Unified Communications Using Cisco BE6000

TECHNOLOGY DESIGN GUIDE

July 2014

Table of Contents

Preface

Cisco Validated Designs (CVDs) provide the foundation 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 email collab-mm-cvd@external.cisco.com.

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

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

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:

- Centralized Unified Communications—Organizations require high-quality voice and video communications that can scale up to thousand users using Cisco Business Edition 6000. They need a solution that is fast to deploy and easy to manage from a central location, without replicating costly features at their remote sites.

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 and IM and Presence
- Telephony call agent
- Voicemail server
- IM & Presence Server
- Virtualized servers
- Voice gateways and conference bridges
- IP telephones with remote-site survivability
- Session Initiation Protocol (SIP) signaling
- Lightweight Directory Access Protocol integration
- Cisco Unified Configurator for Collaboration(CUCC)

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:

- CCNA Voice—1 to 3 years designing, installing, and troubleshooting voice and unified communications applications, devices, and networks.

Related CVD Guides

Cisco Preferred Architecture for Collaboration

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

Introduction

Communication is the lifeblood of an organization, and in today's global economy, the desire to stay in touch in many different ways has never been greater. The methods people have used to collaborate have changed over the years, but the ability to work seamlessly with others has always been very important to the success of a business.

To remain competitive, you need to provide reliable and consistent access to your communications resources. The importance of dependable collaboration channels inside and outside of your organization cannot be overstated. You also need to minimize the time required to select and absorb your collaboration technology investments and reduce your overall operational costs.

Technology Use Case

Collaboration has always been an essential component of a successful organization. New pressures, heightened by a challenging global economic environment, are making organizations realize collaboration is more important than ever. Specifically, they are trying to manage operational expenses and capital expenses while increasing worker productivity and staying ahead of the competition.

You can only accomplish this "do more with less" approach by finding the means to do the following:

- Empower your workforce—Users are empowered when they have communication tools at their disposal that allow them to access and use information when they need it most. Younger employees—especially those of the "Generation Y" demographic, who are now in their twenties—are bringing these networking tools into the workplace. Organizations need to develop a concerted strategy to proactively manage these technologies and, ideally, develop organizational capabilities to best take advantage of them.
- Provide real-time information—Collaborative applications make real-time information available to empowered users and provide for information sharing and privacy. Because information is shared across the entire user community, its accuracy is more easily verified and corrected.
- Accelerate through innovation—Organizations that successfully adopt new collaborative processes are able to move faster, make better decisions, draw from a deeper base of information, and more effectively operate across time and distance barriers. As is always the case in business, either you pull ahead, or the competition will leave you behind.

The challenges are addressed with collaboration services, such as web-conferencing applications, unified communications, and video-collaboration meetings. However, providing these types of capabilities to an entire organization requires a robust and scalable network infrastructure.

Use Case: Centralized Unified Communications

Organizations require high-quality voice and video communications that can scale to tens of thousands of users. They need a 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:

- **Single cluster centralized design**—Makes the solution simpler to deploy and easier to manage from a centralized site while saving on infrastructure components. In the single cluster centralized design, each remote site connects to the headquarters site through a WAN and each site receives call processing features from the headquarters location.
- **Phone auto-registration**—Automatically registers phones for quick and easy deployment.
- **Lightweight Directory Access Protocol integration**—Uses an LDAP directory integration option in Cisco Unified Communications Manager (CM) and Cisco Unity Connection for designs that require a single source of information for user management.
- **North American Numbering Plan**—Allows you to choose between two North American Numbering Plans as part of the path selection for public switched telephone network (PSTN) destinations. Dial plans from other countries can easily be imported using the configuration tool included with this guide.
- **Uniform on-net dial plan**—Uses endpoint addressing that consists of a uniform on-net dial plan containing 4-digit extensions. An optional access code and 2-digit or 3-digit site codes are available with local site 4-digit dialing.
- **Local route groups**—Uses local route groups in order to reduce the number of route patterns required to provision Session Initiation Protocol (SIP) gateways for all sites.
- **Class of service**—Provisions class of service (CoS) categories with the use of partitions and calling search spaces in order to allow emergency, local, long distance and international dialing capabilities.
- **Survivable Remote Site Telephony (SRST)**—Provides failover at each remote site by standard SRST for SIP and Skinny Client Control Protocol (SCCP) phones.
- **Device Mobility**—Uses the Device Mobility feature, which allows Cisco Unified CM to determine the physical locations of devices.
- **Server load balancing**—Load-balances phones across Cisco Unified CM redundancy groups on a phone-by-phone basis.
- **Extension Mobility**—Uses the Cisco Extension Mobility feature for all phones, which enables users to assign a Cisco Unified IP Phone as their own or move from phone-to-phone within the organization.
- **Extend and Connect**—Allows administrators to rapidly deploy UC Computer Telephony Integration (CTI) applications that interoperate with any endpoint. Newer UC solutions are interoperable with legacy systems, so customers can migrate to newer UC solutions over time as existing hardware is deprecated.
- **Media resources**—Provisions individual media resources, such as conference bridges for every site.
- **Call Admission Control**—Provides location-based Call Admission Control (CAC) for a typical hub-and-spoke WAN environment.
- **Voice messaging**—Provisions Cisco Unified CM for voice messaging integration and documents the Cisco Unity Connection configuration.
- **Instant Messaging and Presence**—Provisions Cisco Unified CM IM and presence service integration and documents the Cisco Unified Presence configuration.
- **Point-to-Point Video**—Enables point-to-point video between two participants with video endpoints.

Design Overview

This design guide eases the organization's cost of technology selection and implementation by recommending equipment that is appropriate for organizations, using methods and procedures that have been developed and tested by Cisco. Applying the guidance within this document reduces the time required for adoption of the technology and allows the components to be deployed quickly and accurately, so the organization can achieve a head start in realizing the return on its investment.

IP telephony as a technology is the migration of the old standalone phone switch to a software-based switch, where the data network becomes the physical transport for voice communications, rather than using separate cabling plants for data and voice communications. The market category that defines IP telephony and other forms of voice and video communications is known as *unified communications*.

Cisco Unified Computing System

Because Cisco Unified Communications applications, such as IP telephony and voicemail, have different processing and storage requirements based on the number of users and the features applied, it is important to select the appropriate server platform based on expected usage.

Co-resident means the virtual machine server instance is installed on the same Cisco UCS hardware as other server instances.

For 1000 users or fewer, Cisco Business Edition (BE) 6000 is recommended. A second BE6000 server may be added for organizations that require hardware redundancy.

Cisco Voice Gateways

Voice gateways provide connectivity to networks outside the organization, conferencing resources, and remote survivability. The combination of these voice services into a single platform offers savings over the individual components. The voice services can be integrated into an existing WAN router, or they can be deployed in a standalone router for additional capacity and redundancy.

The decision to integrate voice into an existing router depends on voice capacity and the overall performance of the router selected. If a router is consistently running above 40% CPU, the voice services are better suited for a standalone gateway in order to avoid processing delays for voice traffic. If the router has limited slots available for voice interface cards or digital signal processors, a standalone gateway is recommended to allow additional capacity when needed. Standalone gateways at the headquarters location are connected to the datacenter or server room switches. At a remote location, they are connected to the access or distribution switches.

Because Cisco Integrated Services Router Generation 2 (ISR G2) have different processing capabilities based on the number of phones and the features applied, it is important to select the appropriate platform based on expected usage.

The sizing information in this guide supersedes the information from the various CVD WAN design guides because the number of SRST users determines the proper router model, as listed in the following table.

Table 1 - Standalone voice gateway scaling options

	Voice gateway	Voice T1/E1	Trunk ports	Conference bridge ports
4 users	Cisco 880	N/A	4	2
50 users	Cisco 2911	4	120	25
100 users	Cisco 2921	6	180	50
250 users	Cisco 2951	8	240	75
730 users	Cisco 3925	12	360	100
1200 users	Cisco 3945	18	540	150

Cisco Unified Communications

The products and priorities for this design were based on requirements from customers, partners, and Cisco field personnel. Your specific business requirements may be different from those in this guide, in which case, the product selection may not exactly match your needs. Please contact an authorized Cisco partner or representative to validate any design changes that you plan to deploy.

Cisco Unified Communications has the following software components:

- Cisco Unified CM provides the Internet Protocol private branch exchange (IP PBX) functionality for all users within the headquarters site as well as the remote sites. The first Unified CM appliance is known as the *publisher* because it contains the master database to which all other Unified CM appliances within the same cluster subscribe. The rest of the appliances are known as either *subscribers* or *Trivial File Transfer Protocol (TFTP) servers,* based on their function in the cluster.
- Cisco Unity Connection provides services such as voicemail, voicemail integration with your email inbox, and many other productivity features. Voicemail is considered part of the unified communications foundation.

The following cluster design option is used in this guide:

- A 1:1 publisher subscriber redundancy in Cisco Unified CM configurations.

Single Cluster Centralized Design

The following single cluster centralized design model provides a highly available and scalable call-control and voicemail system capable of email client integration.

The Cisco Business Edition (BE) 6000 uses a single Cisco UCS server platform for up to 1000 users. The virtualized server provides the following:

- The publisher, subscriber and TFTP functions are combined with Cisco Unity Connection on a single hardware platform in order to help lower the capital and operational expenses.
- The Cisco UCS C220 M3 hardware platform for the Cisco BE 6000 is a 1 rack unit form factor.
- The Cisco Business Edition 6000 supports Cisco Unified Presence and Cisco Unified Contact Center Express on the same virtual server platform. You can also add a redundant server to this configuration if an organization requires it.

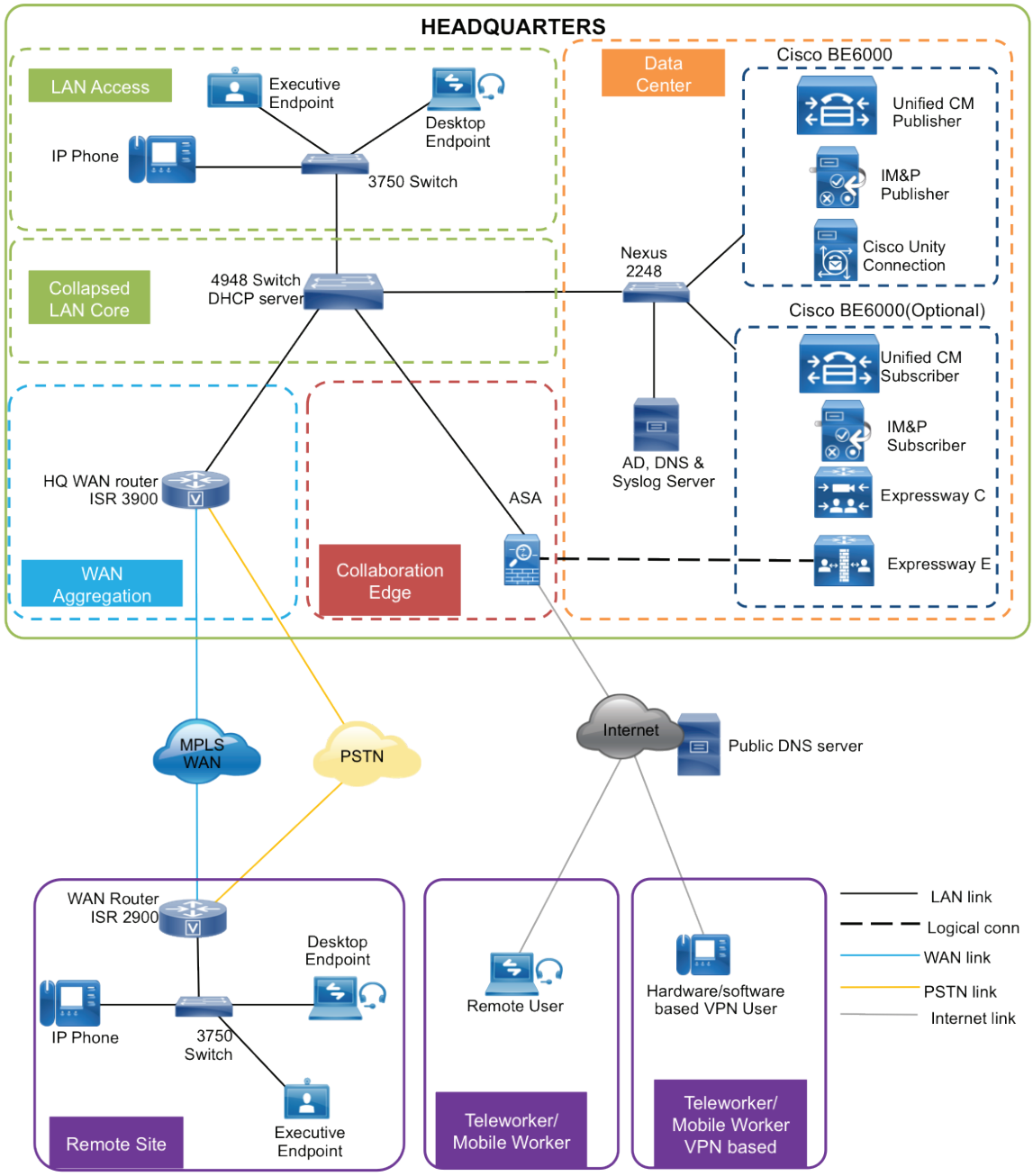
Table 2 - Cisco Unified Communications Manager centralized design model

	500 users	1000 users
Publisher	1	1
Subscribers	1	1
TFTP	1 (shared)	2 (shared)
Groups	1	1
Remote sites	50	90
UCS servers	1	1

For the design model, the following features are provided:

- Connect each server to a different switch within the server room or data center in order to provide for high availability should a switch or link connection fail.
- There is sufficient capacity for multiple devices for each user. For example, you can enable a desk phone and a soft phone with enough computer telephony integration to allow a high percentage of users to have click-to-call or other applications that can remotely control their phones.
- There is additional capacity available for phones that are not assigned to a specific user, such as those in public areas, meeting rooms, storage areas, and break rooms.
- Cisco Unity Connection is deployed as a simple voicemail system. However, with additional configuration, it will provide calendar-based call-handling integration with Microsoft Exchange, Cisco Unified MeetingPlace, and other networkable voicemail systems. Cisco Unity Connection is deployed in the architecture as non-redundant, although a second high-availability server can be added, if required.
- It is possible to support other services, including advanced conferencing, contact center, and video conferencing. These advanced services require additional hardware and software, and they are not covered in this document.

Figure 1 - Cisco Unified CM, Cisco Unity Connection, and IM and Presence



The centralized design consists of a headquarters site and up to 90 remote sites. The Cisco Unified CM and the Cisco Unity Connection server instances are placed at the main site to handle the call processing for up to 1000 telephony users with voice messaging. Optional Cisco BE 6000 server can be placed at the main site for redundancy and to install other applications. Each remote site takes advantage of the Cisco ISR G2 router that was deployed as part of the WAN deployment. Remote worker/mobile worker use cases leveraging Cisco Expressway C & Expressway E are discussed in detail in Collab Edge using Cisco BE 6000 Design Guide.

Auto-Registration

Auto-registration allows Cisco Unified CM to automatically assign a directory number to new phones as they are deployed in your network. With Cisco Unified Configurator for Collaboration (CUCC), auto-registration is enabled in order to allow for quick and easy deployment of phones. After the phones are registered and the guide has been followed completely, users configured in the system should use Cisco Extension Mobility to log into the auto-registered phones to enable off-net dialing.

By default, auto-registered phones are able to dial on-net directory numbers as well as off-net emergency 911 calls. They are not, however, able to dial off-net numbers.

Tech Tip

Leaving auto-registration enabled carries a security risk in that "rogue" phones can automatically register with Cisco Unified CM. You should only allow auto-registration for brief periods when you want to perform bulk phone adds during phone deployment.

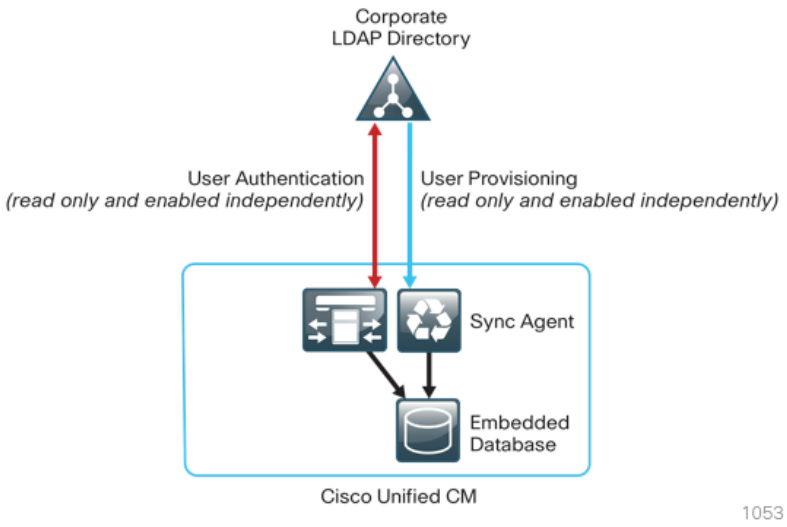
Self Provisioning

The Self-Provisioning feature allows an end user or administrator to add an unprovisioned phone to a Cisco Unified Communications Manager system with minimal administrative effort. A phone can be added by plugging it into the network and following a few prompts to identify the user.This feature enhances the out-of-box experience for end users by allowing them to directly add their desk phone or soft client without contacting the administrator. It simplifies administrator deployments by allowing them to add desk phones on behalf of an end user. The feature lets administrators and users deploy a large number of devices without interacting directly with the Cisco Unified Communications Manager Administration GUI, but from the device itself. The feature relies on the administrator preconfiguring a number of templates and profiles, so that when the phone attempts to self-provision, the necessary information is available in the system for it to create a new device.

