[ASCII alerting name]**
- Allow Control of Device from CTI—**Select**

Figure 2 - Cisco Unified CM Directory Number information



Directory Number Information

Directory Number* 81004007

Route Partition PAR_Base

Description Jabber - kfleshne

Alerting Name Kelly Fleshner

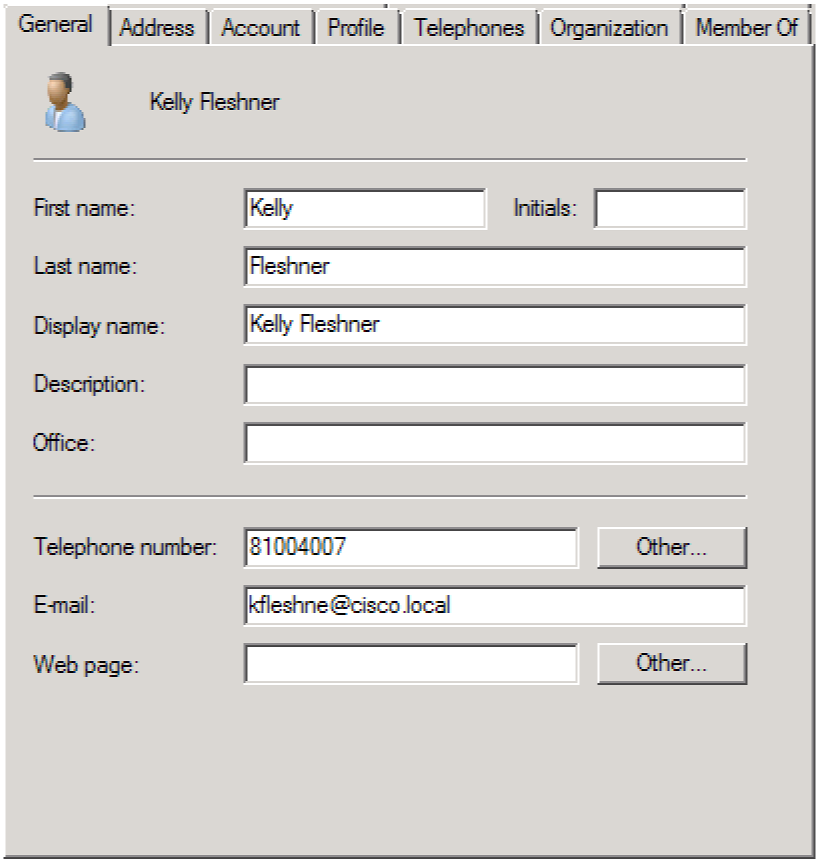
ASCII Alerting Name Kelly Fleshner

☑ Allow Control of Device from CTI

Associated Devices kfleshne_Profile

Dissociate Devices

Figure 3 - Example LDAP general information telephone number attribute

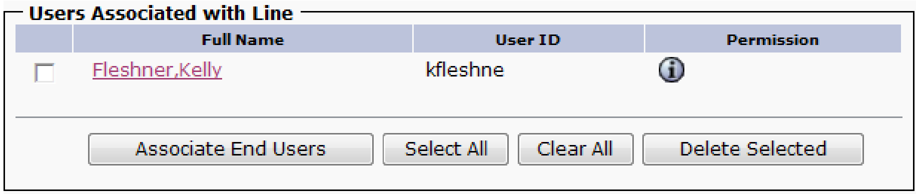


Kelly Fleshner

First name:	Kelly	Initials:	
Last name:	Fleshner		
Display name:	Kelly Fleshner		
Description:			
Office:			
Telephone number:	81004007		
E-mail:	kfleshne@cisco.local		
Web page:			

Step 7: In the Users Associated with Line section at the bottom of the page, click **Associate End Users**, and then click **Find**.

Step 8: Select the Cisco Jabber user, click **Add Selected**, and then click **Save**.



Users Associated with Line

	Full Name	User ID	Permission
□	Fleshner,Kelly	kfleshne	ⓘ

Step 9: On the Directory Number Configuration page, click **Apply Config**, and then on the Apply Configuration page, click **OK**.

Procedure 3 Configure Jabber for Windows users

Associate the client services framework device with the end user to allow them to utilize the phone service from Unified CM.

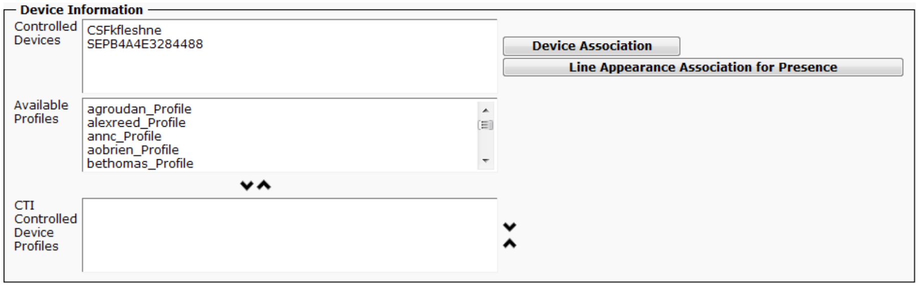
Step 1: Navigate to **User Management > End User**, and then click **Find**.

Step 2: Find the Cisco Jabber user, and then click the username.

Step 3: In the Device Information section, click **Device Association**, and then click **Find**.

Step 4: Select the user's client services framework device (Example: CSFkfleshne), and then click **Save Selected/Changes**.

Step 5: In the Related Links list, choose **Back to User**, and then click **Go**.



Device Information

Controlled Devices: CSFkfleshne
SEPB4A4E3284488

Available Profiles: agroudan_Profile
alexreed_Profile
annc_Profile
aobrien_Profile
bethomas_Profile

CTI Controlled Device Profiles:

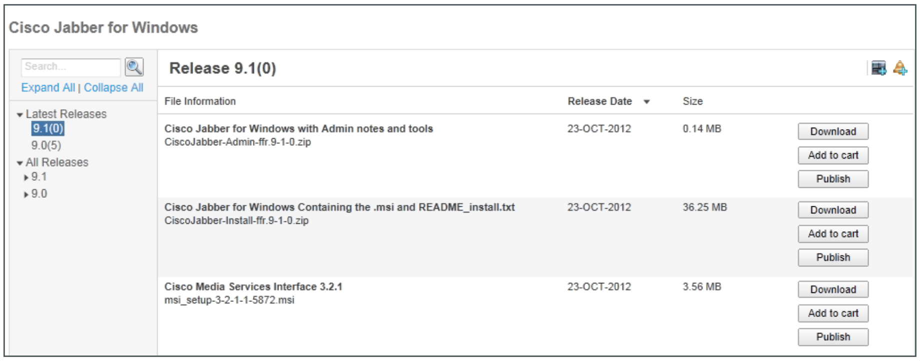
Step 6: Repeat Procedure 2 and Procedure 3 for each Cisco Jabber for Windows user.

Procedure 4 Download and install Jabber for Windows

After adding the software phones into Cisco Unified CM, the users must download the software to their laptop or desktop computers in order to begin using Cisco Jabber for Windows.

Step 1: In a browser, access http://www.cisco.com/, login using your Cisco.com account name, and then navigate to **Support > All Downloads**.

Step 2: From the Download Home section, navigate to **Voice and Unified Communications > Unified Communications Applications > Unified Communications Clients > Cisco Jabber for Windows**, and then click the latest version.

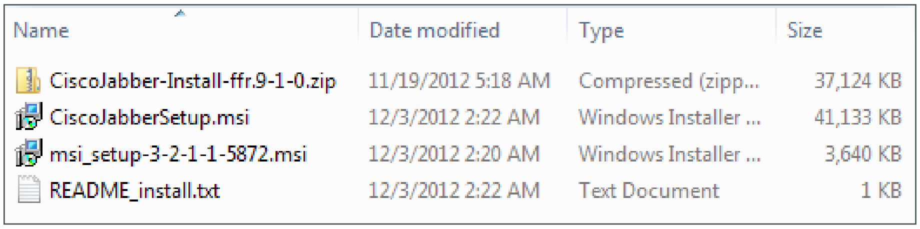


Cisco Jabber for Windows

Release 9.1(0)

File Information	Release Date	Size
Cisco Jabber for Windows with Admin notes and tools CiscoJabber-Admin-ffr.9-1-0.zip	23-OCT-2012	0.14 MB
Cisco Jabber for Windows Containing the .msi and README_install.txt CiscoJabber-Install-ffr.9-1-0.zip	23-OCT-2012	36.25 MB
Cisco Media Services Interface 3.2.1 msi_setup-3-2-1-1-5872.msi	23-OCT-2012	3.56 MB

Step 3: Download the Cisco Jabber for Windows and Cisco Media Services Interface software, and then unzip the Cisco Jabber Install software into the local directory.



Name	Date modified	Type	Size
CiscoJabber-Install-ffr.9-1-0.zip	11/19/2012 5:18 AM	Compressed (zipp...	37,124 KB
CiscoJabberSetup.msi	12/3/2012 2:22 AM	Windows Installer ...	41,133 KB
msi_setup-3-2-1-1-5872.msi	12/3/2012 2:20 AM	Windows Installer ...	3,640 KB
README_install.txt	12/3/2012 2:22 AM	Text Document	1 KB

Step 4: Click on the **msi_setup** file, and then follow the installation instructions in the Cisco Media Services Interface Setup Wizard.