Active Directory Integration

Active Directory integration allows you to provision users automatically from the corporate directory into the Cisco Unified CM database, which makes it possible to maintain a single directory as opposed to separate directories. Therefore, you don't have to add, remove, or modify core user information manually in Unified CM each time a change occurs in the corporate directory. The other advantage is that end users are able to authenticate to Unified CM and Cisco Unity Connection by using the same credentials in Active Directory, which reduces the number of passwords across the network.

Figure 2 - Directory integration with Cisco Unified CM



Dial Plan

The dial plan is one of the key elements of an IP telephony system and an integral part of all call-processing agents. Generally, the dial plan is responsible for instructing the call-processing agent on how to route calls. CUCC configures a North American Numbering Plan (NANP) dial plan as part of the path selection for PSTN destinations. You can modify the dial plan to meet your specific needs, but CUCC has the options to configure the NANP with 7-digit or 10-digit local dialing. The following two sets of patterns can be selected.

Reader Tip

CUCC can be used to deploy the default templates and to create new dial plans or Modify the existing ones.

Figure 3 - NANP with 7-digit local dialing

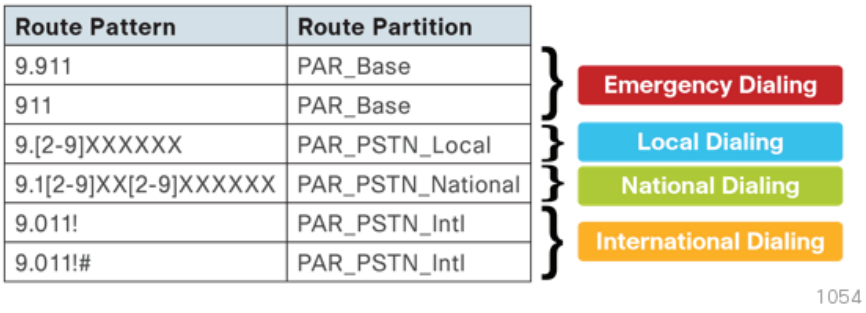


Figure 4 - NANP with 10-digit local dialing

Route Pattern	Route Partition
9.911	PAR_Base
911	PAR_Base
9.[2-9]XX[2-9]XXXXXX	PAR_PSTN_Local
9.1[2-9]XX[2-9]XXXXXX	PAR_PSTN_National
9.011!	PAR_PSTN_Intl
9.011!#	PAR_PSTN_Intl

1055

There are two configured international route patterns: one to route the variable-length dialed digits and one configured with a pound (octothorpe) in order to allow users to bypass the inter-digit timeout. The 911 and 9.911emergency route patterns are created with urgent priority to prevent inter-digit timeout delays when they are entered from a phone.

Site Codes

It is recommended that you use a uniform on-net dial plan containing an access code, a site code, and a 4-digit extension. The use of access and site codes enables the on-net dial plan to differentiate between extensions at remote sites that could otherwise overlap with each other.

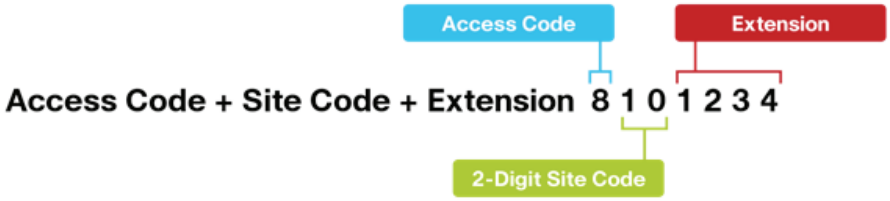
When you use this method, a phone in San Jose, CA can have the same 4-digit extension as one in Houston, TX without creating a numbering conflict. For example: 408-555-**1234** in San Jose and 713-555-**1234** in Houston.

For networks with 90 sites or less, the dial plan consists of the following:

- One digit as an inter-site access code
- Two digits for the site code to accommodate up to 90 sites
- Four digits for the site extension

CUCC requires a format of 8 + SS + XXXX, where 8 is the on-net access code, SS is a 2-digit site code of 10-99, and XXXX is a 4-digit extension number, giving a total of seven digits.

Figure 5 - Two-digit site code format



1056

Class of Service

Class of service is configured in Cisco Unified CM by using calling search spaces and partitions. There are four classes of service, and they provide PSTN access for emergency, local, national, and international dialing.

Figure 6 - Calling search spaces and partitions

	Calling Search Space	Route Partition 1	Route Partition 2	Route Partition 3
1	CSS_Base	PAR_Base	—	—
2	CSS_LocalPSTN	PAR_PSTN_Local	—	—
3	CSS_NationalPSTN	PAR_PSTN_Local	PAR_PSTN_National	—
4	CSS_InternationalPSTN	PAR_PSTN_Local	PAR_PSTN_National	PAR_PSTN_Intl

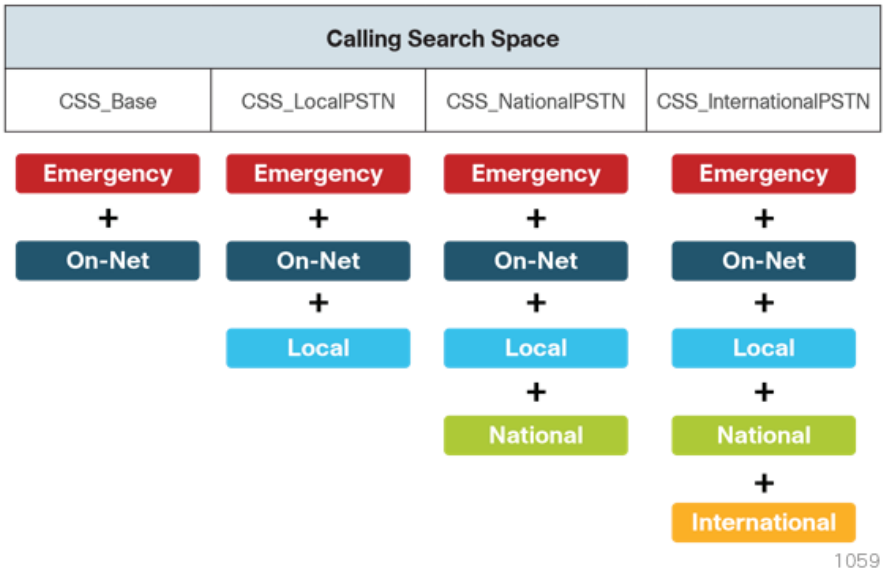
1 Emergency Dialing
2 Local Dialing
3 National Dialing
4 International Dialing

1058

With CUCC, devices are auto-registered with the CSS_Base calling search space. This allows all devices to dial both on-net and emergency off-net numbers.

The remaining calling search spaces are configured on the user device profile directory number and provide local 7-digit or local 10-digit, national, and international dialing capabilities.

Figure 7 - Calling capabilities for calling search spaces



1059

For example, if a user requires international dialing capability, their directory number would be assigned the CSS_InternationalPSTN calling search space, which includes dialing accessibility to all PSTN route patterns as well as national, local, emergency, and on-net numbers.

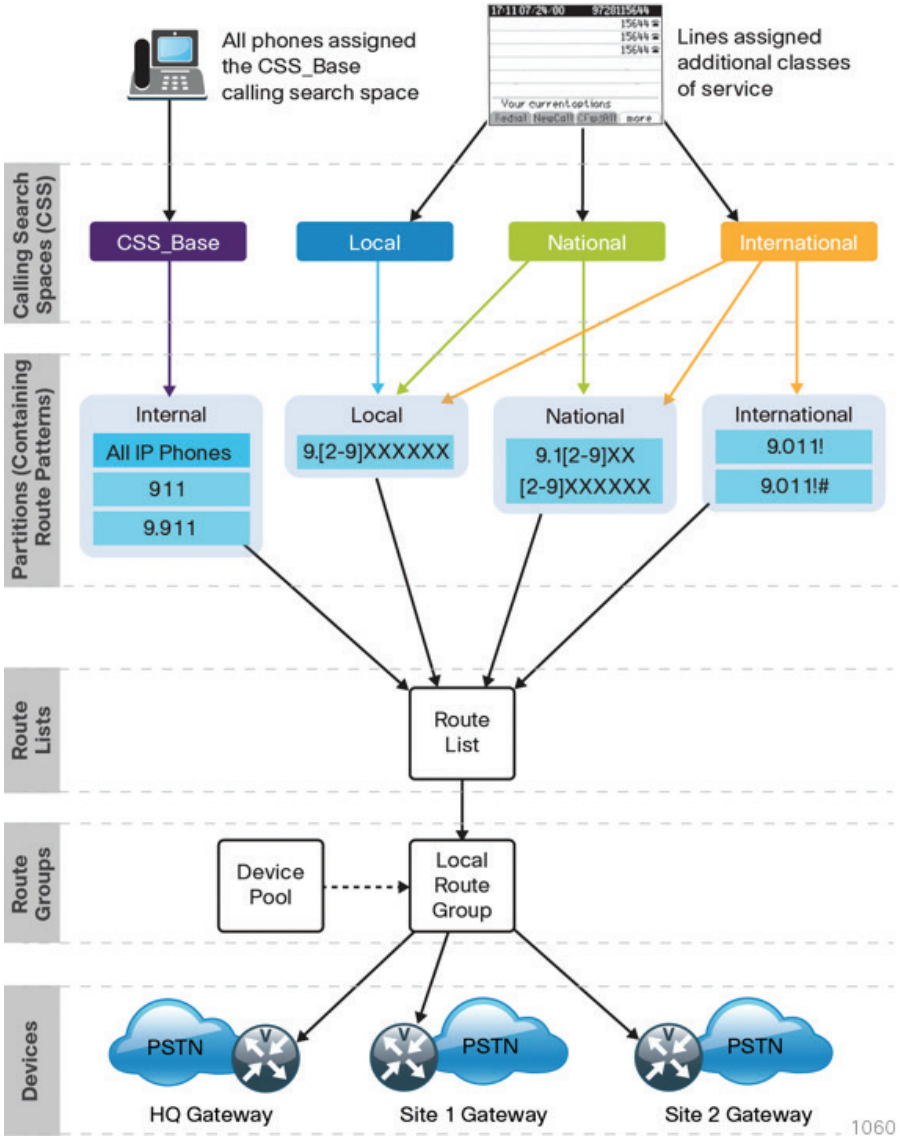
> **Tech Tip**
>
> This CVD is considering 8+ 6-digit dial plan for this deployment, which is based on NANP dial plan principles. In case there is a need for +E.164 dial plan for your deployment, please refer to Collaboration Solution Reference Network Design (SRND) Dial Plan chapter.

Local Route Groups

The Local Route Group feature in Cisco Unified CM decouples the PSTN gateway physical location from the route patterns and route lists that are used to access the gateway. The feature assigns a local route group to each route group, based on the device pool setting of the originating device. Therefore, phones and other devices from different locations can use a single set of route patterns, but Unified CM selects the correct gateway to route the call.

CUCC assigns a unique route group to a device pool so each site can choose the correct SIP gateway. The route group is associated with the device pool by using the local route group setting. This simplifies the process of provisioning by allowing the administrator to create a single set of route patterns for all sites. When a call is made from a device that matches the route pattern, Cisco Unified CM uses the Local Route Group device pool setting to determine the proper route group, which selects the SIP gateway assigned to the site.

Figure 8 - Cisco Unified CM call routing



Survivable Remote Site Telephony

In a centralized design, when IP phones lose connectivity to Cisco Unified CM because the application is unreachable, IP phones in remote-site offices or teleworker homes lose call-processing capabilities. The Survivable Remote Site Telephony (SRST) feature provides basic IP telephony backup services because IP phones fall back to the local router at the remote site when connectivity is lost. IP phones continue to make calls within the site and out the local gateway to the PSTN.

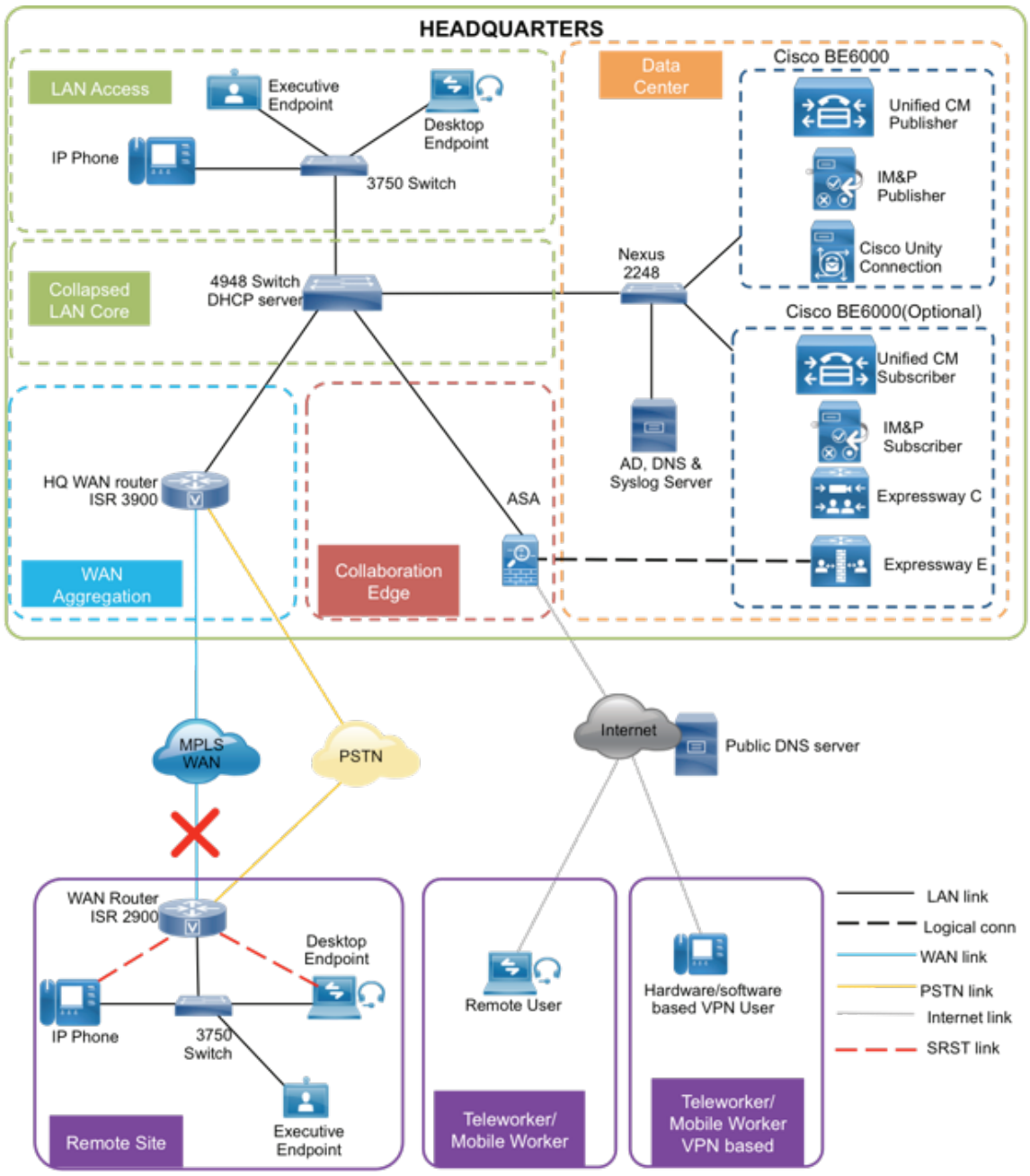
At a remote site with more than one PSTN gateway, configure SRST on the router with the most voice ports. If only one router has PSTN interfaces, SRST must be configured on the router to reduce complexity.

Using the Cisco 2921 ISR router, a maximum of 100 phones are supported at a remote site. If you have more phones than a single SRST router can manage, you should consider using the higher end ISR router 3945.

Phones can use SCCP or SIP to register with the SRST process on the remote-site router. Different commands are needed for each type of phone, and the commands can be configured together or individually on each router within the organization.

The following diagram shows SRST providing service to phones at a remote site when the WAN is down.

Figure 9 – SRST at a remote site



When a remote site falls back to SRST and site codes are in use, voice translation commands are required in the router to maintain 4-digit local dialing. The commands are explained in more detail in the deployment section of this guide.

Device Mobility

CUCC uses a feature called *device mobility* that allows Cisco Unified CM to determine if the IP phone is at its home or a roaming location. Unified CM uses the device's IP subnet to determine the physical location of the IP phone. By enabling device mobility within a cluster, mobile users can roam from one site to another, thus acquiring the site-specific settings. Unified CM then uses these dynamically allocated settings for call routing, codec selection, media resource selection, and Unified CM groups.

This feature is used primarily to reduce the configuration on the devices themselves by allowing configuration of many parameters at the site level. These parameters are dynamically applied based on the subnet to which the device is attached. This allows for a fast and reliable deployment because the administrator does not have to configure each phone individually or ensure the phone is at the correct location.

Extension Mobility

CUCC uses the Extension Mobility feature, enabling end users to personalize a Cisco Unified IP Phone, either temporarily or permanently, based on business requirements. The Extension Mobility feature dynamically configures a phone according to the authenticated user's device profile. Users log into an IP phone with their username and PIN, and their device profile is uploaded to the IP phone. Extension Mobility alleviates the need for device-to-user association during provisioning. This saves deployment time while simultaneously allowing the user to log into any phone within the organization, allowing phone-sharing capabilities.

Extension Mobility can be enabled in such a way that it allows users to log into IP phones but does not allow them to log out. With this method, Extension Mobility is exclusively designed for IP phone deployment, but not as an ongoing feature in the organization. By default, the CUCC configuration allows users to log out of the IP phone, which enables Extension Mobility for both IP phone deployment and user feature functionality.

Tech Tip

The user-provisioning capabilities of this guide require an IP phone that supports services to allow the use of Extension Mobility. All users imported with CUCC will have a default PIN of *112233*

Extend and Connect

Extend and Connect allows users to benefit from UC enabled applications, such as Jabber, from any telephone. By associating a CTI enabled profile with any callable number, administrators can offer users the ability to control calls from their home or digital PBX line from their computer. Refer to the Configuring Extend and Connection section of this document for further details.

Media Resources

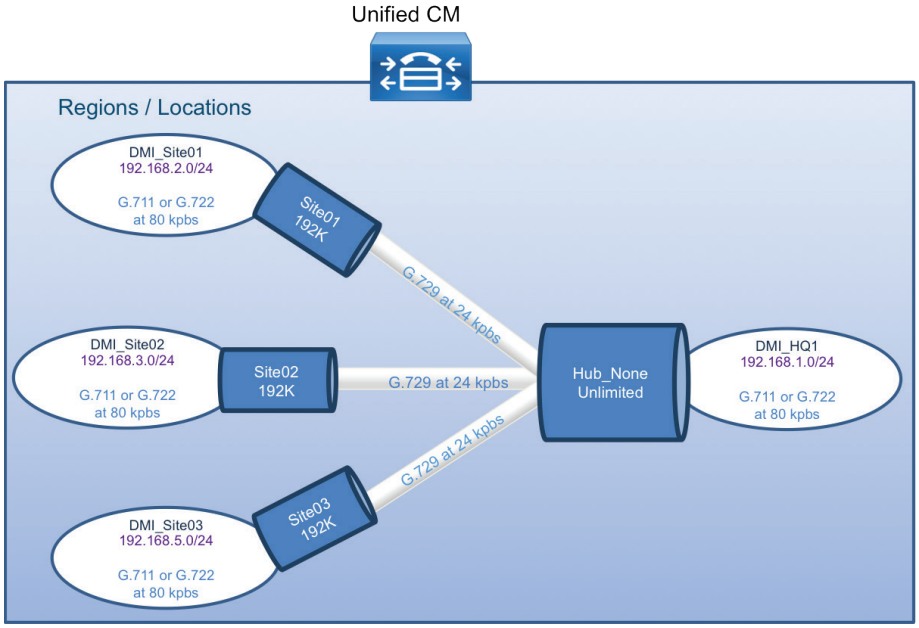
Media resources have been provisioned as part of the procedure for every site in order to ensure that remote sites use their local conference bridges and avoid unnecessary voice traffic over the WAN. The naming of the conference bridges needs to match those provisioned by CUCC. The names are always CFB1<*Site Name*> and CFB2<*Site name*>, if there are two. For example, if the headquarters site is HQ1, the conference bridge names are CFB1HQ1 and CFB2HQ1.

Call Admission Control

The default design is a hub-and-spoke topology in which each remote site is connected to the headquarters site over a bandwidth-constrained WAN. The CUCC design uses regions and locations to define locations-based Call Admission Control. For calls within a site, the regions are configured for the G.722 or G.711 codec running at 80 kbps, and there are no limits to the number of calls allowed within a site. For calls between the sites, the regions are configured for the G.729 codec running at 24 kbps. The size of the site determines the CUCC default voice bandwidth setting for inter-site calls. For sites with only 500 users, the default setting is two inter-site calls (48 kbps). The amount of bandwidth in and out of each site can be modified within CUCC, if the defaults do not match the provisioned WAN bandwidth.

By default, Call Admission Control is not calculated for calls to and from the central site (headquarters). It's expected that as long as the spokes are provisioned for Call Admission Control, the hub will not be oversubscribed on a traditional WAN. This is the case for all hub-and-spoke topologies; however, for a Multiprotocol Label Switching (MPLS)-based network, which is considered a hub-less hub and spoke, you will need to modify the headquarters site default bandwidth within CUCC to provide the correct Call Admission Control based on the speed of the link.

Figure 10 - Hub-and-spoke topology for Call Admission Control



Point-to-Point Video

CUCC can be used to deploy the video endpoint, which would enable point-to-point video between two participants. Desktop Video endpoints such as EX60, EX90 and DX650 can be deployed using CUCC.

IM and Presence

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 solutions can be deployed using a mixture of on-premise and cloud based solutions.

The on-premises Jabber solution includes the following components:

- 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
- Cisco 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)

This guide describes 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.

      You can make, receive, and control your phone calls whether you are in or out of the office and support business-quality video communication up to high-definition (720p) and high-fidelity wideband audio. You can also 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.

Self Care

Unified Communications Self-Care Portal is used to configure user settings for your Cisco Unified IP Phones and Jabber applications. Using Unified Communications Self Care Portal, end user can configure settings such as speed dial numbers, contact lists, phone services, and voicemail notifications. Administrator can control the access to the Self Care portal, end users can also access the Self Care portal provided information on how to use it. Before a user can start using the Self Care portal the user should be added as a user on the Cisco Unified Communications Manager end user group. The Url to access the Self Care portal is https://cucmhostname:portnumner/ucmuser.

CUCC Directories and Filenames

The Cisco Unified Configurator for Collaboration (CUCC) tool is available in a Windows and Mac version. The different versions can be downloaded from the following URLs:

- Windows: http://www.cisco.com/go/cvd/collaboration
- Mac: http://www.cisco.com/go/cvd/collaboration
- CUCC has several directories and key filenames that are referenced throughout this guide. The following table lists the directories and filenames.

Table 3 - CUCC directories and filenames

Type	Path or filename	Description
Default	.\	Default directory
	.\CUCC.exe or CUCC.app	CUCC application
	.\Sample User.csv	Sample csv file for New Users and Device Profiles
	.\Readme.txt	This table
Log	.\log	System log directory
	.\log\ccts.log	General log for all areas
	.\log\new_server.log	New Server and Site log
	.\log\export_gateway.log	Gateway Template log
	.\log\new_user.log	New Users and Device Profiles log
	.\log\modify_server.log	Modify Server and Site log
	.\log\modify_user.log	Modify Users and Device Profiles log
	.\log\phone.log	Phone Deployment log
Summary	.\Overview	Summary overview directory for data used in Server and Site
Output	.\packet	Output packet directory
	.\packet\gateway	Output text files for Gateway Templates formatted as follows: SIP_Site_Name_GWY.txt
	.\packet\saveAllData	Output tar file for Saved Entered Data
	.\packet\server	Output tar files for Server and Site formatted as follows: Server_YYYYMMDDhhmm.tar
	.\packet\user	Output tar files for Users and Device Profiles formatted as follows: User_YYYYMMDDhhmm.tar

Type	Path or filename	Description
Input	.\template	Input template directory
	.\template\dialplan	Input csv files for Dial Plan
	.\template\user	Input csv and xml files for Users and Device Profiles
	.\template\gateway	Input xml file for Gateway Templates
	.\template\Server	Input tar file for base Unified CM configuration
	.\template\site	Input csv sample files for Site Information
	.\template\temp	Input csv files extracted from base Unified CM tar file
	.\template\udp	Input xml files for Device Profiles

Deployment Details

This guide uses CUCC to install, configure, and deploy basic telephony and simple voice messaging. This turnkey solution is easy and quick. It also provides a solid foundation for further configuration and deployment of advanced unified communications features, without the need to redesign or reengineer when a new element or service is added.

The first process presents detailed procedures for preparing your network for IP phones and provides a section on how to choose the correct Cisco Unified IP Phones for your organization.

PROCESS

Preparing the Network for IP Phones

1. Enable DHCP option 150

The campus design is voice-ready because it includes the QoS settings, VLANs, and IP subnets needed for voice endpoints. It also includes the Dynamic Host Configuration Protocol (DHCP) scopes for the voice VLANs. However, the DHCP option that automatically assigns the call-control agent to the voice endpoints is covered in this module because it is specific to the Cisco Unified Communications solution.

Procedure 1 Enable DHCP option 150

DHCP is used to obtain an IP address, subnet mask, default gateway, domain name, DNS addresses, and TFTP server information. When you are configuring DHCP for use in a Cisco Unified CM deployment, this design recommends a localized server or Cisco IOS device to provide DHCP service at each site. This type of deployment ensures that DHCP services are available to remote-site telephony devices during WAN failures.

DHCP option 150 provides the IP addresses of the TFTP servers, which allows the phones to download their configuration files and firmware. This option is added to the voice scopes for wired and wireless networks. Option 150 allows up to two IP addresses to be returned to phones as part of the DHCP scope.

The phone always tries the first address in the list, and it only tries the subsequent address if it cannot establish communications with the first TFTP server. The second address provides a redundancy mechanism that enables phones to obtain TFTP services from another server if their primary TFTP server is unreachable. However, it does not provide dynamic load balancing between the two servers. This design recommends that you configure different ordered address lists of TFTP servers in the DHCP scopes to allow for manual load balancing.

For example:

- In subnet 192.168.2.0/24, option 150: CUCM-Pub (primary), CUCM-Sub (secondary)
- In subnet 192.168.5.0/24, option 150: CUCM-Sub (secondary), CUCM-Pub (primary)

Under normal operations, a phone in subnet 192.168.2.0/24 will request TFTP services from CUCM-Pub, while a phone in subnet 192.168.5.0/24 will use CUCM-Sub. If CUCM-Pub fails, then phones from both subnets will request TFTP services from CUCM-Sub. The method for load sharing between the DHCP scopes is left up to the network administrator, because they will have the best knowledge of how many phones reside in each subnet.

If the remote site has a single WAN router without a distribution layer, the best place for DHCP is on the router. If the remote site has dual WAN routers or a distribution layer, the DHCP service should be located on a standalone server or on a distribution switch.

In all situations, phones need option 150 added to their DHCP scope configurations. If the headquarters site uses the primary TFTP server as the first choice, the remote sites should use the secondary TFTP as the first choice until the phone count is balanced between the two servers.

If you are using a Microsoft DHCP server, complete Option 1 of this procedure. If you are using the Cisco IOS DHCP server feature, complete Option 2.

Option 1: Enable option 150 on Microsoft DHCP server

Use the following commands in order to enable option 150 on a Microsoft DHCP server.

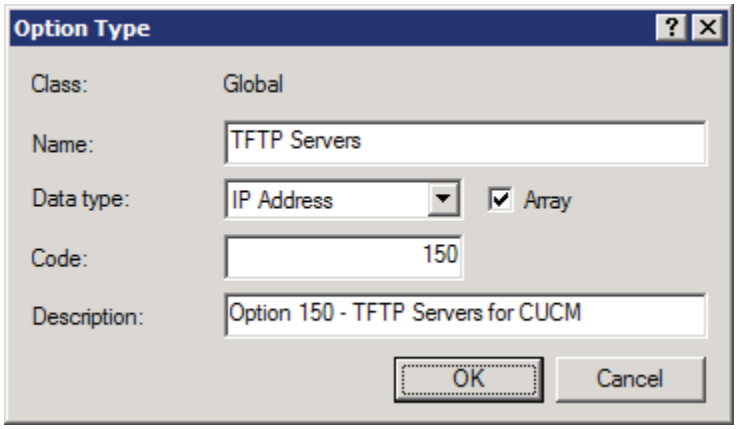
Step 1: From the Microsoft server, open the DHCP Server Administration Tool.

Step 2: On the left side of the page, navigate to **[active directory name] > IPv4** (Example: ad.cisco.local > IPv4).

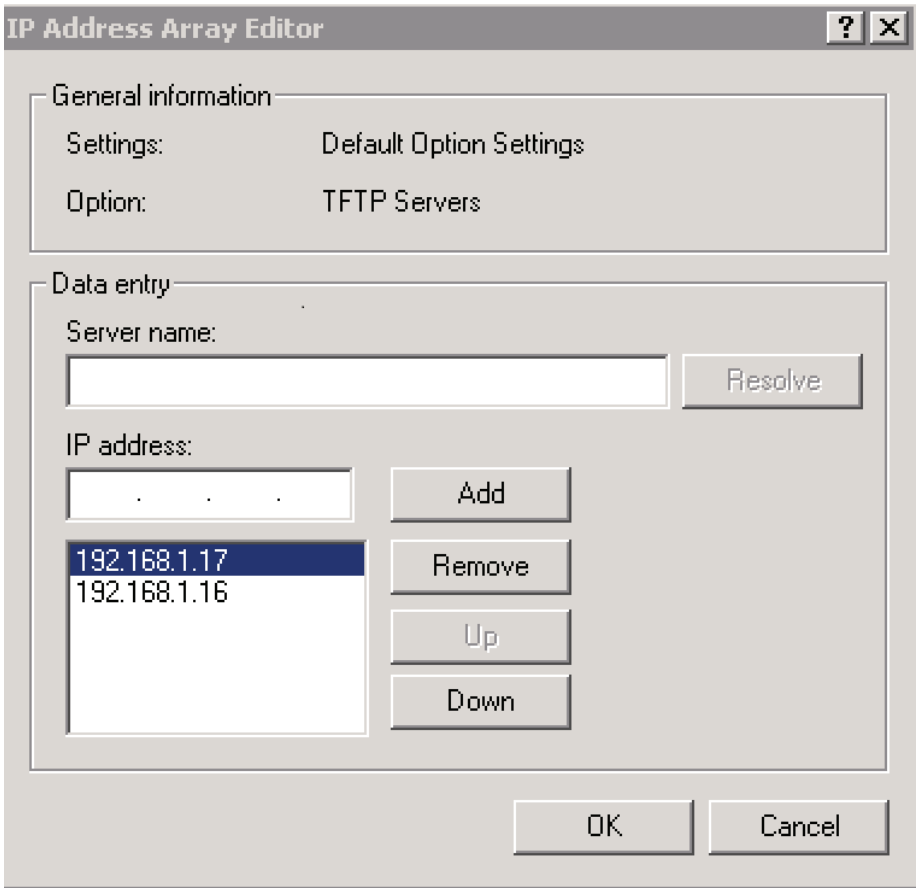
Step 3: Right-click **IPv4**, and then choose **Set Predefined Options** from the list.

Step 4: Click **Add**, enter the following information, and then click **OK**:

- Name–**TFTP Servers**
- Data Type–**IP Address**
- Array–Select the check box.
- Code–**150**
- Description–**Option 150 – TFTP Servers for CUCM**



Step 5: Click **Edit Array**, add up to two IP addresses for your TFTP servers, and then click **OK**.



Step 6: On the Predefined Options and Value page, verify the information, and then click **OK**.

Option 2: Enable option 150 using Cisco IOS DHCP server feature

Use the following commands in order to enable option 150 in the appropriate DHCP pools in Cisco IOS devices.

Step 1: Log in to the device with a username that has the ability to make configuration changes.