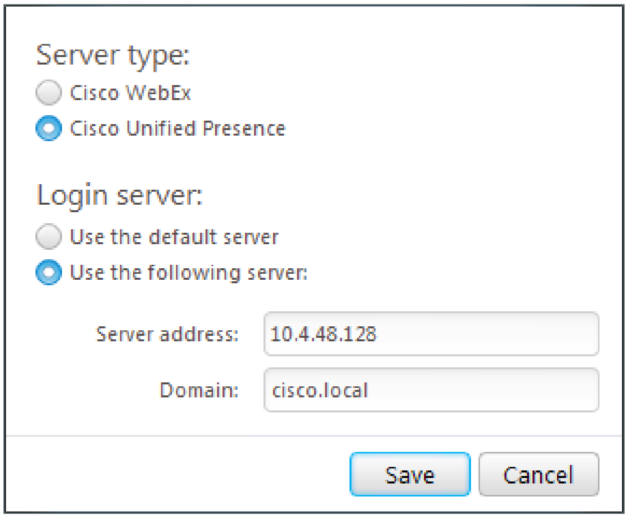
Step 5: Depending on your operating system, you have to accept several security messages as the software installs. After the software installs, click **Finish**.

Step 6: Click the **CiscoJabberSetup.msi** file, and follow the installation instructions in the Cisco Jabber wizard.

Step 7: Depending on your operating system, you have to accept several security messages as the software installs. After the software installs, select **Launch Cisco Jabber**, and then click **Finish**.

Step 8: On the Connection Settings page, enter the following information, and then click **Save**:

- Server type—**Cisco Unified Presence**
- Login server—**Use the following server**
- Server address—**10.4.48.128**
- Domain—**cisco.local**



Server type:

○ Cisco WebEx

● Cisco Unified Presence

Login server:

○ Use the default server

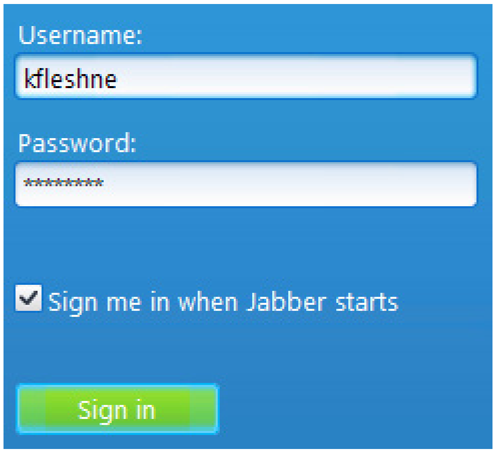
● Use the following server:

Server address: 10.4.48.128

Domain: cisco.local

Step 9: On the login page, enter the following information, and then click **Sign In**:

- Username—**[username]**
- Password—**[password]**
- Sign me in when Jabber Starts—**Select**



Username: kfleshne

Password: *********

☑ Sign me in when Jabber starts

Step 10: Add contacts and favorites as needed.

Step 11: Repeat this procedure for each Cisco Jabber for Windows user.

PROCESS

Configuring Cisco Jabber for iPad

1. Prepare the servers for Jabber for iPad
2. Configure SIP Profile in Unified CM
3. Configure Jabber for iPad softphones
4. Configure Jabber for iPad users
5. Download and install Jabber for iPad

This process is only necessary if you plan to deploy Cisco Jabber for iPad. The procedures for deploying Cisco Jabber for iPhone can be found in the next process.

Configure the Jabber for iPad softphones and users in Cisco Unified CM, and then download and install the Cisco Jabber for iPad software.

Download the latest shipping version of the Cisco Jabber for iPad Cisco Options Package (COP) file and install it on the Cisco Unified CM servers in your cluster. You need a valid Cisco.com account in order to download the COP file. You also need Secure File Transfer Protocol (SFTP) server software in order to safely transfer the file to your Unified CM servers.

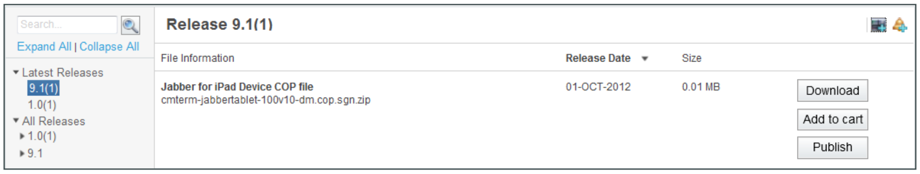
Next, you download the client software to the iPad from the App store and begin the configuration procedure.

Procedure 1 Prepare the servers for Jabber for iPad

In this procedure, after transferring the COP file to the publisher and subscriber servers, you have to restart the Cisco Tomcat service in order to complete the installation. To avoid interruptions in phone service, ensure that each server has returned to active service before you perform this procedure on the next server.

Step 1: In a web browser, access www.cisco.com, login with your user ID, and then navigate to **Support > All Downloads**.

Step 2: On the **Select a Product** page, navigate to **Products > Voice and Unified Communications > Unified Communications Applications > Unified Communications Clients > Cisco Jabber for iPad > Latest Releases**, and then choose to download the compressed version of the **Jabber for iPad Device COP file** to a local directory on your PC.



Release 9.1(1)

File Information	Release Date	Size
Jabber for iPad Device COP file cmterm-jabbertablet-100v10-dm.cop.sgn.zip	01-OCT-2012	0.01 MB

Step 3: Unzip the Jabber for iPad COP file into the local directory on your PC using your favorite file archive program. For example: **7-Zip**.

Step 4: Start the SFTP server software on your PC, and then configure it with a username and password for accessing the downloaded software in a specified directory.

Step 5: In a web browser, access the Cisco Unified CM administration interface of the publisher server in your cluster.

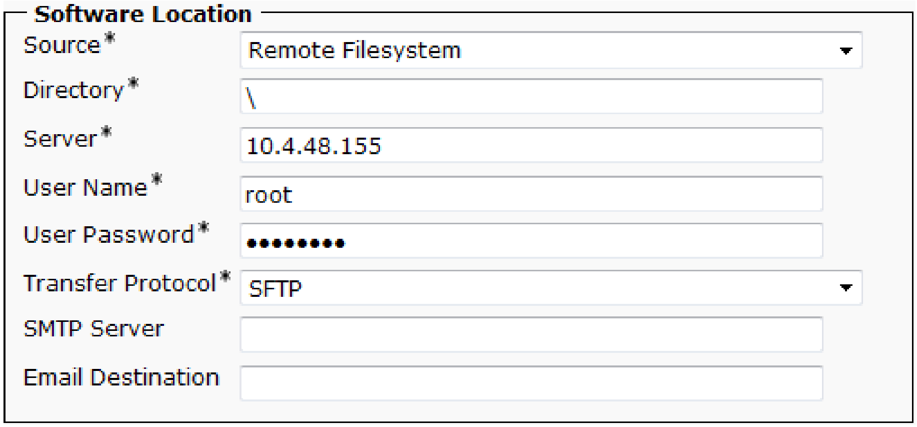
Step 6: In the center of the page, under Installed Applications, click the **Cisco Unified Communications Manager** link.

Step 7: In the Navigation list at the top of the page, choose **Cisco Unified OS Administration**, and then click **Go**.

Step 8: Enter the case-sensitive username and password for the platform administrator, and then click **Login**. For example: **Admin** and **[password]**

Step 9: Navigate to **Software Upgrades > Install/Upgrade**, enter the following information and then, click **Next**:

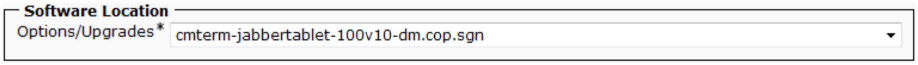
- Source—**Remote Filesystem**
- Directory—****
- Server—**10.4.48.155** (IP address of the PC running SFTP server software)
- User Name—**root** (user name on SFTP PC to access files)
- User Password—**[password]** (user password on SFTP PC to access files)
- Transfer Protocol—**SFTP**



Software Location

Source*	Remote Filesystem
Directory*	\
Server*	10.4.48.155
User Name*	root
User Password*	••••••••
Transfer Protocol*	SFTP
SMTP Server	
Email Destination	

Step 10: In the **Options/Upgrades** list, choose the Cisco Jabber tablet COP file that was extracted from the .zip in Step 3, and then click **Next**.

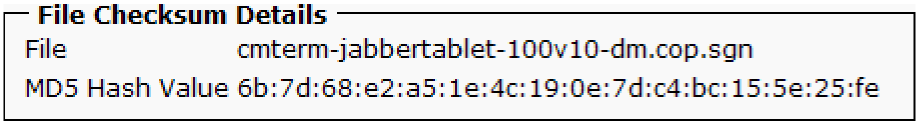


Software Location

Options/Upgrades*	cmterm-jabbertablet-100v10-dm.cop.sgn

Step 11: After the file is downloaded and validated, verify the MD5 Hash Value on the server matches the MD5 Hash Value on your PC.

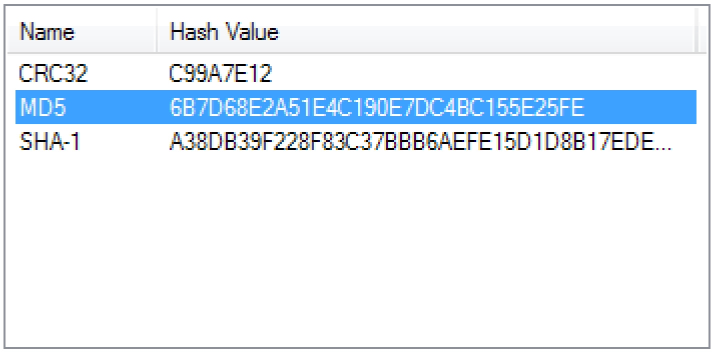
Figure 4 - MD5 Hash Value from Cisco Unified CM



File Checksum Details

File	cmterm-jabbertablet-100v10-dm.cop.sgn
MD5 Hash Value	6b:7d:68:e2:a5:1e:4c:19:0e:7d:c4:bc:15:5e:25:fe

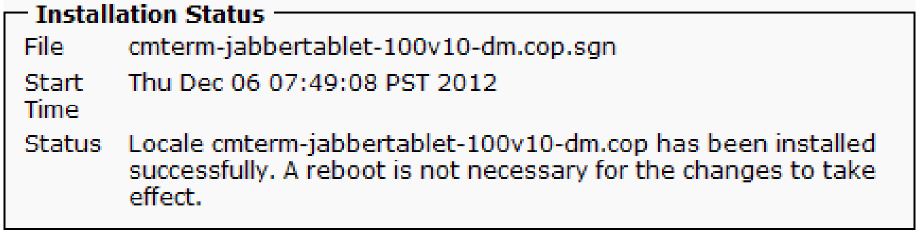
Figure 5 - MD5 Hash Value from your PC



Name	Hash Value
CRC32	C99A7E12
MD5	6B7D68E2A51E4C190E7DC4BC155E25FE
SHA-1	A38DB39F228F83C37BBB6AEFE15D1D8B17EDE...