Step 2: In the global configuration section, edit the DHCP pools supporting IP phones to include option 150 so the phones can find the TFTP servers at 192.168.1.17 (secondary) and 192.168.1.16 (primary).

```
ip dhcp pool wired-voice
  network 192.168.5.0 255.255.255.0
  default-router 192.168.5.1
  dns-server 192.168.1.10
  option 150 ip 192.168.1.17 192.168.1.16
  domain-name cisco.local

ip dhcp pool wired-voice2
  network 192.168.2.0 255.255.255.0
  default-router 192.168.2.1
  dns-server 192.168.1.10
  option 150 ip 192.168.1.17 192.168.1.16
  domain-name cisco.local
```

Phone Models

For decades, traditional phone systems have provided basic dial tone and voicemail services, but there is little they can offer in terms of advanced communication features. Organizations who lead the way in technological innovation expect the next generation of handsets to provide features that will transform the way they operate their business. Even as they lead the way with new tools and technology, they want to cut costs by eliminating expensive wiring to every desktop and lowering electricity usage. The high cost of energy and the push for a greener planet is causing organizations to rethink every aspect of their business to see if they can lower their carbon footprint.

At the other end of the spectrum, cost-conscious organizations want to lower costs and see short term returns on their investments. Aging phones systems have been discontinued, and spare parts are getting harder to find. These challenges are causing organizations to search for a cost-effective solution to their telephony needs.

Several new Cisco Unified IP Phones have been introduced over the last few years to address the high-end and cost-conscious business models. Cisco Unified IP Phones 9951 and 9971 support video telephony by adding a USB camera to a high-end color phone. This allows customers to meet face-to-face with others in their organization by using the simple interface of a telephone. The color screens are larger with higher resolution than other models, and they support more tilt options to allow better viewing of the video images. They support Bluetooth and USB to give the end user more flexibility when choosing headsets. Cisco Unified IP Phone 9971 supports Wi-Fi connectivity, which frees users from the constraints of a hardwired telephone infrastructure within their buildings. Cisco Unified IP Phone 8945 also supports video telephony with a built-in camera and a high-resolution color display. Cisco Unified IP Phone 8900 Series and 9900 Series have a deep-sleep power-save option, which can reduce power consumption by up to 90 percent compared to the normal operation of the phone. This design recommends Unified IP Phone 8945 for a four-line video phone and Unified IP Phone 9971 for a five-line, video, and Wi-Fi–enabled phone.

Cisco Unified IP Phone 7800 Series is a high-fidelity voice communications portfolio designed for people-centric collaboration. It combines always-on reliability and security, full-featured easy-to-use IP telephony, and wideband audio to increase productivity, with an earth-friendly design for reduced costs. These basic phone models provide essential calling functionality and still maintain the inherent flexibility of an IP-based endpoint, which operates from an existing Ethernet port for power and connectivity. The Cisco IP Phone 7800 Series brings a higher quality standard, with full wideband audio support for handset, headset and speaker, to our voice-centric portfolio. A new ergonomic design includes support for larger grayscale, graphical backlit displays.

Cisco Unified IP Phone 7821 is a two-line, endpoint that is designed for information workers and managers. The Cisco IP phone 7841 is a four-line endpoint that is designed for information workers, the administrative staff and managers who have moderate level of voice communication needs. The Cisco IP phone 7861 has 16 lines and is ideal for the users such as administrative staff, managers and agents in contact centers.

Cisco Unified Wireless IP Phone 7925 is recommended for mobility, Cisco Unified IP Conference Station 7937 is recommended for conference rooms, and the Cisco IP Communicator software client is recommended to provide a desktop computer solution.

The phones take full advantage of the Cisco recommended QoS settings by using Class Selector 3 (CS3) for signaling, Assured Forwarding 41 (AF41) for video, and Expedited Forwarding (EF) for voice. These settings are recommended for Cisco Medianet because they provide optimum voice and video quality while maintaining the integrity of the data flows within the network. The phones can also use SRST at the remote sites in order to provide survivability in the case of a WAN outage.

Cisco Unified IP Phone 7900 Series are also available as an alternative for users who do not need the high-end features of the Unified IP Phone 8900 and 9900 Series phones, but require more functionality than what is found in the Unified IP Phone 7800 Series models.

Network Preparation Summary

To ensure that your phones are registered at the correct time, you need to deploy DHCP option 150 and select your IP phone models before you perform the deployment procedures found in the next process.

PROCESS

Preparing the Platform for Cisco Unified CM

1. Configure platform connectivity to the LAN
2. Prepare the server for Unified CM

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

- Download the Open Virtual Archive (OVA) file from the Cisco website at: http://software.cisco.com/download/release.html?mdfid=285963825&flowid=50402&softwareid=283088407&release=10.5(1)&relind=AVAILABLE&rellifecycle=&reltype=latest

  For an installation using ESXi 4.1, choose the latest OVA file with vmv7 in the name. For example: **cucm_10.5_vmv7_v1.7.ova**

  For an installation using ESXi 5.0 or higher, choose the latest OVA file with vmv8 in the name. For **example: cucm_10.5_vmv8_v1.7.ova**

- Check the Cisco website to determine if there is a patch for your version of Cisco Unified CM: http://software.cisco.com/download/release.html?mdfid=285963825&flowid=50402&softwareid=282074295&release=10.5(1)&relind=AVAILABLE&rellifecycle=&reltype=latest

Procedure 1 Configure platform connectivity to the LAN

The Cisco Unified CM server can be connected to a Cisco Nexus switch in the data center or a Cisco Catalyst switch in the server room. Please choose the option that is appropriate for your environment.

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

Step 1: Log in 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 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.

```
interface Ethernet1/1/4
 description Unified CM
 switchport access vlan 148
```

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

Step 1: Log in 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 server is connected.

```
default interface GigabitEthernet1/0/6
```

Step 3: Configure the port as an access port.

```
interface GigabitEthernet1/0/6
 description Unified CM
 switchport access vlan 148
```

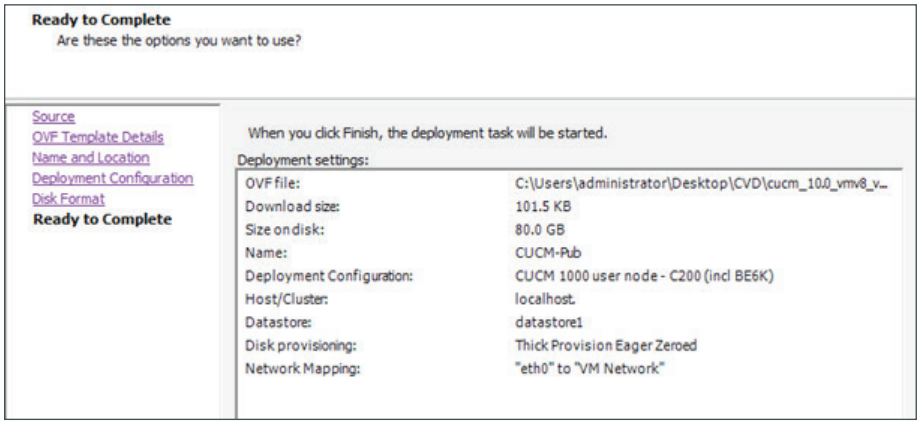
Procedure 2 Prepare the server for Unified CM

Follow the steps below to deploy an OVA file in order to define the virtual machine requirements.

Step 1: Open VMware vSphere Client, click the server hardware you want to use for this install, and then navigate to **File > Deploy OVF Template**.

Step 2: In the Deploy OVF Template wizard, enter the following information:

- On the Source page, click **Browse**, select the Cisco Unified CM OVA file downloaded from Cisco or from the datastore of the Cisco BE 6000 server, click **Open**, and then click **Next**.
- On the OVF Template Details page, verify the version information, and then click **Next**:
- On the Name and Location page, in the Name box, enter the virtual machine name **CUCM-Pub**. In the Inventory Location tree, select the location to deploy the server, and then click **Next**.
- On the Deployment Configuration page, in the **Configuration** list, choose the following node, and then click **Next**.
  - **1000-user node (BE6K)**—for a cluster of 1000 or fewer users.
- On the Disk Format page, choose **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-Pub), 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**, navigate to the location of the Cisco Unified CM bootable installation file (or browse the datastore to find the CUCM installation file), select the correct ISO image, and then click **OK**.

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

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

After the ISO loads, the virtual machine is prepared for installation.

PROCESS

Installing Cisco Unified CM

1. Install the first Cisco Unified CM platform
2. Install licenses and start services
3. Configure additional servers
4. Install the redundant server
5. Start services

The following information is needed for the installation:

- 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
- Lightweight Directory Access Protocol (LDAP) information for integration with Microsoft's Active Directory:
    - Manager Distinguished Name (read access required)
    - User Search Base
    - Host name or IP address and port number for the LDAP server

When users are created in Active Directory, either the telephone number or the IP phone attribute is mandatory. Otherwise, the users cannot be imported into Cisco Unity Connection.

Complete the tasks listed below before you start the installation:

- In DNS, configure Cisco Unified CM host names
- Obtain license files from the Cisco licensing system
- On the PC or Mac used for administration, install an archive program for opening .tar files

For standard deployments, this design recommends that you configure Cisco Unified CM to use IP addresses rather than host names. However, during the initial installation of the publisher node in a Unified CM cluster, the publisher is referenced in the server table by the host name you provided for the system. When new subscribers are added to a publisher, the initial use of host names makes it easier to identify the servers for troubleshooting purposes. The host names will be changed to IP addresses later in this guide.

Each subscriber should be added to this server table one device at a time, and there should be no definitions for non-existent subscribers at any time, other than for the new subscribers being installed.

Procedure 1 Install the first Cisco Unified CM platform

This procedure is for installing the first Cisco Unified CM platform. If this is not the first Unified CM platform, skip ahead to Procedure 6, "Install the redundant server."

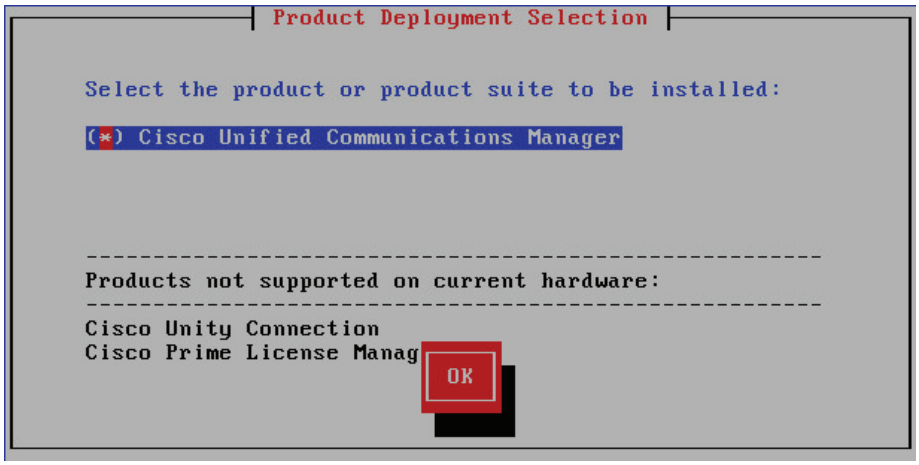
After the ISO/DVD loads, continue the installation on the server console.

Step 1: On the DVD Found page, choose **OK**.

Step 2: If the media check passes, 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, choose **Cisco Unified Communications Manager**, and then choose **OK**



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: On the Apply Patch page, choose **No**.

Step 7: If the Import Windows Data page is displayed, choose **No**.

Step 8: On the Basic Install page, choose **Continue**.

Step 9: On the Timezone Configuration page, use the arrow keys to select the correct time zone, and then choose **OK**.

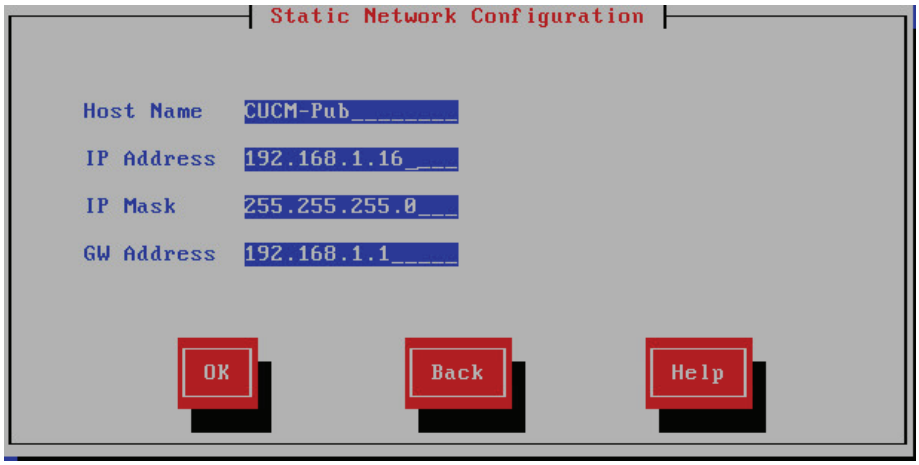
Step 10: On the Auto Negotiation Configuration page, choose **Continue**.

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

Step 12: On the DHCP Configuration page, choose **No**.

Step 13: On the Static Network Configuration page, enter the following information, and then choose **OK**:

- Host Name–**CUCM-Pub** first node (publisher)
- IP Address–**192.168.1.16**
- IP Mask–**255.255.255.0**
- GW Address–**192.168.1.1**



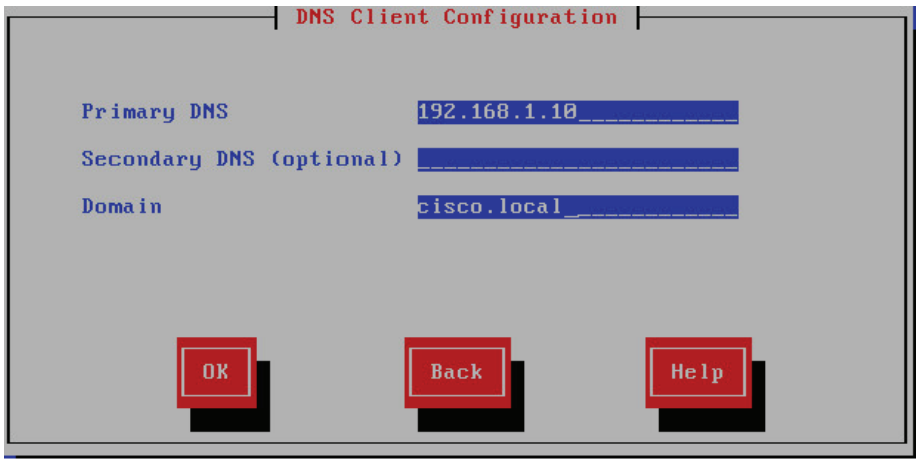
Tech Tip

During the software installation, the server performs a reverse DNS lookup on the name and IP address entered above. The installation halts if the lookup does not succeed, so please verify your server information is properly entered into DNS and the associated pointer records are created beforehand.

Step 14: On the DNS Client Configuration page, choose **Yes**.

Step 15: Enter the following information, and then choose **OK**:

- Primary DNS–**192.168.1.10**
- Domain–**cisco.local**

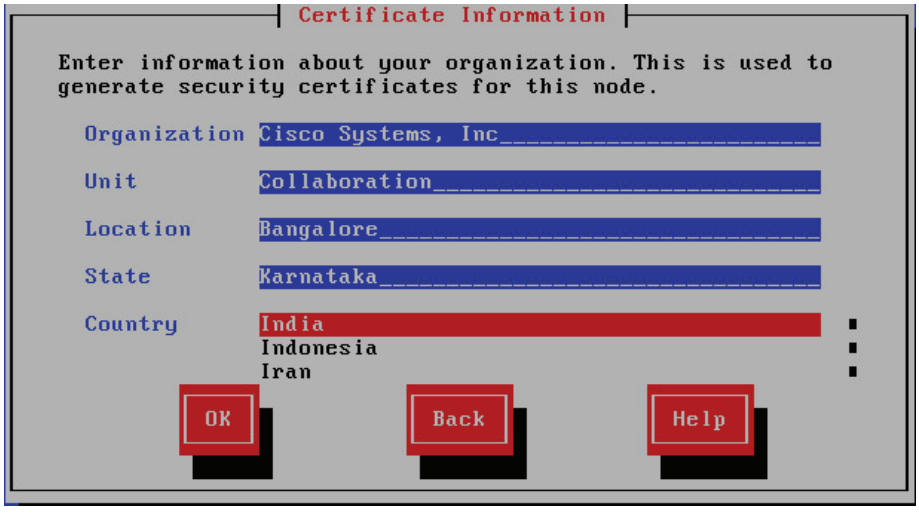


Step 16: On the Administrator Login Configuration page, enter the following information, and then choose **OK**:

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

> **Tech Tip**
>
> The password must start with an alphabetic character and have at least six characters, and it can contain alphanumeric characters, hyphens, or underscores.

Step 17: On the Certificate Information page, enter the details that will be used to generate the certificate used for secure communications, and then choose **OK**.



Step 18: On the First Node Configuration page, choose **Yes**.