Step 12: If the MD5 Hash Values do not match, transfer the file again.

If they match, click **Next**, and then confirm the file is successfully installed.



Installation Status

File	cmterm-jabbertablet-100v10-dm.cop.sgn
Start Time	Thu Dec 06 07:49:08 PST 2012
Status	Locale cmterm-jabbertablet-100v10-dm.cop has been installed successfully. A reboot is not necessary for the changes to take effect.

Step 13: Log into the command line interface of the server by using the case-sensitive platform administrator username and password. For example: **Admin** and **[password]**

Step 14: Restart the Cisco Unified CM Cisco Tomcat service from the command line interface. This clears the Tomcat image cache and displays the table device icon properly.

```
utils service restart Cisco Tomcat
```

Step 15: If the service does not restart properly, execute the same command again. Depending on your server hardware, the restart can take up to five minutes. Wait for the service to return to an active state before continuing.

Step 16: Repeat Step 5 through Step 15 for each subscriber server in your cluster.

Procedure 2 Configure SIP Profile in Unified CM

To enable unified communications with voice and video calling capabilities from Cisco Unified CM, a software phone device is required per Cisco Jabber for iPad user.

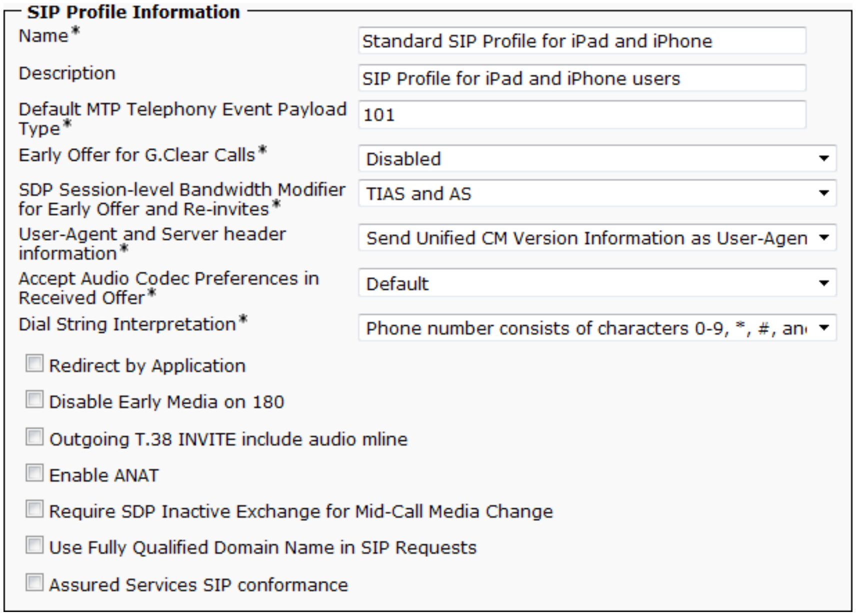
The first stage in building a software phone device is to create a SIP profile that enables the Cisco Jabber for iPad application to run in the background. You cannot edit or configure the default SIP profile, so you must create a new SIP profile from the default and modify the specific settings.

Step 1: Navigate to **Device > Device Settings > SIP Profile**, and then click **Find**.

Step 2: Locate the **Standard SIP Profile**, and then on the right side of the page in line with the profile, click the **Copy** icon.

Step 3: On the SIP Profile Configuration page, in the SIP Profile Information section, enter the following information:

- Name—**Standard SIP Profile for iPad and iPhone**
- Description—**SIP Profile for iPad and iPhone Users**



SIP Profile Information

Name*	Standard SIP Profile for iPad and iPhone
Description	SIP Profile for iPad and iPhone users
Default MTP Telephony Event Payload Type*	101
Early Offer for G.Clear Calls*	Disabled
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites*	TIAS and AS
User-Agent and Server header information*	Send Unified CM Version Information as User-Agen
Accept Audio Codec Preferences in Received Offer*	Default
Dial String Interpretation*	Phone number consists of characters 0-9, *, #, an

☐ Redirect by Application

☐ Disable Early Media on 180

☐ Outgoing T.38 INVITE include audio mline

☐ Enable ANAT

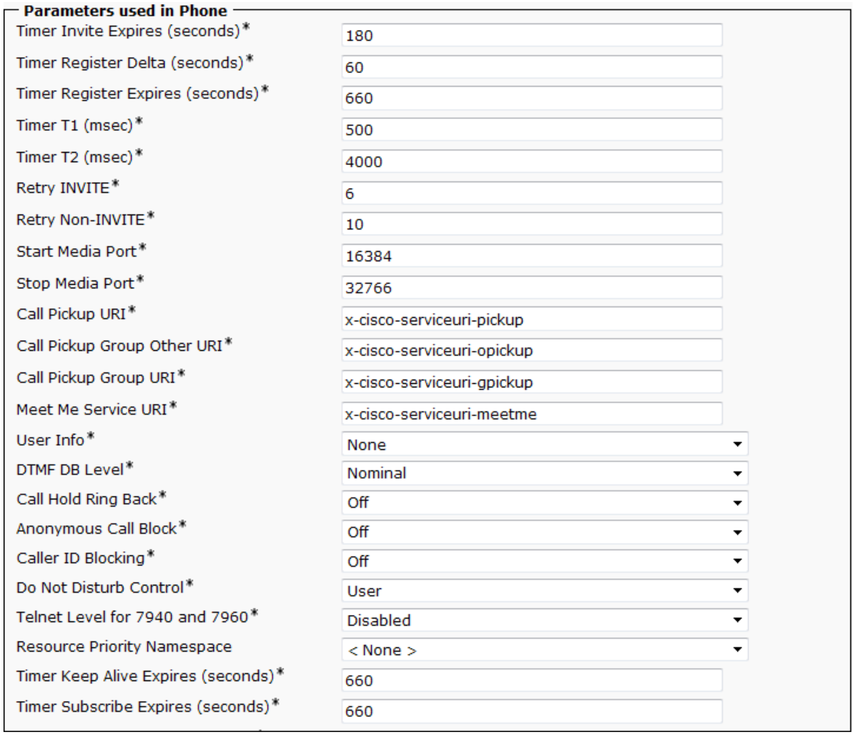
☐ Require SDP Inactive Exchange for Mid-Call Media Change

☐ Use Fully Qualified Domain Name in SIP Requests

☐ Assured Services SIP conformance

Step 4: In the Parameters Used in Phone section, enter the following information, and then click **Save**:

- Timer Register Delta (seconds)—**60**
- Timer Register Expires (seconds)—**660**
- Timer Keep Alive Expires (seconds)—**660**
- Timer Subscribe Expires (seconds)—**660**



Parameters used in Phone

Timer Invite Expires (seconds)*	180
Timer Register Delta (seconds)*	60
Timer Register Expires (seconds)*	660
Timer T1 (msec)*	500
Timer T2 (msec)*	4000
Retry INVITE*	6
Retry Non-INVITE*	10
Start Media Port*	16384
Stop Media Port*	32766
Call Pickup URI*	x-cisco-serviceuri-pickup
Call Pickup Group Other URI*	x-cisco-serviceuri-opickup
Call Pickup Group URI*	x-cisco-serviceuri-gpickup
Meet Me Service URI*	x-cisco-serviceuri-meetme
User Info*	None
DTMF DB Level*	Nominal
Call Hold Ring Back*	Off
Anonymous Call Block*	Off
Caller ID Blocking*	Off
Do Not Disturb Control*	User
Telnet Level for 7940 and 7960*	Disabled
Resource Priority Namespace	< None >
Timer Keep Alive Expires (seconds)*	660
Timer Subscribe Expires (seconds)*	660

Procedure 3 Configure Jabber for iPad softphones

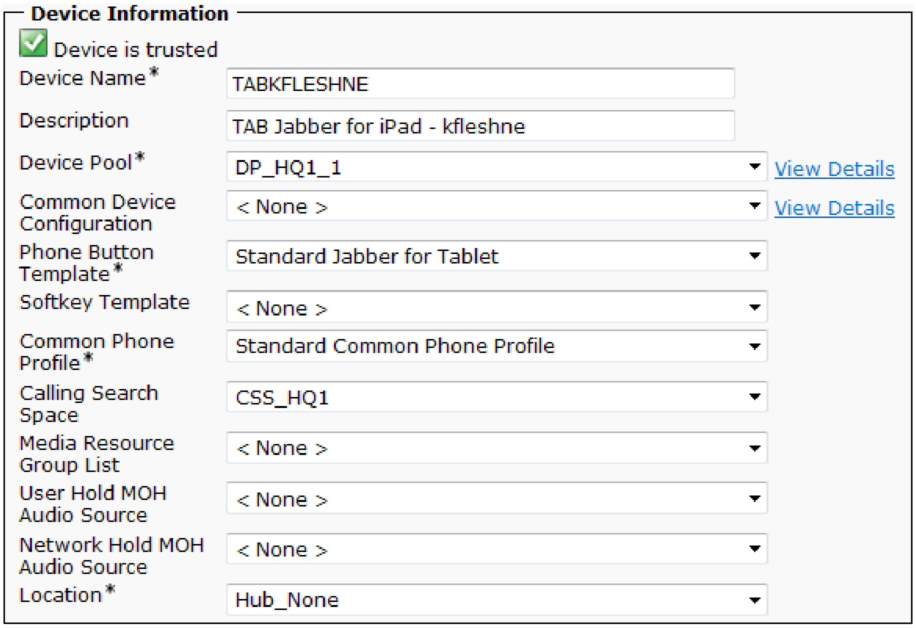
The Cisco Jabber for Tablet (TAB) phone type is used within Cisco Unified CM in order to deploy Jabber for iPad clients that require unified communications.