Step 19: On the Network Time Protocol Client Configuration page, next to the NTP Server 1 prompt, enter **192.168.1.10**, add up to four more NTP host names or IP addresses, and then choose **OK**.

Step 20: On the Security Configuration page, enter a security password, confirm the password, and then choose **OK**.

You use the security password during the remaining nodes installation process.

Step 21: On the SMTP Host Configuration page, choose **No**.

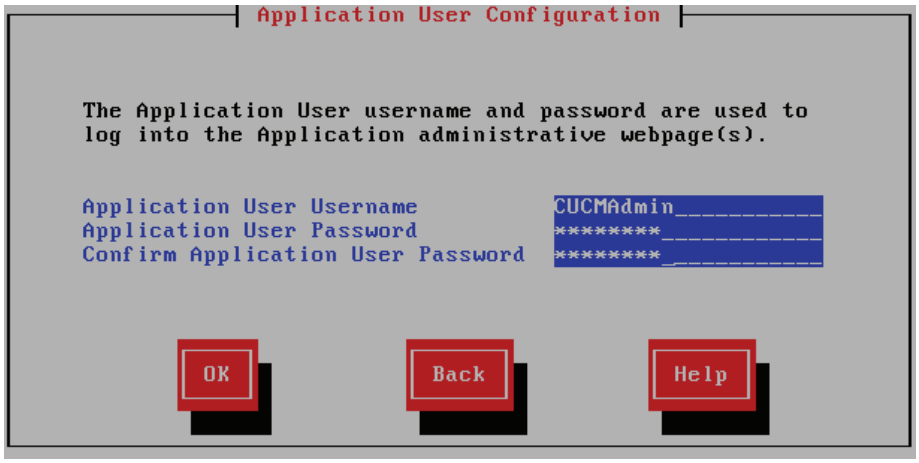
Step 22: On the Smart Call Home Enable Page, choose Disable all Call Home on System Start.

Tech Tip

Smart Call Home offers proactive diagnostics and real time alerts on click Cisco devices, which provides higher network availability and increased operational efficiency. Smart Call Home is a secure connected service of Cisco Unified Communications Essential Operate Services ESW for the Cisco Unified Communication Manager. To enable Smart Call home feature, please refer the document available at cisco.com.

Step 23: On the Application User Configuration page, enter the following information, and then choose **OK**:

- Application User Username–**CUCMAdmin**
- Application User Password–**[password]**
- Confirm Application User Password–**[password]**



Step 24: 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 25: In vSphere Client, navigate to the virtual machine's Getting Started tab, and then click **Edit virtual machine settings**.

Step 26: On the Hardware tab, select **CD/DVD Drive 1**.

Step 27: Clear **Connect at power on**, and then click **OK**.

Procedure 2 Install licenses and start services

After the first Unified CM platform is installed, there are several configuration steps that have to be completed in order to prepare the publisher for the remaining servers.

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

Step 2: On the login page, enter the following application username and password from Step 23, and then click **Login**:

- User Name–**CUCMAdmin** (case-sensitive)
- Password–**[password]**

Step 3: Navigate to **Inventory > Product Instances**, and then click **Add**.

Tech Tip

The username and password for adding the product instances is the case-sensitive platform administrator ID that was created when installing the server software.

Step 4: Enter the following information for Cisco Unified CM, and then click **Test Connection**:

- Name–**CUCM-Pub**
- Description–**CUCM Publisher**
- Product Type–**Unified CM**
- Hostname/IP Address–**192.168.1.16** (publisher)
- Username–**Admin** (case-sensitive platform administrator ID from Step 16)
- Password–**[password]**

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

Step 6: If the connection is successful, click **OK**.

If the connection is not successful, repeat Step 4 through Step 6 with the correct information.

Step 7: Click **Synchronize Now**.

Step 8: Navigate to **Licenses > Fulfillment**, and then select **Other Fulfillment Options > Fulfill Licenses from File**.

> **Tech Tip**
>
> Extract the .bin file from the .zip before trying to install the license in the next step. The installation process returns an error if you try to install the .zip file.

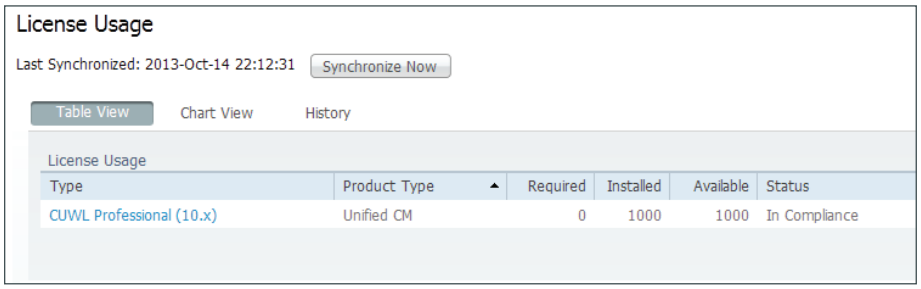
Step 9: On the Install License File page, click **Browse**, locate the directory that contains the license files you obtained prior to installation, select the .bin file, click **Open**, and then click **Install**. A message confirms that the license was successfully installed.

Step 10: Repeat Step 8 through Step 9 for each additional license file for your installation. After all files have been installed, click **Close**.

Next, you verify the licenses have been properly installed.

Step 11: Navigate to **Monitoring > License Usage**, and then confirm the status is In Compliance.

If there is a problem, please notify your Cisco representative in order to obtain new license files.



Step 12: In a web browser, access the IP address or hostname of the publisher, and in the center of the page, under Installed Applications, click **Cisco Unified Communications Manager**.

Step 13: Enter the **Username** and **Password** from the Application User Configuration page in Step 23 of the previous procedure, and then click **Login**.

Step 14: In the **Navigation** list at the top of the page, choose **Cisco Unified Serviceability**, and then click **Go**.

Step 15: Navigate to **Tools > Service Activation**, in the **Server** list, choose **CUCM-Pub**, and then click **Go**.

Step 16: Select **Check All Services**, clear the ones that are not needed for this node, and then click **Save**.

Tech Tip

You may safely disable the following services if you don't plan to use them:

Cisco Messaging Interface

Cisco DHCP Monitor Service

Cisco TAPS Service

Cisco Directory Number Alias Sync

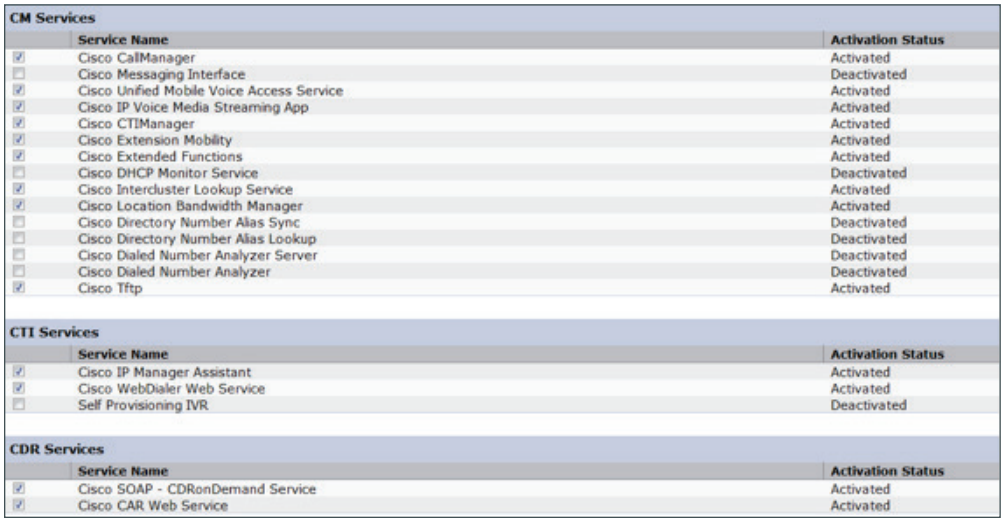
Cisco Directory Number Alias SyncCisco Dialed Number Analyzer Server

Cisco Dialed Number Analyzer

Self Provisioning IVR

Step 17: In the message window, click **OK**.

Figure 11 - Recommended publisher services when using non-dedicated TFTP server



CM Services

	Service Name	Activation Status
☑	Cisco CallManager	Activated
☐	Cisco Messaging Interface	Deactivated
☑	Cisco Unified Mobile Voice Access Service	Activated
☑	Cisco IP Voice Media Streaming App	Activated
☑	Cisco CTIManager	Activated
☑	Cisco Extension Mobility	Activated
☑	Cisco Extended Functions	Activated
☐	Cisco DHCP Monitor Service	Deactivated
☑	Cisco Intercluster Lookup Service	Activated
☑	Cisco Location Bandwidth Manager	Activated
☐	Cisco Directory Number Alias Sync	Deactivated
☐	Cisco Directory Number Alias Lookup	Deactivated
☐	Cisco Dialed Number Analyzer Server	Deactivated
☐	Cisco Dialed Number Analyzer	Deactivated
☑	Cisco Tftp	Activated

CTI Services

	Service Name	Activation Status
☑	Cisco IP Manager Assistant	Activated
☑	Cisco WebDialer Web Service	Activated
☐	Self Provisioning IVR	Deactivated

CDR Services

	Service Name	Activation Status
☑	Cisco SOAP - CDROnDemand Service	Activated
☑	Cisco CAR Web Service	Activated

Figure 12 – Recommended publisher services (continued)

Database and Admin Services

	Service Name	Activation Status
☑	Cisco Bulk Provisioning Service	Activated
☑	Cisco AXL Web Service	Activated
☑	Cisco UXL Web Service	Activated
☐	Cisco TAPS Service	Deactivated

Performance and Monitoring Services

	Service Name	Activation Status
☑	Cisco Serviceability Reporter	Activated
☑	Cisco CallManager SNMP Service	Activated

Security Services

	Service Name	Activation Status
☑	Cisco CTL Provider	Activated
☑	Cisco Certificate Authority Proxy Function	Activated

Directory Services

	Service Name	Activation Status
☑	Cisco DirSync	Activated

Activating services may take a few minutes to complete, so please wait for the page to refresh before you continue.

Procedure 3 Configure additional servers

After installing the licenses and starting the services, the subscribers, TFTP and voicemail servers must be added to the publisher. When new subscribers and TFTP servers are added to a publisher, the initial use of host names makes it easier to identify the servers for troubleshooting purposes. The host names will be changed to IP addresses later in this guide.

Do not add servers that will not be installed prior to running the CUCC tool.

Step 1: In the **Navigation** list at the top of the page, choose **Cisco Unified CM Administration**, and then click **Go**.

Step 2: Navigate to **System > Server**, and then click **Add New**

Step 3: Select the server type as CUCM Voice/Video

Step 4: Enter the host name of the additional Cisco Unified CM server, a description, and then click **Save**.

Status

Status: Ready

Server Information

Server Type	CUCM Voice/Video
Host Name/IP Address*	CUCM-Sub
IPv6 Address (for dual IPv4/IPv6)	
MAC Address	
Description	Subscriber

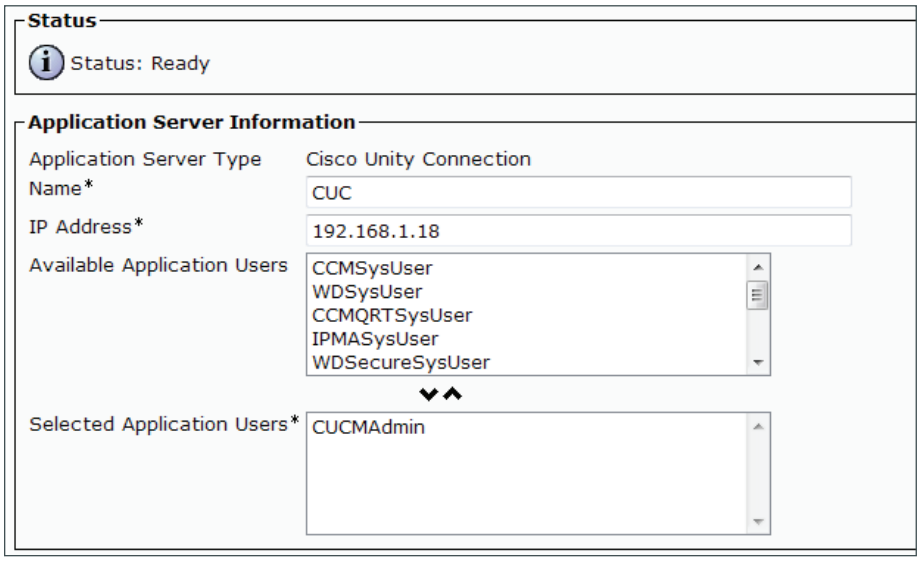
The next several steps add Cisco Unity Connection as an application server to the cluster.

Step 5: Navigate to **System > Application Server**, and then click **Add New**.

Step 6: On the first Application Server Configuration page, in Application Server Type list, choose **Cisco Unity Connection**, and then click **Next**.

Step 7: On the second Application Server Configuration page, in the Name box, enter **CUC**, and then in the IP Address box, enter **192.168.1.18**.

Step 8: In the **Available Application Users** list, select the account you created during the installation of Cisco Unified CM (Example: CUCMAdmin), move the account to the **Selected Application Users** list by clicking the **v** character, and then click **Save**.



Step 9: When the subscriber and Cisco Unity Connection servers have been added to the publisher's database, repeat the procedures in "Preparing the Platform for Cisco Unified CM" for each additional Unified CM server, and then return to Procedure 6, "Install the redundant server."

Procedure 4 Install the redundant server

This procedure installs the remaining Cisco Unified CM subscriber in a cluster.

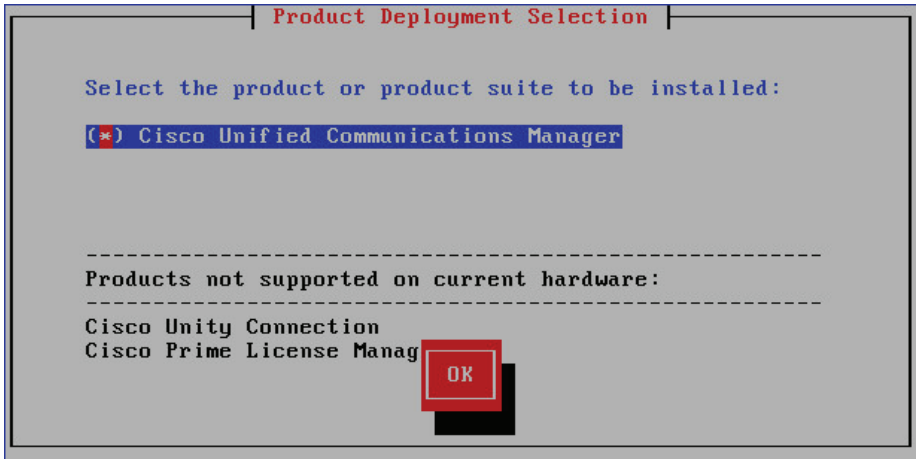
After the DVD loads, continue the installation on the server console.

Step 1: If you have not done so already, on the DVD Found page, choose **Yes**.

Step 2: If the media check passes, 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, choose **Cisco Unified Communications Manager**, and then choose **OK**.



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: On the Apply Patch page, choose **No**.

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

Step 8: On the Timezone Configuration page, use the arrow keys to select the correct time zone, and then choose **OK**.

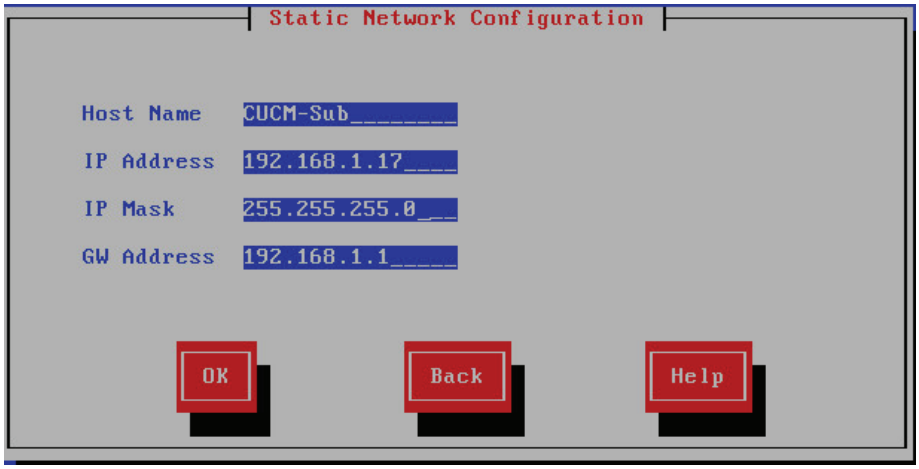
Step 9: On the Auto Negotiation Configuration page, choose **Continue**.