Step 1: Navigate to **Device > Phone**, and then click **Add New**.

Step 2: In the **Phone Type** list, choose **Cisco Jabber for Tablet**, and then click **Next**.

Step 3: On the Phone Configuration page, in the Device Information section, enter the following information:

- Device Name—**TABKFLESHNE** (TAB plus username, all uppercase)
- Description—**TAB Jabber for iPad - kfleshne**
- Device Pool—**DP_HQ1_1**
- Phone Button Template—**Standard Jabber for Tablet**
- Common Phone Profile—**Standard Common Phone Profile**
- Calling Search Space—**CSS_HQ1**
- Location—**Hub_None**



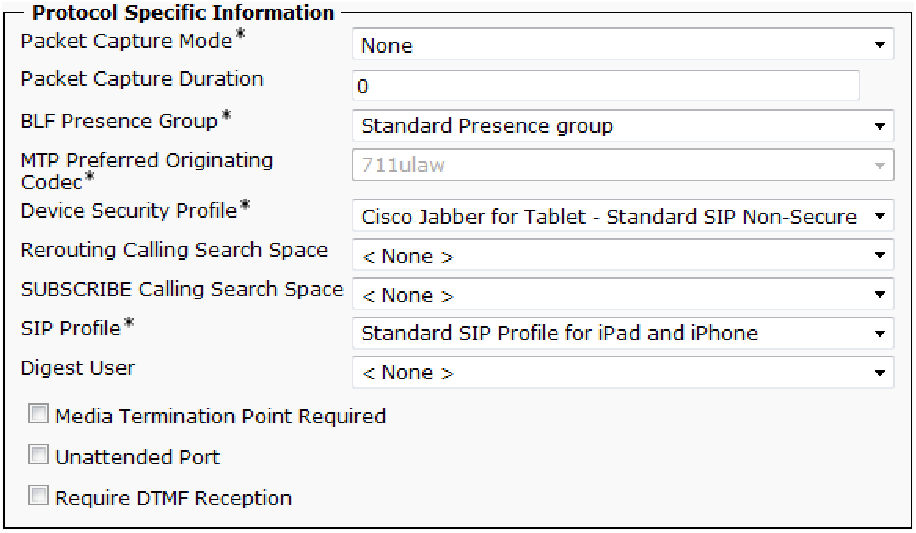
Device Information

☑ Device is trusted

Device Name*	TABKFLESHNE	
Description	TAB Jabber for iPad - kfleshne	
Device Pool*	DP_HQ1_1	View Details
Common Device Configuration	< None >	View Details
Phone Button Template*	Standard Jabber for Tablet	
Softkey Template	< None >	
Common Phone Profile*	Standard Common Phone Profile	
Calling Search Space	CSS_HQ1	
Media Resource Group List	< None >	
User Hold MOH Audio Source	< None >	
Network Hold MOH Audio Source	< None >	
Location*	Hub_None	

Step 4: In the Protocol Specific Information section, enter the following information, and then click **Save**:

- Device Security Profile—**Cisco Jabber for Tablet - Standard SIP Non-Secure**
- SIP Profile—**Standard SIP Profile for iPad and iPhone**



Protocol Specific Information

Packet Capture Mode*	None
Packet Capture Duration	0
BLF Presence Group*	Standard Presence group
MTP Preferred Originating Codec*	711ulaw
Device Security Profile*	Cisco Jabber for Tablet - Standard SIP Non-Secure
Rerouting Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile for iPad and iPhone
Digest User	< None >

□ Media Termination Point Required

□ Unattended Port

□ Require DTMF Reception

Step 5: In the message windows, click **OK**.

Step 6: On the Phone Configuration page, in the Association Information section, click **Line [1] - Add a new DN**.

Tech Tip

When using an LDAP directory service, the Cisco Jabber client's click-to-call the phone number that is listed in the Telephone Number attribute of LDAP.

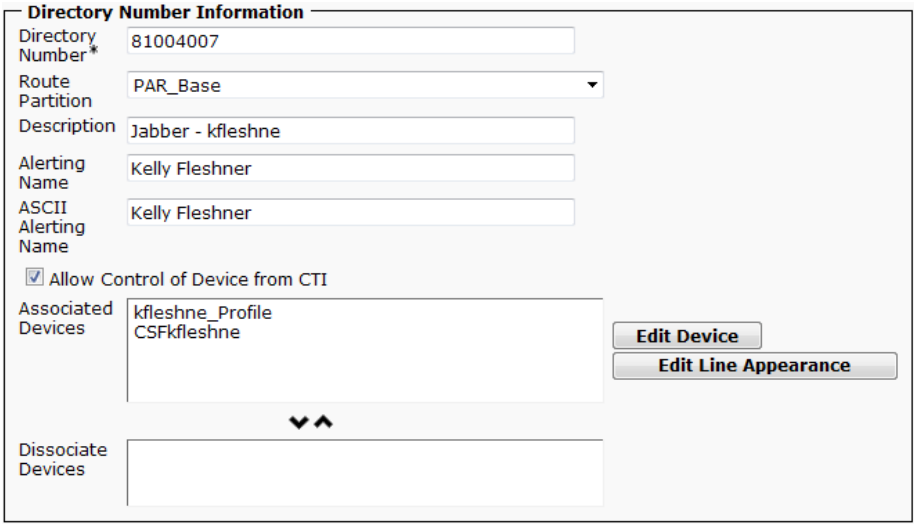
Confirm that the Telephone Number attribute in your LDAP implementation matches the Directory Number used in Cisco Unified CM for your Cisco Jabber client.

Figure 7 has an example of the LDAP General Information page in Microsoft Active Directory.

Step 7: On the Directory Number Configuration page, in the Directory Number Information section, enter the following information:

- Directory Number—**81004007**
- Route Partition—**PAR_Base**
- Description—**Jabber - kfleshne**
- Alerting Name—**[Alerting name]**
- ASCII Alerting Name—**[ASCII alerting name]**
- Allow Control of Device from CTI—**Select**

Figure 6 - Cisco Unified CM Directory Number information



Directory Number Information

Directory Number* 81004007

Route Partition PAR_Base

Description Jabber - kfleshne

Alerting Name Kelly Fleshner

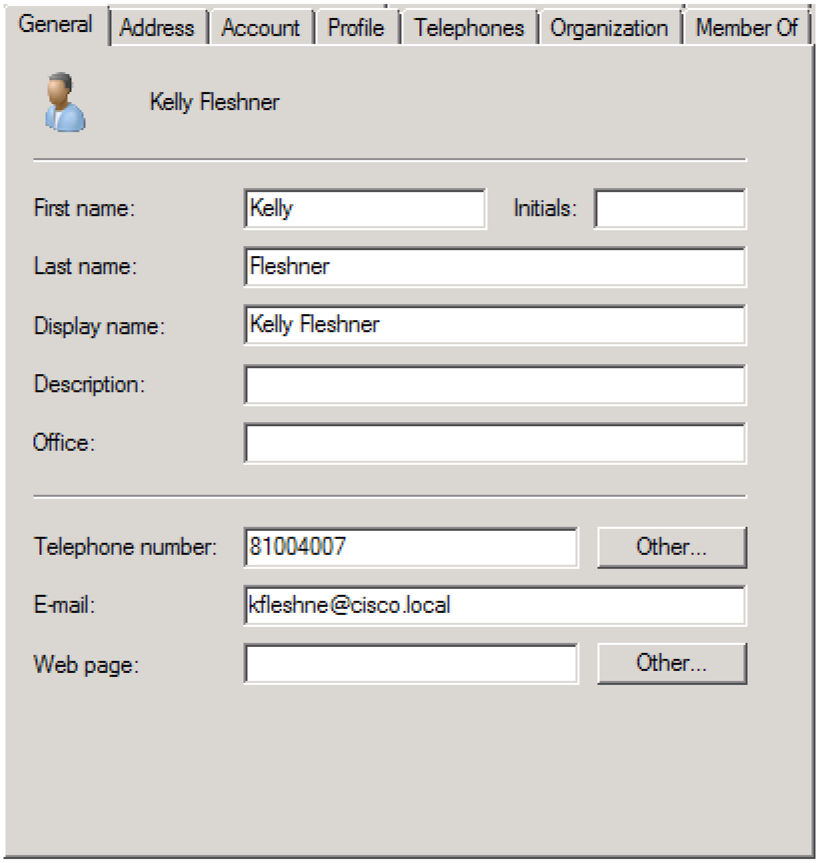
ASCII Alerting Name Kelly Fleshner

☑ Allow Control of Device from CTI

Associated Devices kfleshne_Profile
CSFkfleshne

Dissociate Devices

Figure 7 - Example LDAP general information telephone number attribute



First name: Kelly

Initials:

Last name: Fleshner

Display name: Kelly Fleshner

Description:

Office:

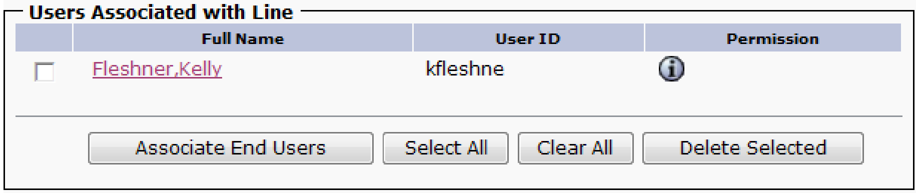
Telephone number: 81004007

E-mail: kfleshne@cisco.local

Web page:

Step 8: In the Users Associated with Line section at the bottom of the page, click **Associate End Users**, and then click **Find**.

Step 9: Select the Cisco Jabber user, click **Add Selected**, and then click **Save**.



Users Associated with Line

	Full Name	User ID	Permission
□	Fleshner,Kelly	kfleshne	ⓘ

Step 10: On the Directory Number Configuration page, click **Apply Config**, and then on the Apply Configuration page, click **OK**.

Procedure 4 Configure Jabber for iPad users

Associate the Cisco Jabber for tablet device with the end user to allow them to utilize the phone service from Unified CM.

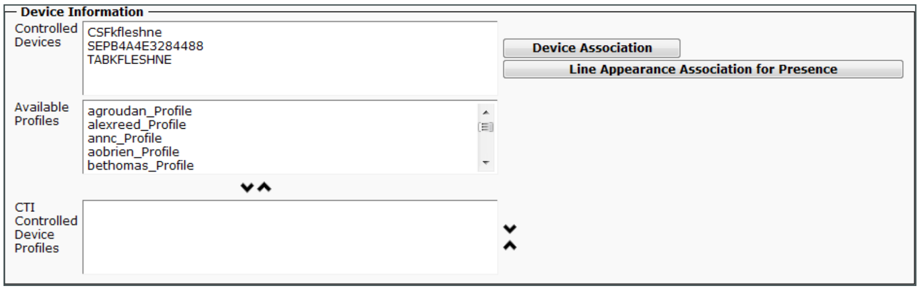
Step 1: Navigate to **User Management > End User**, and then click **Find**.

Step 2: Find the Cisco Jabber user, and then click the username.

Step 3: In the Device Information section, click **Device Association**, and then click **Find**.

Step 4: Select the user's Cisco Jabber for iPad device (Example: TABKFLESHNE), and then click **Save Selected/ Changes**.

Step 5: In the Related Links list, choose **Back to User**, and then click **Go**.



Device Information

Controlled Devices: CSFkfleshne
SEPB4A4E3284488
TABKFLESHNE

Available Profiles: agroudan_Profile
alexreed_Profile
annc_Profile
aobrien_Profile
bethomas_Profile

CTI Controlled Device Profiles:

Step 6: Repeat Procedure 3 and Procedure 4 for each Cisco Jabber for iPad user.

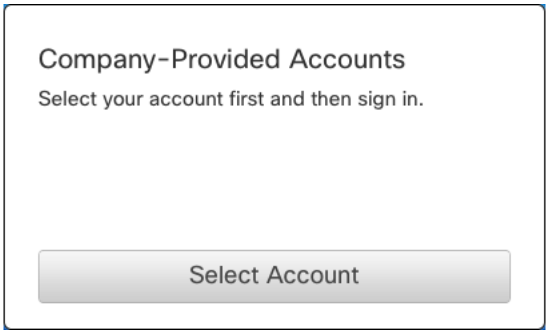
Procedure 5 Download and install Jabber for iPad

After adding the software phones into Cisco Unified CM, the users must download the software to their iPads in order to begin using Cisco Jabber for iPad.

Step 1: On the iPad, tap the **App Store** icon, and then in the search box, enter **Cisco Jabber for iPad**.

Step 2: Locate the application, tap **FREE**, enter your Apple ID password, and then tap **OK**.

Step 3: After the application finishes installing, tap the **Jabber** icon, and then tap **Select Account**.

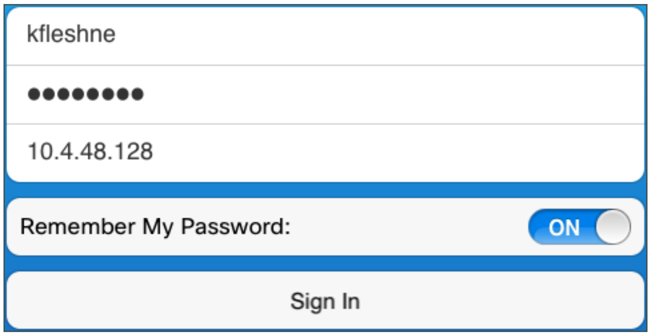


Company-Provided Accounts

Select your account first and then sign in.

Step 4: Under Cisco Instant Messaging, choose **Unified Presence**, enter the following information, and then tap **Sign In**:

- Username—**kfleshne**
- Password—**[password]**
- Server address—**10.4.48.128** (Unified CM IM and Presence server)
- Remember My Password—**On**



kfleshne

●●●●●●●●●

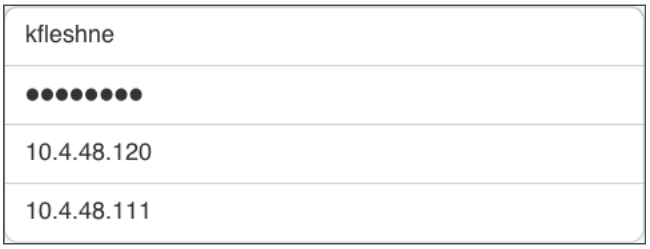
10.4.48.128

Remember My Password: ON

Step 5: On the right side of the page, tap **Set Up Video and Voice Calling Account**, and then choose **Unified Communications Manager**.

Step 6: Enter the following information, choose **Save**, and then tap **Done**:

- Username—**kfleshne**
- Password—**[password]**



kfleshne

●●●●●●●●●

10.4.48.120

10.4.48.111

Step 7: In the top right corner of the page, tap the **Settings** icon, scroll down to the bottom of the page, and then tap **Voicemail Pilot Number**.

Step 8: On the Voicemail Pilot Number page, enter the voice mail pilot (Example: 8009400), choose **Settings**, and then tap **Done**.

8009400

Step 9: Add contacts and favorites as needed.

Step 10: Repeat this procedure for each Cisco Jabber for iPad user.

PROCESS

Configuring Cisco Jabber for iPhone

1. Configure SIP Profile in Unified CM
2. Configure Jabber for iPhone softphones
3. Configure Jabber for iPhone users
4. Download and install Jabber for iPhone

This process is only necessary if you plan to deploy Cisco Jabber for iPhone. The procedures for deploying Cisco Jabber for iPad can be found in the previous process.

First, you configure Jabber for iPhone softphones and users in Cisco Unified CM. Next, you download the Cisco Jabber for iPhone software from the App store and begin the configuration procedure on your phone.

Procedure 1 Configure SIP Profile in Unified CM

If you have already configured the Standard SIP Profile for iPad and iPhone in the “Configure SIP Profile in Unified CM” procedure in the previous process, please skip ahead to the next procedure in this process. If you have not previously configured a SIP profile in Unified CM, please follow the steps below.

To enable unified communications with voice and video calling capabilities from Cisco Unified CM, a software phone device is required per Cisco Jabber for iPhone user.

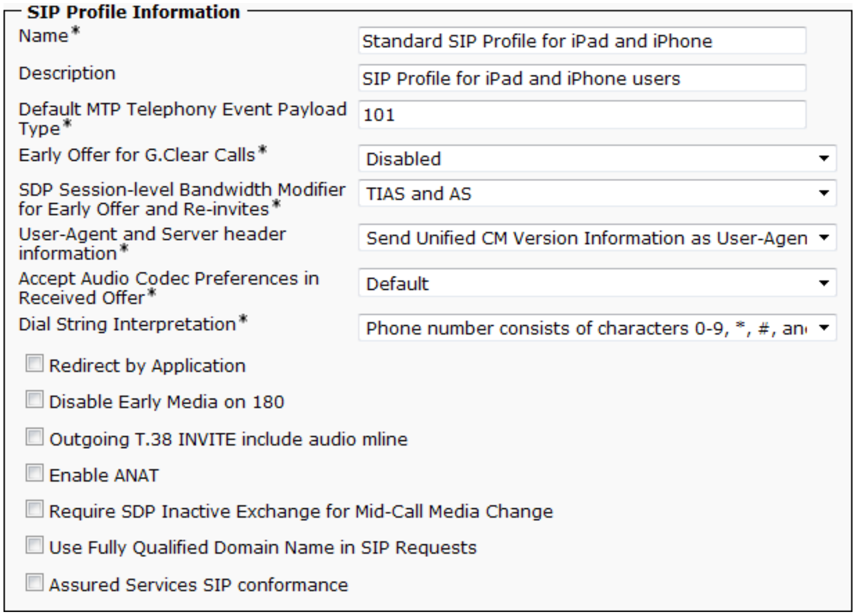
The first stage in building a software phone device to deploy with Cisco Jabber for iPhone users is to create a SIP profile that enables the application to run in the background. You cannot edit or configure the default SIP profile, so you must create a new SIP profile from the default and modify the specific settings.

Step 1: Navigate to **Device > Device Settings > SIP Profile**, and click **Find**.

Step 2: Locate the **Standard SIP Profile**, and on the right hand side of the page, click the **Copy** icon.