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-Sub** (subscriber)
- IP Address—**192.168.1.17**
- IP Mask—**255.255.255.0**
- GW Address—**192.168.1.1**



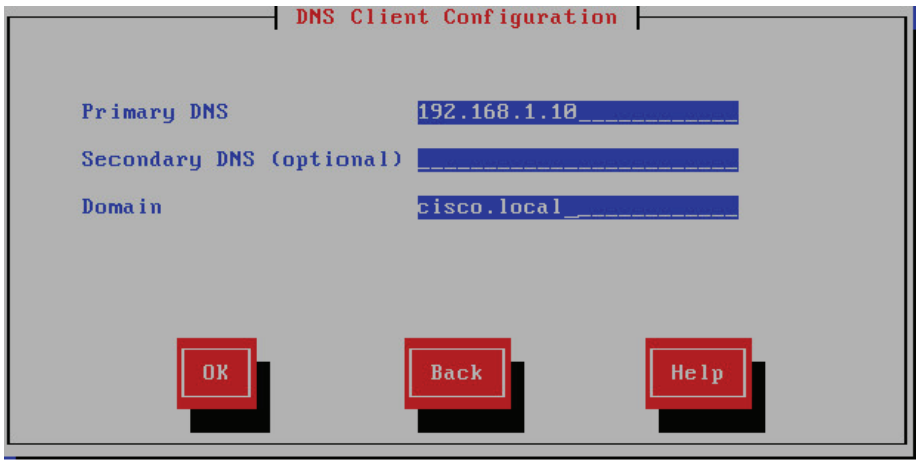
Tech Tip

During the software installation, the server performs a reverse DNS lookup on the name and IP address entered above. The installation halts if the lookup does not succeed, so please verify your server information is properly entered into DNS and the associated pointer records are created beforehand.

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

Step 14: Enter the following information, and then choose **OK**:

- Primary DNS–**192.168.1.10**
- 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]**

Tech Tip

The password must start with an alphabetic character and be at least six characters long, and it can contain alphanumeric characters, hyphens, or underscores.

Step 16: On the Certificate Information page, enter the details that will be used to generate the certificate used for secure communications, and then choose **OK**.

Step 17: On the First Node Configuration page, choose **No**.

Tech Tip

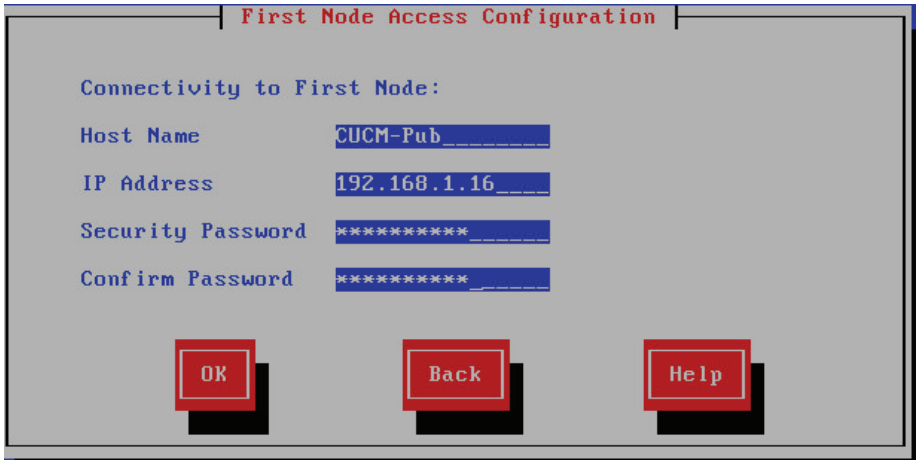
Before proceeding with the remaining nodes installation, ensure that the first node has finished installing and the subscribers have been added under the publisher's **System > Server** menu using the Cisco Unified CM administration interface.

Step 18: On the First Node Configuration page, read the warning, and then choose **OK** to acknowledge you have installed the first node and verified that it is reachable from the network.

Step 19: On the Network Connectivity Test Configuration page, choose **No**.

Step 20: On the First Node Access Configuration page, enter the following information, and then choose **OK**:

- Host Name–**CUCM-Pub** (name of publisher)
- IP Address–**192.168.1.16** (IP address of publisher)
- Security Password–**[password]** (from publisher)
- Confirm Password–**[password]**



Step 21: On the SMTP Host Configuration page, choose **No**.

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 hardware.

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

Step 23: In 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 5 Start services

After the software installation completes, the services must be started from the publisher.

Step 1: In a web browser, access the Cisco Unified CM administration interface on the 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: In the **Navigation** list on the top right side of the page, choose **Cisco Unified Serviceability**, and then click **Go**.

Step 4: Navigate to **Tools > Service Activation**.

Step 5: In the **Server** list, choose the next additional server, and then click **Go**.

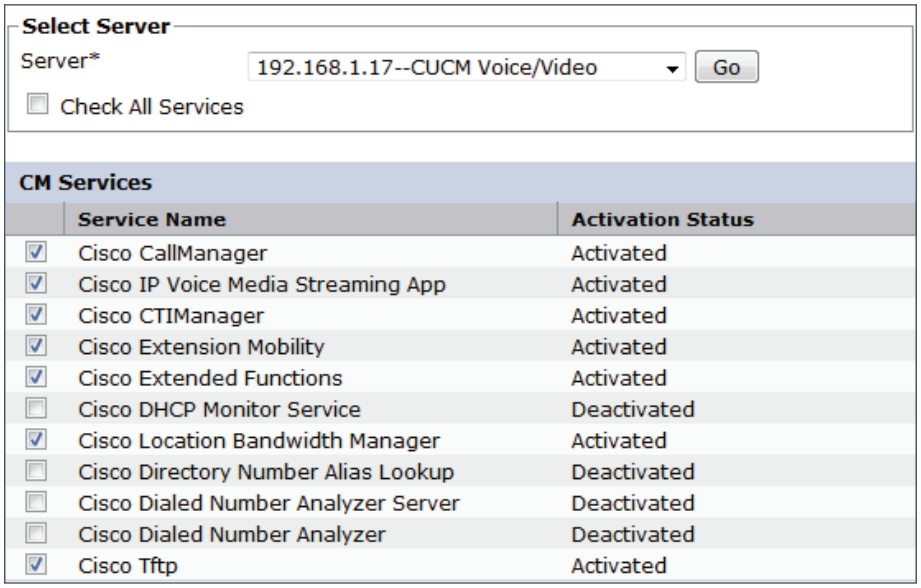
Tech Tip

If you will have more than 1250 phones in your cluster, dedicated TFTP servers are recommended, and the TFTP service is not activated on the subscriber nodes in the cluster. This design also recommends that you disable the Cisco CallManager service on the dedicated TFTP servers in order to save CPU processing.

Step 6: Select **Check All Services**, clear the ones that are not needed for this node, and then click **Save**.

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

Figure 13 - Recommended subscriber services when using non-dedicated TFTP servers



Activating services may take a few minutes to complete, so please wait for the page to refresh before continuing.

PROCESS

Preparing the Platform for Cisco Unity Connection

1. Configure platform connectivity to the LAN
2. Prepare the server for Unity Connection

Cisco Unity Connection is used as the voicemail platform for the unified communications foundation. It is configured as a simple voicemail-only system that uses a single server.

For a quick and easy installation experience, it is essential to know up-front what information you will need. To install Cisco Unity Connection, make sure you have completed the following steps before you start:

- Download the Open Virtual Archive (OVA) file from the Cisco website at: http://software.cisco.com/download/release.html?mdfid=283062758&flowid=&softwareid=282074348&os=null&release=OVA-10.0&relind=null&rellifecycle=null&reltype=null

  For an installation using ESXi 4.1, choose the latest OVA file with vmv7 in the name. For example: **CUC_10_vmv7_v1.5.ova**

  For an installation using ESXi 5.0 or higher, choose the latest OVA file with vmv8 in the name. For example: **CUC_10_vmv8_v1.5.ova**

- Check the Cisco website to determine if there is a patch for your version of Cisco Unity Connection: http://software.cisco.com/download/release.html?mdfid=285963825&flowid=50402&softwareid=282074295&release=10.5(1)&relind=AVAILABLE&rellifecycle=&reltype=latest

Procedure 1 Configure platform connectivity to the LAN

The Cisco Unity Connection server can be connected to a Cisco Nexus switch in the data center or a Cisco Catalyst switch in the server room.

Option 1: Connect the Cisco Unity Connection server to a Cisco Nexus 2248UP switch

Step 1: Log in 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 Unity Connection 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.

```
interface Ethernet1/1/14
 description Unity Connection
 switchport access vlan 148
```

Tech Tip

When deploying a dual-homed Cisco Nexus 2248 switch, this configuration is applied to both Nexus 5548 switches.

Option 2: Connect the Cisco Unity Connection 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 Unity Connection server is connected to trust the DSCP markings.

Step 1: Log in 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 Unity Connection server is connected.

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

Step 3: Configure the port as an access port

```
interface GigabitEthernet1/0/16
 description Unity Connection
 switchport access vlan 148
 switchport host
```

Procedure 2 Prepare the server for Unity Connection

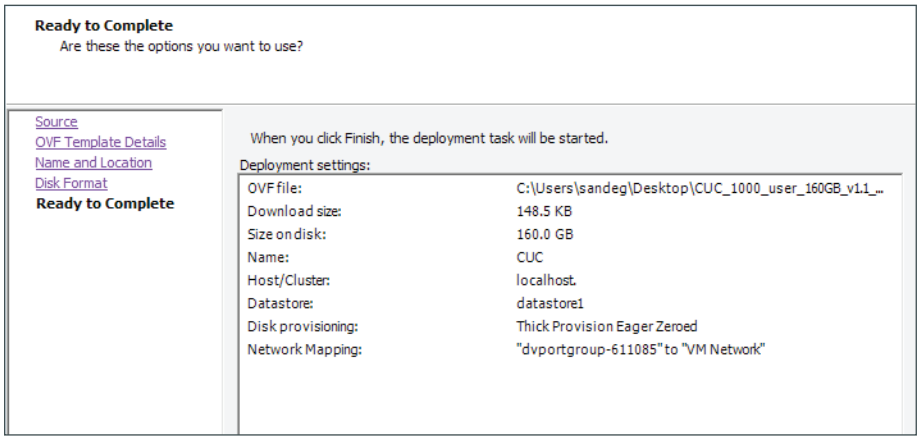
Follow the steps below to deploy an OVA file in order to define the virtual machine (VM) requirements.

Step 1: Open VMware vSphere Client, click on the server hardware you want to use for this install, and then navigate to **File > Deploy OVF Template**.

Step 2: In the Deploy OVF Template wizard, enter the following information:

- On the Source page, next to the Deploy from a file or URL box, click **Browse**, select the Cisco Unity Connection OVA file that you downloaded from Cisco, click **Open**, and then click **Next**.
- On the OVF Template Details page, verify the version information, and then click **Next**:
- On the Name and Location page, in the Name box, enter the virtual machine name **CUC1**. In the **Inventory Location** tree, select the location to deploy the server, and then click **Next**.
- On the Deployment Configuration page, in the Configuration list, select the following option, and then click **Next**:

  1000 users—For 1000 users or fewer.
- On the Storage page, select the destination for the virtual machine files, and then click **Next**.
- On the Disk Format page, choose **Thick Provisioned 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, 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**.

Tech Tip

Cisco Unity Connection shares the same ISO image with Cisco Unified Communications Manager.

Step 6: Select **Datastore ISO File**, click **Browse**, navigate to the location of the Cisco Unity Connection bootable installation file, select the correct ISO image, and then click **OK**.

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

Step 8: Click the **Console** tab. The virtual machine boots and is prepared for installation.

PROCESS

Installing Cisco Unity Connection

1. Install Cisco Unity Connection platform
2. Install licenses and start services

The following information is needed for the installation:

- Time zone for the server
- Host name, IP address, network mask, and default gateway
- DNS 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
- LDAP information for integration with an LDAP server:
    - Manager Distinguished Name (read-access required)
    - User Search Base (for example: the User Search Base in domain cisco.local is cn=users, dc=cisco, dc=local)
    - Host name or IP address and port number for the LDAP server

When users are created in Active Directory, either the telephone number or the IP phone attribute is mandatory. Otherwise, the users cannot be imported into Cisco Unity Connection.

Complete the tasks listed below before you start the installation:

- In DNS, configure the Cisco Unity Connection host name (CUC)
- Obtain license files from the licensing system prior to installing Cisco Unity Connection

Procedure 1 Install Cisco Unity Connection platform

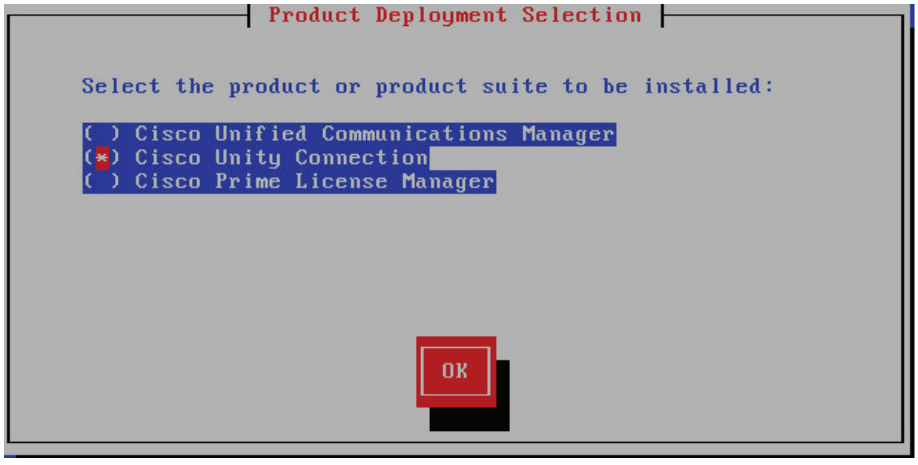
After the ISO/DVD loads, continue the installation on the server console.

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

Step 2: If the media check passes, 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, choose **Cisco Unity Connection**, and then choose **OK**.



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: On the Apply Patch page, choose **No**.

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

Step 8: On the Timezone Configuration page, use the arrow keys to select the correct time zone, and then choose **OK**.

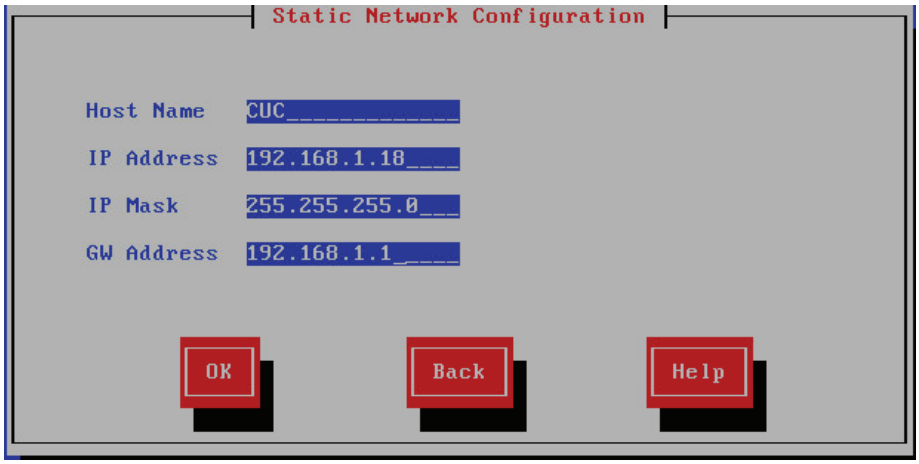
Step 9: On the Auto Negotiation Configuration page, choose **Continue**.

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**:

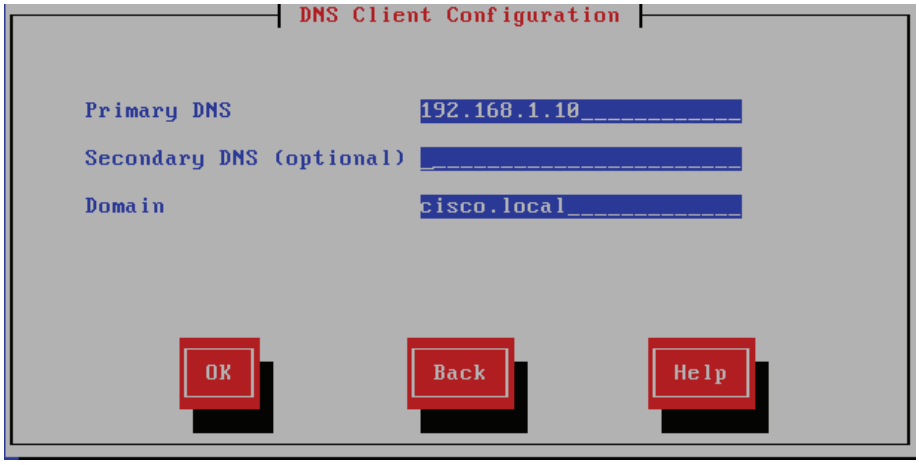
- Host Name–**CUC**
- IP Address–**192.168.1.18**
- IP Mask–**255.255.255.0**
- GW Address–**192.168.1.1**



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

Step 14: Enter the following information, and then choose **OK**:

- Primary DNS–**192.168.1.10**
- 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]**

Tech Tip

The password must start with an alphabetic character and be at least six characters long, and it can contain alphanumeric characters, hyphens, and underscores.

Step 16: On the Certificate Information page, enter the details that will be used to generate the certificate used for secure communications, and then choose **OK**.

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

Step 18: On the Network Time Protocol Client Configuration page, for the NTP host name or IP address, enter **192.168.1.10** , add up to four more NTP host names or IP addresses, and then choose **OK**.

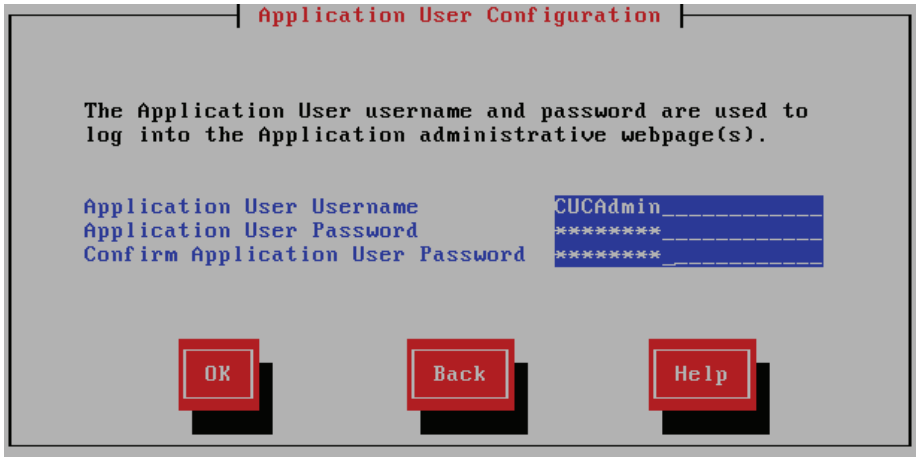
Step 19: On the Security Configuration page, enter a security password, confirm the password, and then choose **OK**.

You use this password in the future if you add another Cisco Unity Connection node.

Step 20: On the SMTP Host Configuration page, choose **No**. You can configure mail notifications at a later stage, if desired.

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

- Application User Username–**CUCAdmin**
- Application User Password–**[password]**
- Confirm Application User Password–**[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 hardware.

After the software has finished loading, 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 Install licenses and start services

After the Unity Connection platform is installed, there are several configuration steps that have to be completed in order to add the licenses and start the services.

Step 1: In a web browser, access the Cisco Unified CM publisher, and in the center of the page, under Installed Applications, click **Cisco Prime License Manager**.

Step 2: On the login page, enter the following case-sensitive Cisco Unified CM application username and password, and then click **Login**:

- User Name—**CUCMAdmin** (case-sensitive)
- Password—**[password]**

Step 3: Navigate to **Inventory > Product Instances**, and then click **Add**.

> **Tech Tip**
>
> The username and password for adding the Product Instances is the case-sensitive platform administrator ID that was entered when installing the server software.

Step 4: Enter the following information for Cisco Unity Connection, and then click **Test Connection**:

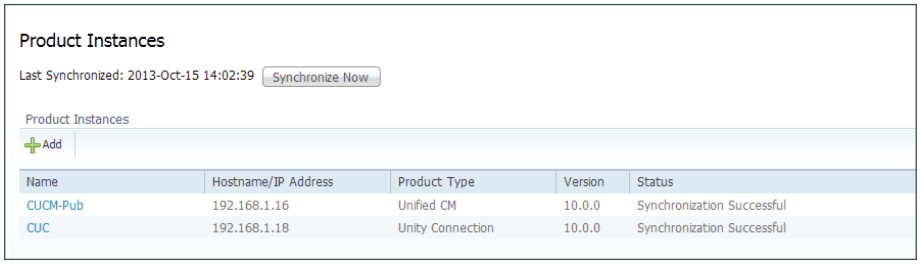
- Name—**CUC**
- Description—**Unity Connection**
- Product Type—**Unity Connection**
- Hostname/IP Address—**192.168.1.18**
- Username—**Admin** (platform administrator ID from Step 15)
- Password—**[password]**

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

Step 6: If the connection is successful, click **OK**.

If the connection is not successful, repeat Step 4 through Step 6 with the correct information.

Step 7: Click **Synchronize Now**.



Step 8: Navigate to **Licenses> Fulfillment** and then select **Other Fulfillment Options > Fulfill Licenses from File**.

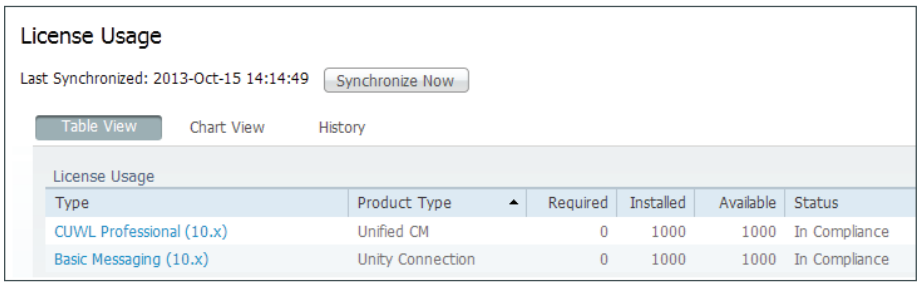
Step 9: On the Install License File page, click **Browse**, locate the directory that contains the license files you obtained prior to installation, select the .bin file, click **Open**, and then click **Install**.

Step 10: Repeat Step 9 for each additional license file for your installation. After all files have been installed, click **Close**.

Next, you verify that the licenses have been properly installed.

Step 11: Navigate to Licenses > **Usage**, and then confirm the status is In Compliance.

If there is a problem, please notify your Cisco representative in order to obtain new license files.



Step 12: In a web browser, access the Cisco Unity Connection server, and then in the center of the page, under Installed Applications, click **Cisco Unity Connection**.

Step 13: Enter the **Username** and **Password** you entered on the Application User Configuration page in Step 21 of the previous procedure, and then click **Login**.

Step 14: In the **Navigation** list, choose **Cisco Unified Serviceability**, and then click **Go**.

Step 15: Navigate to **Tools > Service Activation**, select **Check All Services**, and then click **Save**. In the message window, click **OK**.

Activating services may take a few minutes to complete, so wait for the page to refresh before you continue.

PROCESS

Configuring Cisco Unified CM and Cisco Unity Connection

1. Configure Cisco Unified CM server and site
2. Synchronize the LDAP database
3. Change host names to IP addresses

After all of the Cisco Unified CM and Cisco Unity Connection servers have been installed, start the server configurations using the Cisco Unified Configurator for Collaboration (CUCC) tool, which is available in a Windows and Mac version. The different versions can be downloaded from the following URLs:

- Windows: http://www.cisco.com/go/cvd/collaboration
- Mac: http://www.cisco.com/go/cvd/collaboration

System version 4.0 supports Cisco Unified CM and Cisco Unity Connection versions 8.5, 8.6, 9.0 and 10.0.

The Cisco Unified CM template consists of a series of comma-separated values (CSV) files that contain the base configuration for the cluster. This configuration is modified for your specific environment, based on information entered into the tool.

Please choose the correct number of servers for your installation. Choosing a number that is higher than the installed servers can cause unpredictable results when running the tool.

Procedure 1 Configure Cisco Unified CM server and site

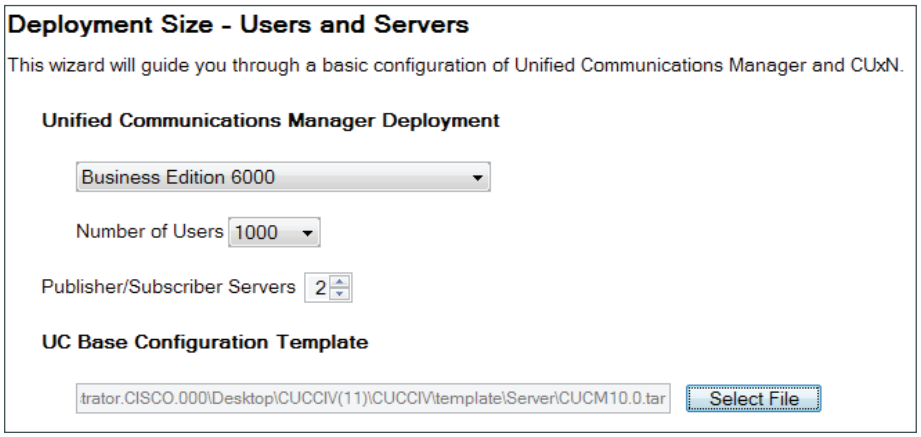
Step 1: Unzip the CUCC software package to a folder on your PC or Mac, change to the directory, and then double-click **CUCC**.

Step 2: Read the Terms of use page and if you agree, click **Accept**.

Step 3: Navigate to **Deploy New Configuration** and enter the following information:

- Business Edition 6000
- Number of users –**1000**
- Publisher/Subscriber Servers –**2**

Step 4: In the Unified CM Template section, click **Select File**, choose the template called **CUCM10.0.tar**, and then click **Next**.



Step 5: On the Server and Site Information page, enter the following information:

- Publisher Node–**CUCM-Pub** (Publisher)
- Subscriber Node–**CUCM-Sub** (Subscriber)
- Check to enable synchronizing users with LDAP–**Selected**
- Check to save all data for future sessions–**Selected**

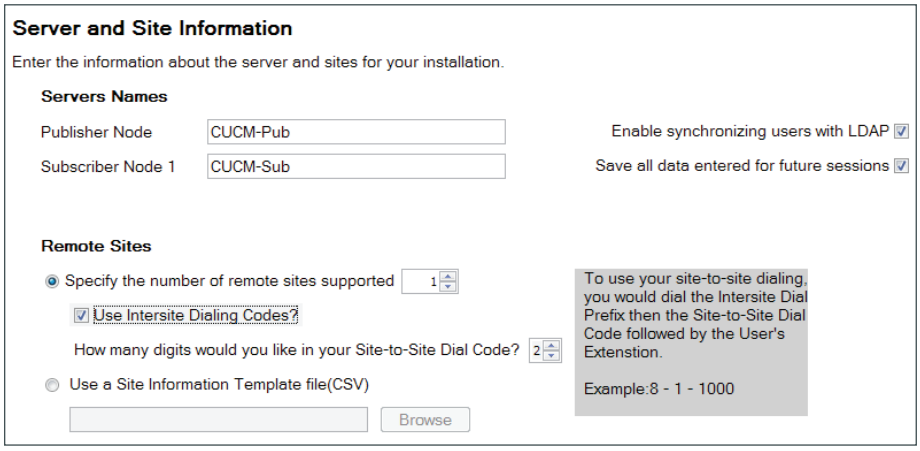
Tech Tip

The server node names that you enter on this page need to be exactly the same (including case) as specified during installation.

Step 6: In the Remotes Sites section, if you do not have a Site Information comma-separated variables (CSV) file, enter the following information, and then click **Next**:

- Specify the number of remote sites supported–**1**
- Use Intersite Dialing Codes–Selected
- Digits for Site-to-Site Dial Code–**2**

If you have your own Site Information CSV file, choose the **Select the Site Information CSV** option button, and then click **Select File**. Choose the .csv file from the **./template/site** directory, click **Open**, and then click **Next**.



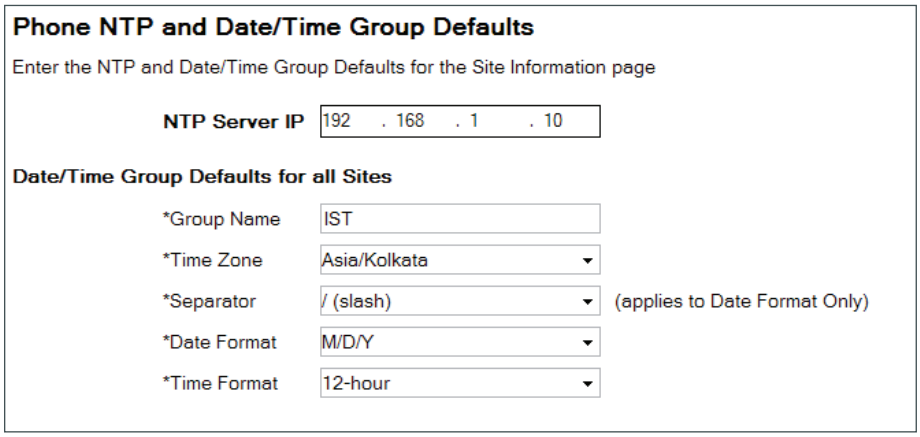
Step 7: On the Phone NTP and Date/Time Group Defaults page, enter the following information, and then click **Next**:

- NTP Server IP Address–**192.168.1.10**
- Group Name–**IST**
- Time Zone–**Asia/Kolkata**
- Separator–**/ (slash)**
- Date Format–**M/D/Y**
- Time Format–**12-hour**

Tech Tip

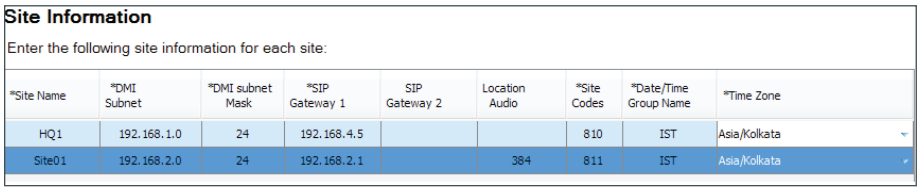
The Date/Time Group Name and Time Zone are used as the default settings for the Site Information page. These values can be modified per site, as required for your installation.

The rest of the fields are the defaults for all Date/Time Groups created by CUCC, but their values cannot be modified on subsequent pages.



Step 8: On the Site Information page, enter the correct information for each corresponding site, and then click **Next**:

- Site Name–**HQ1**
- DMI subnet–**192.168.1.0**
- DMI subnet Mask–**24**
- SIP Gateway 1–**192.168.4.5**
- Location Audio Kbps– (leave blank for HQ, which means unlimited)
- Site Code–**810**
- Date/Time Group Name–**IST**
- Time Zone–**Asia/Kolkata**



Site Information

Enter the following site information for each site:

*Site Name	*DMI Subnet	*DMI subnet Mask	*SIP Gateway 1	SIP Gateway 2	Location Audio	*Site Codes	*Date/Time Group Name	*Time Zone
HQ1	192.168.1.0	24	192.168.4.5			810	IST	Asia/Kolkata
Site01	192.168.2.0	24	192.168.2.1		384	811	IST	Asia/Kolkata

Step 9: In the LDAP System Information section, choose the following options from the lists:

- LDAP Server Type–**Microsoft Active Directory**
- IP Address/Host Name–**192.168.1.10**
- Port–**389**
- Distinguished Name–**Administrator@cisco.local**
- Password–**[password]**
- User Search Base–**cn=users, dc=cisco, dc=local**

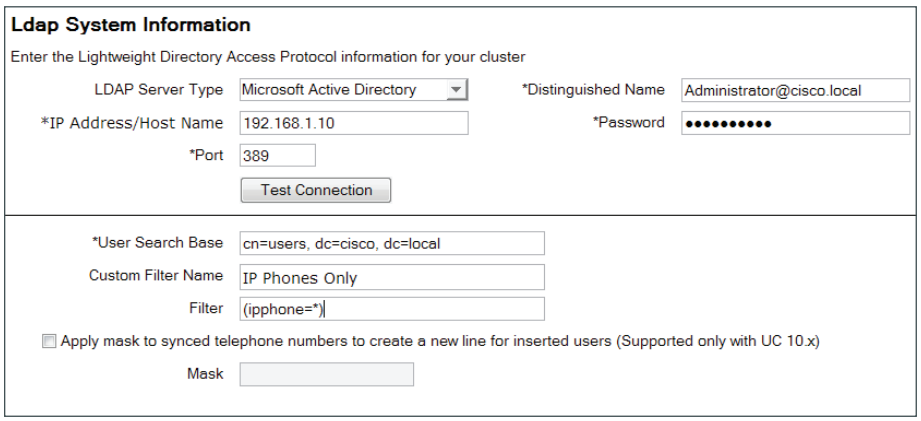
Step 10: If you want to filter the LDAP users, create a custom filter. In the LDAP Custom Filter section, enter the following information:

- Filter Name–**IP Phones Only**
- Filter–**(ipphone=*)**

In this example, an LDAP filter is created that limits the selection of users to the entries that contain information in the ipphone field. If the ipphone field is blank, the user is not synchronized.