Step 3: On the SIP Profile Configuration page, in the SIP Profile Information section, enter the following information:

- Name—**Standard SIP Profile for iPad and iPhone**
- Description—**SIP Profile for iPad and iPhone Users**



SIP Profile Information

Name*	Standard SIP Profile for iPad and iPhone
Description	SIP Profile for iPad and iPhone users
Default MTP Telephony Event Payload Type*	101
Early Offer for G.Clear Calls*	Disabled
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites*	TIAS and AS
User-Agent and Server header information*	Send Unified CM Version Information as User-Agen
Accept Audio Codec Preferences in Received Offer*	Default
Dial String Interpretation*	Phone number consists of characters 0-9, *, #, an

☐ Redirect by Application

☐ Disable Early Media on 180

☐ Outgoing T.38 INVITE include audio mline

☐ Enable ANAT

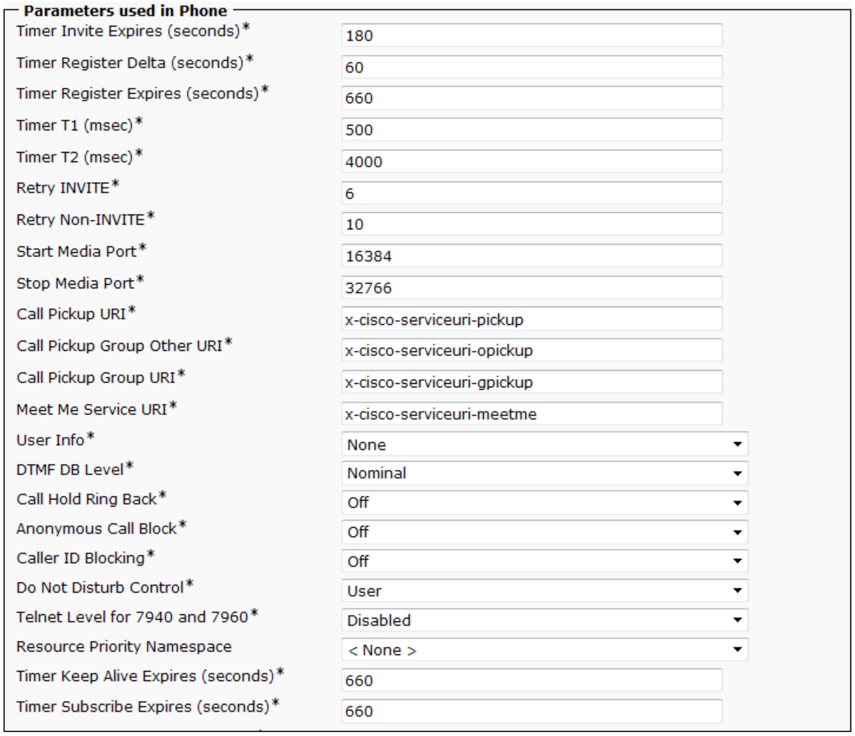
☐ Require SDP Inactive Exchange for Mid-Call Media Change

☐ Use Fully Qualified Domain Name in SIP Requests

☐ Assured Services SIP conformance

Step 4: In the Parameters Used in Phone section, enter the following information, and then click Save:

- Timer Register Delta (seconds)—**60**
- Timer Register Expires (seconds)—**660**
- Timer Keep Alive Expires (seconds)—**660**
- Timer Subscribe Expires (seconds)—**660**



Parameters used in Phone

Timer Invite Expires (seconds)*	180
Timer Register Delta (seconds)*	60
Timer Register Expires (seconds)*	660
Timer T1 (msec)*	500
Timer T2 (msec)*	4000
Retry INVITE*	6
Retry Non-INVITE*	10
Start Media Port*	16384
Stop Media Port*	32766
Call Pickup URI*	x-cisco-serviceuri-pickup
Call Pickup Group Other URI*	x-cisco-serviceuri-opickup
Call Pickup Group URI*	x-cisco-serviceuri-gpickup
Meet Me Service URI*	x-cisco-serviceuri-meetme
User Info*	None
DTMF DB Level*	Nominal
Call Hold Ring Back*	Off
Anonymous Call Block*	Off
Caller ID Blocking*	Off
Do Not Disturb Control*	User
Telnet Level for 7940 and 7960*	Disabled
Resource Priority Namespace	< None >
Timer Keep Alive Expires (seconds)*	660
Timer Subscribe Expires (seconds)*	660

Procedure 2 Configure Jabber for iPhone softphones

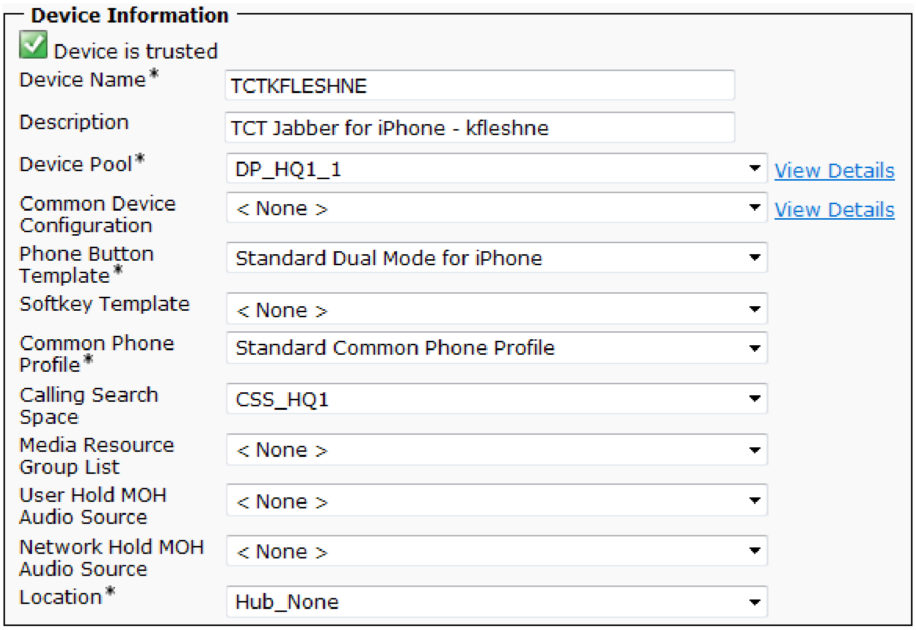
The Cisco Dual Mode for iPhone (TCT) phone type is used within Cisco Unified CM in order to deploy Cisco Jabber for iPhone clients that require unified communications.

Step 1: Navigate to **Device > Phone**, and then click **Add New**.

Step 2: In the **Phone Type** list, choose **Cisco Dual Mode for iPhone**, and then click **Next**.

Step 3: On the Phone Configuration page, in the Device Information section, enter the following information:

- Device Name—**TCTKFLESHNE** (TCT plus username, all uppercase)
- Description—**TCT Jabber for iPhone - kfleshne**
- Device Pool—**DP_HQ1_1**
- Phone Button Template—**Standard Dual Mode for iPhone**
- Common Phone Profile—**Standard Common Phone Profile**
- Calling Search Space—**CSS_HQ1**
- Location—**Hub_None**



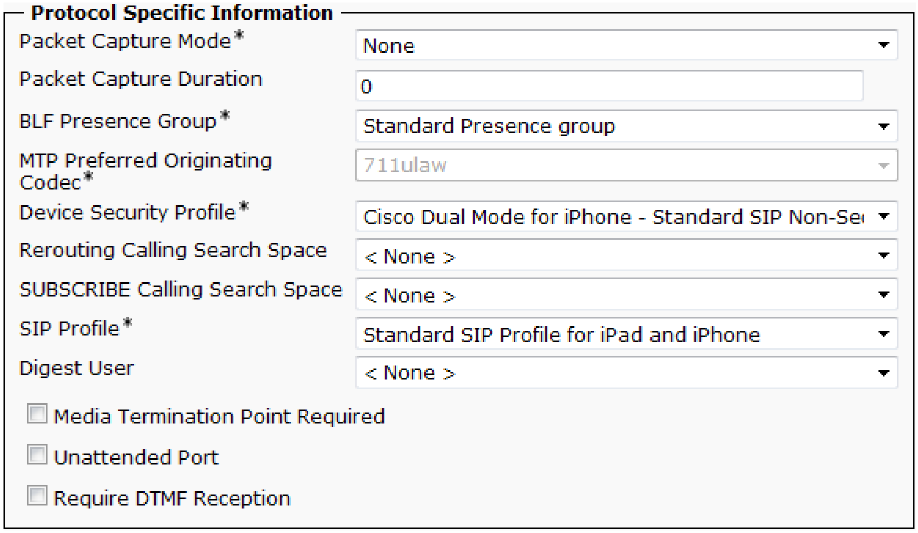
Device Information

☑ Device is trusted

Device Name*	TCTKFLESHNE	
Description	TCT Jabber for iPhone - kfleshne	
Device Pool*	DP_HQ1_1	View Details
Common Device Configuration	< None >	View Details
Phone Button Template*	Standard Dual Mode for iPhone	
Softkey Template	< None >	
Common Phone Profile*	Standard Common Phone Profile	
Calling Search Space	CSS_HQ1	
Media Resource Group List	< None >	
User Hold MOH Audio Source	< None >	
Network Hold MOH Audio Source	< None >	
Location*	Hub_None	

Step 4: In the Protocol Specific Information section, enter the following information:

- Device Security Profile—**Cisco Dual Mode for iPhone - Standard SIP Non-Secure**
- SIP Profile—**Standard SIP Profile for iPad and iPhone**



Protocol Specific Information

Packet Capture Mode*	None
Packet Capture Duration	0
BLF Presence Group*	Standard Presence group
MTP Preferred Originating Codec*	711ulaw
Device Security Profile*	Cisco Dual Mode for iPhone - Standard SIP Non-Se
Rerouting Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile for iPad and iPhone
Digest User	< None >

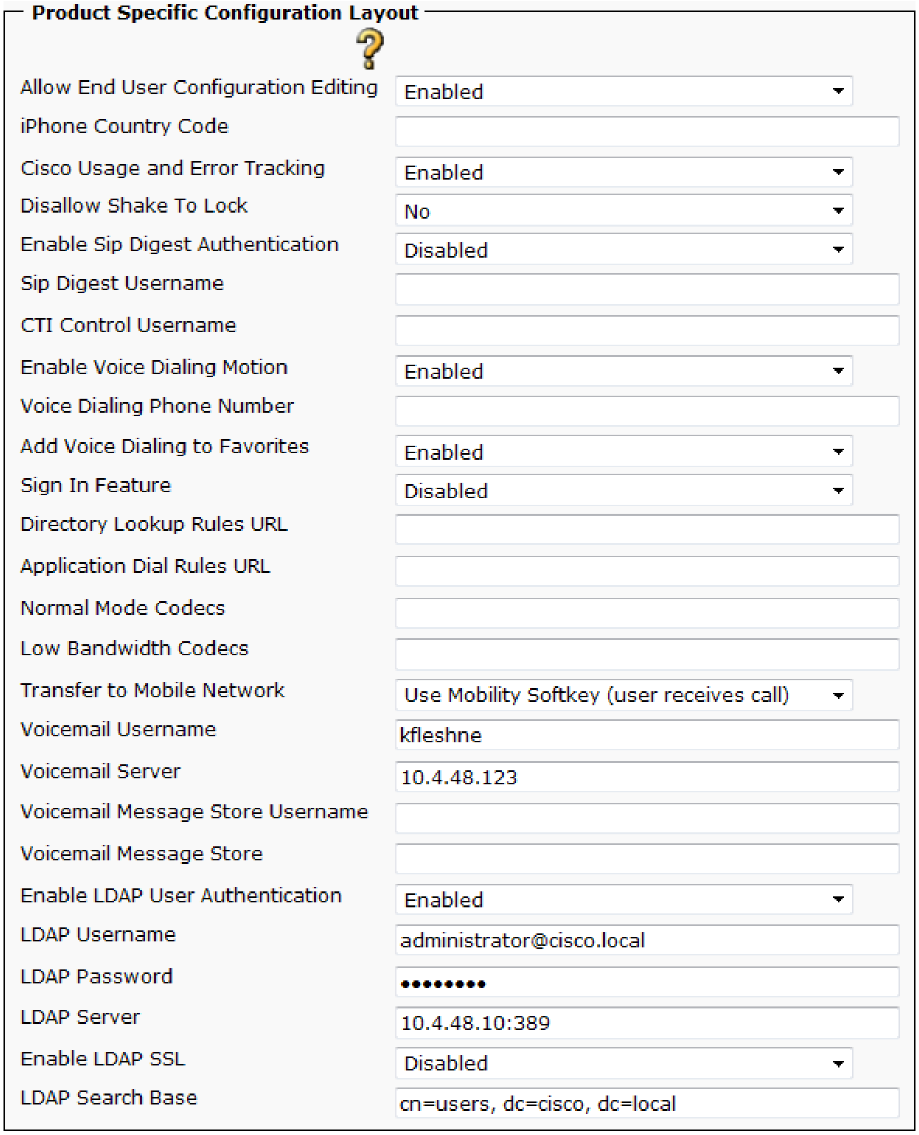
□ Media Termination Point Required

□ Unattended Port

□ Require DTMF Reception

Step 5: In the Product Specific Configuration Layout section, enter the following information, and then click Save:

- Allow End User Configuration Editing—**Enabled**
- Voicemail Username—**kfleshne**
- Voicemail Server—**10.4.48.123** (Unity Connection)
- Enable LDAP User Authentication—**Enabled**
- LDAP Username—**administrator@cisco.local**
- LDAP Password—**[password]**
- LDAP Server—**10.4.48.10:389** (LDAP server and port)
- Enable LDAP SSL—**Disabled**
- LDAP Search Base—**cn=users, dc=cisco, dc=local**



Product Specific Configuration Layout

Allow End User Configuration Editing	Enabled
iPhone Country Code	
Cisco Usage and Error Tracking	Enabled
Disallow Shake To Lock	No
Enable Sip Digest Authentication	Disabled
Sip Digest Username	
CTI Control Username	
Enable Voice Dialing Motion	Enabled
Voice Dialing Phone Number	
Add Voice Dialing to Favorites	Enabled
Sign In Feature	Disabled
Directory Lookup Rules URL	
Application Dial Rules URL	
Normal Mode Codecs	
Low Bandwidth Codecs	
Transfer to Mobile Network	Use Mobility Softkey (user receives call)
Voicemail Username	kfleshne
Voicemail Server	10.4.48.123
Voicemail Message Store Username	
Voicemail Message Store	
Enable LDAP User Authentication	Enabled
LDAP Username	administrator@cisco.local
LDAP Password	••••••••
LDAP Server	10.4.48.10:389
Enable LDAP SSL	Disabled
LDAP Search Base	cn=users, dc=cisco, dc=local

Step 6: In the message window, click OK.

Step 7: On the Phone Configuration page, in the Association Information section, click **Line [1] - Add a new DN**.

Tech Tip

When using an LDAP directory service, the Cisco Jabber client's click-to-call the phone number that is listed in the Telephone Number attribute of LDAP.

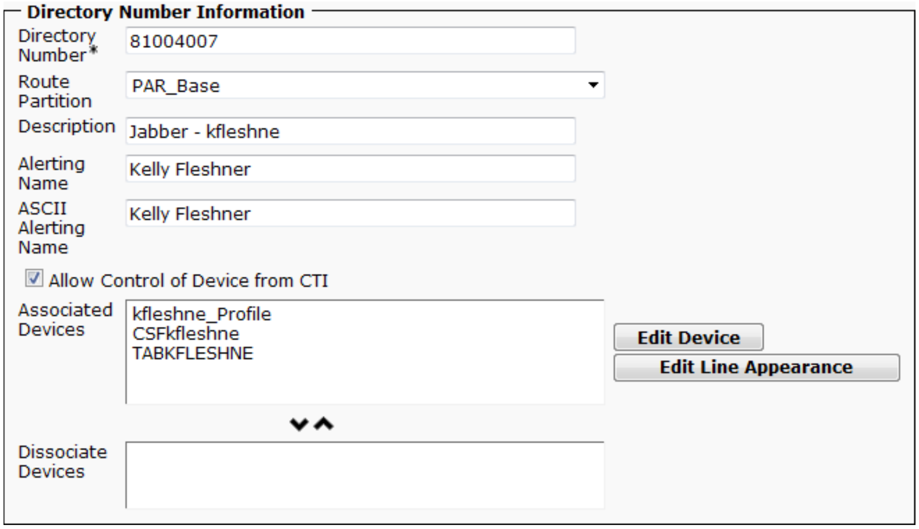
Confirm that the Telephone Number attribute in your LDAP implementation matches the Directory Number used in Cisco Unified CM for your Cisco Jabber client.

Figure 9 has an example of the LDAP General Information page in Microsoft Active Directory.

Step 8: On the Directory Number Configuration page, in the Directory Number Information section, enter the following information:

- Directory Number—**81004007**
- Route Partition—**PAR_Base**
- Description—**Jabber - kfleshne**
- Alerting Name—**[Alerting name]**
- ASCII Alerting Name—**[ASCII alerting name]**
- Allow Control of Device from CTI—**Select**

Figure 8 - Cisco Unified CM Directory Number information



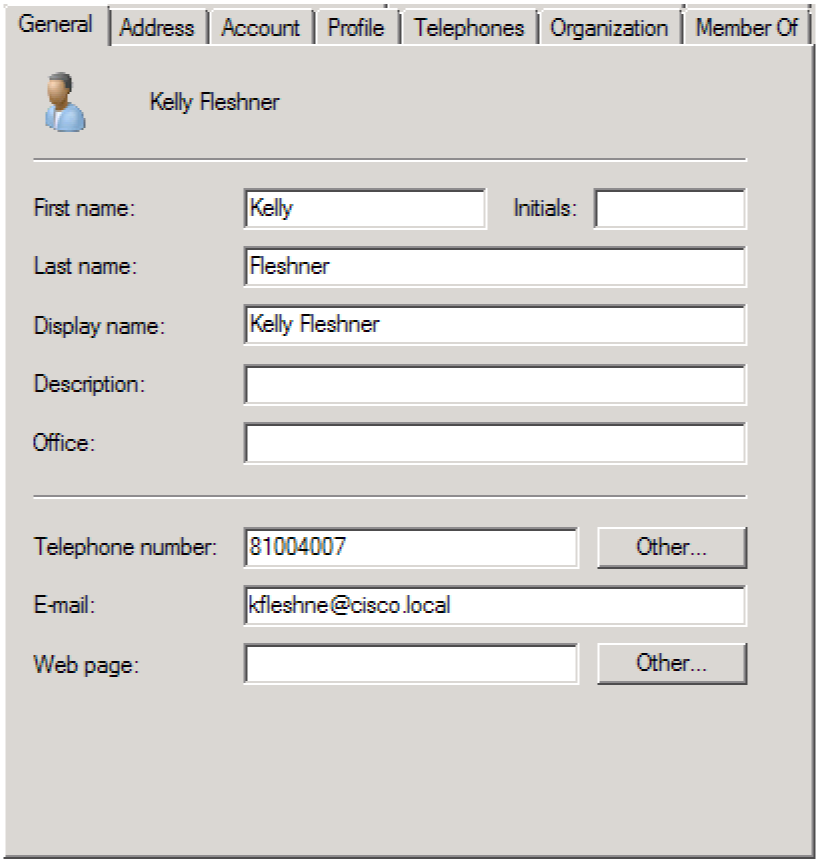
Directory Number Information

Directory Number*	81004007
Route Partition	PAR_Base
Description	Jabber - kfleshne
Alerting Name	Kelly Fleshner
ASCII Alerting Name	Kelly Fleshner

☑ Allow Control of Device from CTI

Associated Devices	kfleshne_Profile CSFkfleshne TABKFLESHNE
Dissociate Devices	

Figure 9 - Example LDAP general information telephone number attribute



Kelly Fleshner

First name: Kelly

Initials:

Last name: Fleshner

Display name: Kelly Fleshner

Description:

Office:

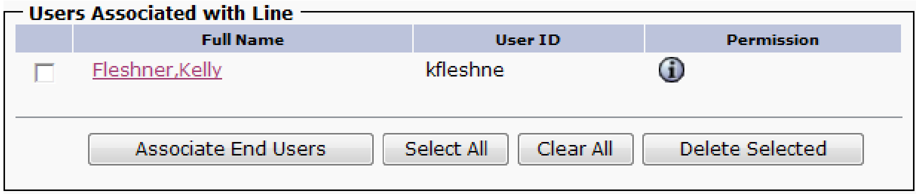
Telephone number: 81004007

E-mail: kfleshne@cisco.local

Web page:

Step 9: In the Users Associated with Line section at the bottom of the page, click **Associate End Users**, and then click **Find**.

Step 10: Select the Cisco Jabber user, click **Add Selected**, and then click **Save**.



Users Associated with Line

	Full Name	User ID	Permission
□	Fleshner,Kelly	kfleshne	ⓘ

Step 11: On the Directory Number Configuration page, click **Apply Config**, and then on the Apply Configuration page, click **OK**.

Procedure 3 Configure Jabber for iPhone users

Associate the Cisco Jabber for iPhone device with the end user to allow them to utilize the phone service from Unified CM.

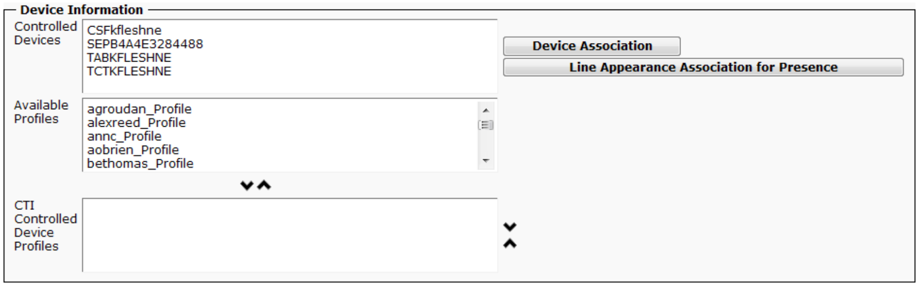
Step 1: Navigate to **User Management > End User**, and then click **Find**.

Step 2: Find the Cisco Jabber user, and then click the username.

Step 3: In the Device Information section, click **Device Association**, and then click **Find**.

Step 4: Select the user's Cisco Jabber for iPhone device (Example: TCTKFLESHNE), and then click **Save Selected/Changes**.

Step 5: In the Related Links list, choose **Back to User** and then click **Go**.


Device Information

Controlled Devices: CSFkfleshne
SEPB4A4E3284488
TABKFLESHNE
TCTKFLESHNE

Available Profiles: agroudan_Profile
alexreed_Profile
annc_Profile
aobrien_Profile
bethomas_Profile

CTI Controlled Device Profiles:

Step 6: Repeat Procedure 2 and Procedure 3 for each Cisco Jabber for iPhone user.

Procedure 4 Download and install Jabber for iPhone

After adding the software phones into Unified CM, the users must download two separate applications to their iPhones to begin using Cisco Jabber and Cisco Jabber IM for iPhone.

Step 1: On the iPhone, tap the **App Store** icon, and then in the search box, enter **Cisco Jabber**.

Step 2: Locate the application **Cisco Jabber**, tap **FREE**, enter your Apple ID password, and then tap **OK**.

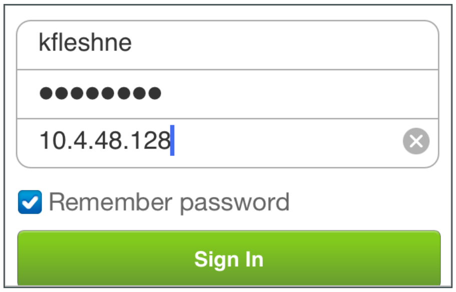
Step 3: On the iPhone, tap the **App Store** icon, and then in the search box, enter **Cisco Jabber IM**.

Step 4: Locate the application **Cisco Jabber IM for iPhone**, tap **FREE**, enter your Apple ID password, and then tap **OK**.

Step 5: After the two applications finish installing, tap the **Cisco Jabber IM for iPhone** icon, and then tap **Cisco Unified Presence**.

Step 6: Enter the following information, and then tap **Sign In**:

- Username—**kfleshne**
- Password—**[password]**
- Server address—**10.4.48.128** (Unified CM IM and Presence server)
- Remember My Password—**Select**



kfleshne

●●●●●●●●●

10.4.48.128

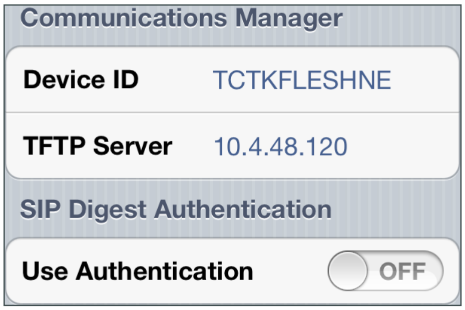
☑ Remember password

Step 7: Add contacts and favorites as needed.

Step 8: Push the Home button on the iPhone, tap the **Cisco Jabber** icon, tap **Accept**, and then tap **Enter Account Settings**.

Step 9: Tap **Begin**, tap **Continue**, enter the following information, and then tap **Save**:

- Device ID—**TCTKFLESHNE** (TCT plus username, all uppercase)
- TFTP Server—**10.4.48.120** (CUCM TFTP server)
- User Authentication—**Off**



Communications Manager

Device ID TCTKFLESHNE

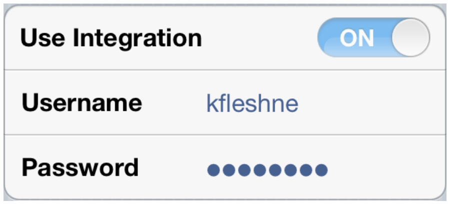
TFTP Server 10.4.48.120

SIP Digest Authentication

Use Authentication OFF

Step 10: On the Desk Phone Integration page, tap **Yes**, enter the following information, and then tap **Save**:

- User Integration—**On**
- Username—**kfleshne**
- Password—**[password]**



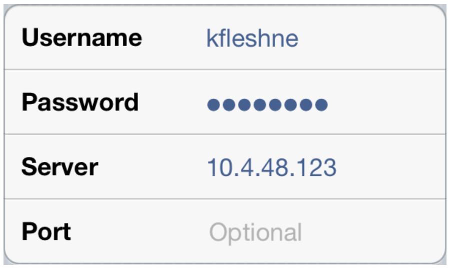
Use Integration ON

Username kfleshne

Password ●●●●●●●●

Step 11: On the Unified Messaging page, tap **Continue**, enter the following information, and then tap **Save**:

- Username—**kfleshne**
- Password—**[password]**
- Server—**10.4.48.123** (Unity Connection)
- Port—**[blank]**



Username kfleshne

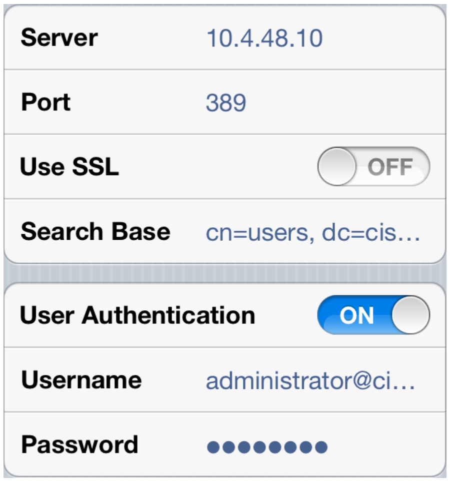
Password ●●●●●●●●

Server 10.4.48.123

Port Optional

Step 12: On the Corporate Directory page, tap **Continue**, enter the following information, and then tap **Save**:

- Server–**10.4.48.10** (LDAP)
- Port–**389**
- Use SSL–**Off**
- Search Base–**cn=users, dc=cisco, dc=local**
- User Authentication–**On**
- Username–**administrator@cisco.local**
- Password–**[password]**



Server	10.4.48.10
Port	389
Use SSL	OFF
Search Base	cn=users, dc=cis…
User Authentication	ON
Username	administrator@ci…
Password	●●●●●●●●

Step 13: Tap **Continue**.

Step 14: Add contacts and favorites as needed.

Step 15: Repeat this procedure for each Cisco Jabber for iPhone user.

Appendix A: Product List

Data Center or Server Room

Functional Area	Product Description	Part Numbers	Software
Virtual Servers	Cisco UCS C240 M3 C-Series Solution Pak for unified communications applications	UCUCS-EZ-C240M3S	9.1(1a) ESXi 5.0
	Cisco UCS C220 M3 C-Series Solution Pak for unified communications applications	UCUCS-EZ-C220M3S	
	Cisco UCS C220 M3 for Business Edition 6000	UCSC-C220-M3SBE	

Data Center Core

Functional Area	Product Description	Part Numbers	Software
Core Switch	Cisco Nexus 5596 up to 96-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5596UP-FA	NX-OS 5.2(1)N1(3) Layer 3 License
	Cisco Nexus 5596 Layer 3 Switching Module	N55-M160L30V2	
	Cisco Nexus 5548 up to 48-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5548UP-FA	
	Cisco Nexus 5548 Layer 3 Switching Module	N55-D160L3	
	Cisco Nexus 5500 Layer 3 Enterprise Software License	N55-LAN1K9	
	Cisco Nexus 5500 Storage Protocols Services License, 8 ports	N55-8P-SSK9	
Ethernet Extension	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T (enhanced) Fabric Extender	N2K-C2248TP-E	–
	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T Fabric Extender	N2K-C2248TP-1GE	
	Cisco Nexus 2000 Series 32 1/10 GbE SFP+, FCoE capable Fabric Extender	N2K-C2232PP-10GE	

Server Room

Functional Area	Product Description	Part Numbers	Software
Stackable Ethernet Switch	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 ports	WS-C3750X-48T-S	15.0(2)SE2 IP Base license
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 ports	WS-C3750X-24T-S	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Standalone Ethernet Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 ports	WS-C3560X-48T-S	15.0(2)SE2 IP Base license
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 ports	WS-C3560X-24T-S	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

Feedback

Please use the feedback form to send comments and suggestions about this guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY 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 THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

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.

B-0000418-1 08/13