- Check the Apply Mask To synced telephone numbers option only if you would like to create a new line for inserted users; do not check this option otherwise.

Step 11: Click **Test Connection.** This verifies connectivity to the LDAP server and confirms the credentials entered are valid. On the Connection Test page, click **OK**



Step 12: If the LDAP server information is correct, click **Next**.

If it is not correct, fix the information, and then repeat Step 11 and Step 12.

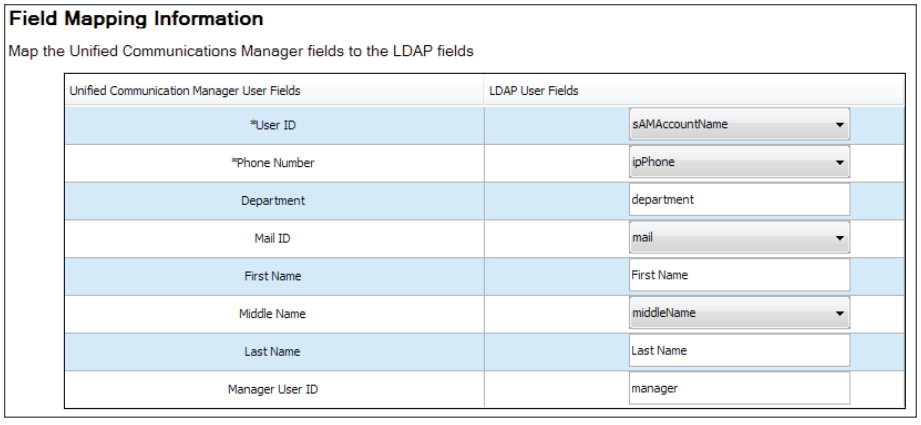
Tech Tip

If configured, the phone number field populates the user's telephone number field in the Cisco Unified CM directory. This field is synchronized from Active Directory from either the ipPhone attribute or the telephoneNumber attribute, whichever is selected.

Typically, the telephoneNumber attribute contains the user's E.164-formatted number and the ipPhone attribute contains the user's extension. It is recommended to use the ipphone attribute, provided that it is configured with the user's correct extension.

Step 13: On the Field Mapping Information page, choose the following options, and then click **Next**:

- Phone Number–**ipPhone**
- Mail ID–**mail**
- Middle Name–**middleName**



Step 14: On the Unified CM Dial-Plan information page choose the Auto-registration option, enter the following information:

- Directory number extension range start–**8000001**
- Directory number extension range end–**8009000**

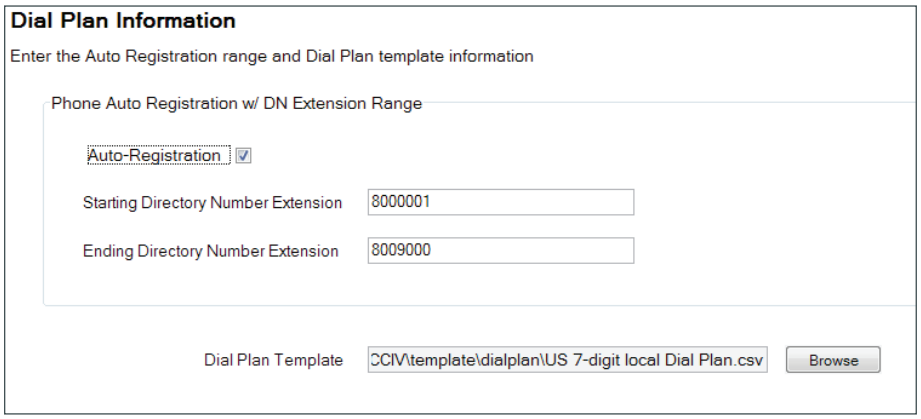
Tech Tip

The Dial Plan templates consist of a set of default route patterns that are used for 7-digit and 10-digit local dialing in the US. Users configured in the system should use Cisco Extension Mobility to log into the auto-registered phones to enable off-net dialing.

Reader Tip

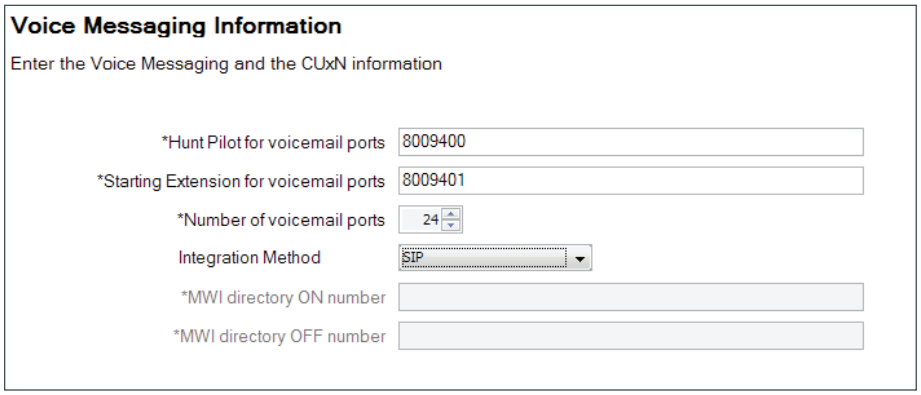
CUCC can be used to deploy the default templates and to create new dial plans or Modify the existing ones.

Step 15: In the Dial Plan Template section, click **Select File**, choose the correct template for your installation, and then click **Next**. For example: **US 7-digit local Dial Plan.csv**.



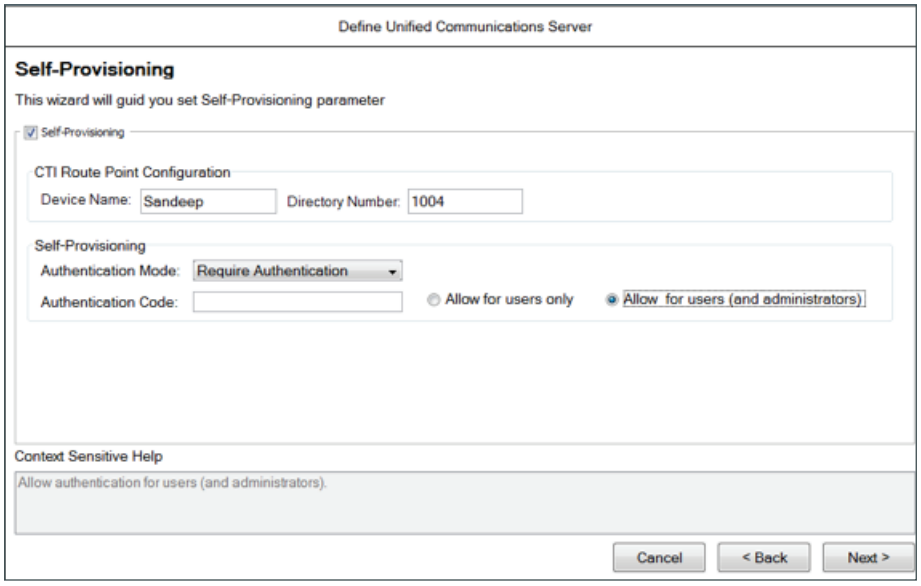
Step 16: On the Voice Messaging Information page, enter the following information, and then click **Next**:

- Hunt Pilot for voicemail ports–**8009400**
- Start of the extension range of voicemail ports–**8009401**
- Number of voicemail ports–**24**
- Integration Method–**SIP**



Step 17: On the Self Provisioning page enter the following information and click **Next**.

- Check mark the box for Self Provisioning
- Device Name–**user1**
- Directory Number–**1004**
- Authentication Mode–**Requires Authentication**
- Authentication Code–**XXXX**
- Select Allow for users (and administrator)



Step 18: The Summary Information page provides a summary of all inputs entered into CUCC up to this point. If the information shown is correct, click **Next**.

If any of the information shown is incorrect, click **Back**, and then correct it.

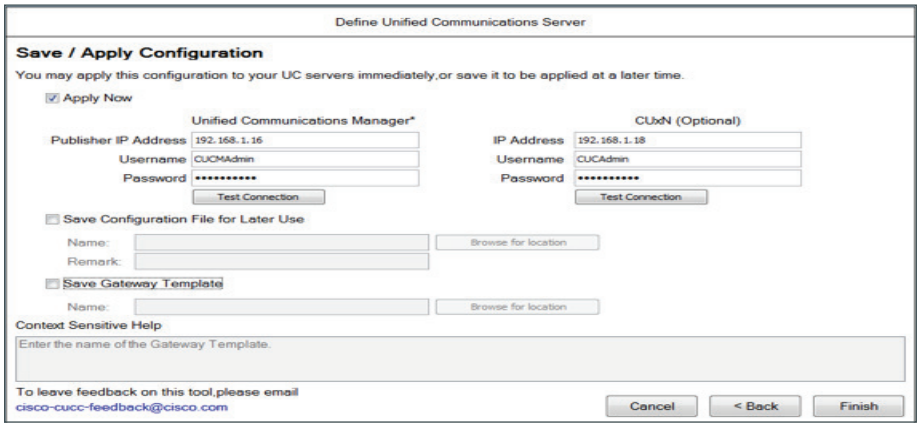
Step 19: On the Save / Apply Configuration page, if you want to update the Cisco Unified CM publisher in real-time, enter the following information:

- IP Address/Host Name–**192.168.1.16 (publisher)**
- User Name–**CUCMAdmin**
- Password–**[password]**

Step 20: On the Save/Apply Configuration Page if you want to update the Cisco Unity Connection in real-time, enter the following information:

- IP Address/Host Name–192.168.1.18
- User Name–CUCAdmin
- Password –[password]

Step 21: Click **Test Connection**. This verifies connectivity to the Cisco Unified CM server and confirms the credentials entered are valid. On the Connection Test page, click **OK**.



Step 22: If you want to save the configuration file for later use, select **Save Configuration File for Later Use**, enter a remark, and save the file.

Tech Tip

You can use the saved package file at a later time to update a Cisco Unified CM server with the **Modify or Re-Deploy Configuration** option of CUCC.

Step 23: If you want to create a gateway template for each voice gateway entered on the Site Information page, select **Gateway Template**, and then click **Save As**.

On the Save dialog box, accept the default directory name or navigate to a new directory of your own choosing, and then click **Save**.

Tech Tip

The gateway template default directory is .\packet\gateway and they have a standard naming format of: SIP_[Site_Name]_GWY.txt. The files are generated with the site-specific information known to CUCC. However, they do not include the hardware and carrier-specific details about your individual voice gateway routers.

The template files are modified with your specific information and then copied into your voice gateway routers when following the procedures and steps in the "Configuring Conference Bridges, PSTN, Dial Peers, and SRST" process later in this guide.

Step 24: After choosing your configuration method from the options listed in the previous steps, click **Configure**.

Step 25: Select **Apply Now**, and then click **Finish**

Wait for the update to complete before proceeding.

CUCC updates approximately 2.5 sites and 5 gateways per minute. This means an installation with 50 sites and 100 gateways takes twenty minutes.

Procedure 2 Synchronize the LDAP database

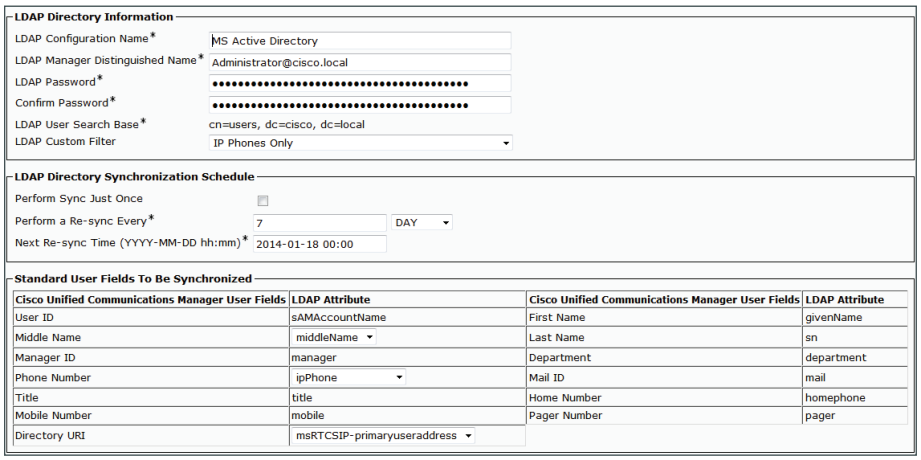
If you have chosen to update the Cisco Unified CM server and you are using LDAP, you must manually synchronize the LDAP database and perform several additional steps before the first phase of CUCC is complete.

If you are not using LDAP, skip to Procedure 3 "Change host names to IP addresses."

Step 1: From the Cisco Unified CM administration page, navigate to **System > LDAP > LDAP Directory**, and then click **Find**.

Step 2: Click the name of LDAP directory that you created with CUCC (Example: MS Active Directory).

Step 3: Click **Perform Full Sync Now**, and then on the dialog box that appears, click **OK**. The user import process begins.



LDAP Directory Information

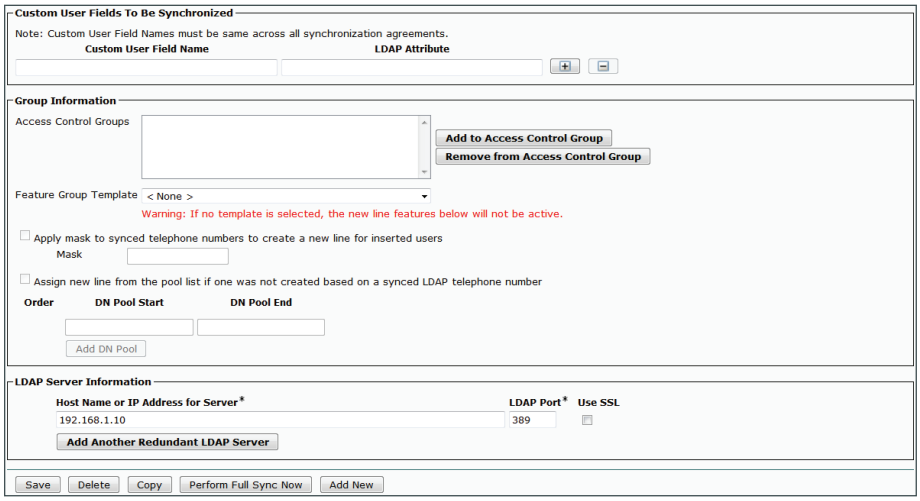
LDAP Configuration Name*	MS Active Directory
LDAP Manager Distinguished Name*	Administrator@cisco.local
LDAP Password*	••
Confirm Password*	••
LDAP User Search Base*	cn=users, dc=cisco, dc=local
LDAP Custom Filter	IP Phones Only

LDAP Directory Synchronization Schedule

Perform Sync Just Once	
Perform a Re-sync Every*	7 DAY
Next Re-sync Time (YYYY-MM-DD hh:mm)*	2014-01-18 00:00

Standard User Fields To Be Synchronized

Cisco Unified Communications Manager User Fields	LDAP Attribute	Cisco Unified Communications Manager User Fields	LDAP Attribute
User ID	sAMAccountName	First Name	givenName
Middle Name	middleName	Last Name	sn
Manager ID	manager	Department	department
Phone Number	ipPhone	Mail ID	mail
Title	title	Home Number	homephone
Mobile Number	mobile	Pager Number	pager
Directory URI	msRTCSIP-primaryuseraddress		



The Cisco Unified CM synchronization LDAP process reads approximately 200 users per minute. This means an installation with 1,000 users takes five minutes to complete.

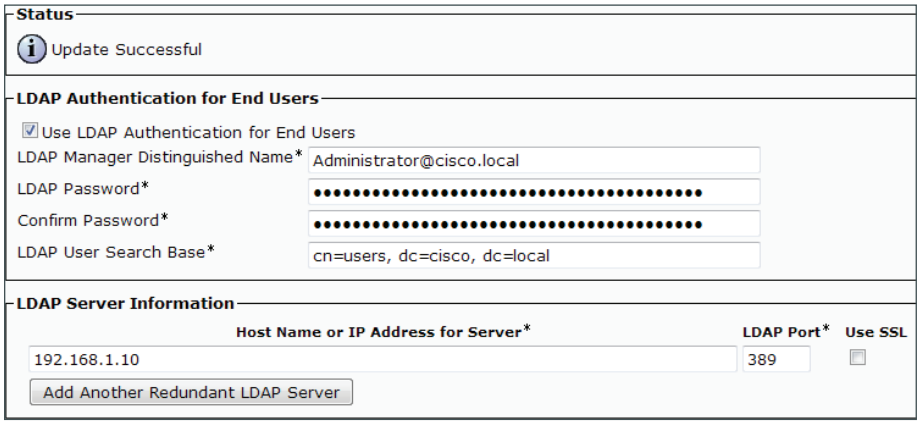
Please wait until the LDAP synchronization completes before continuing.

Step 4: To confirm the users have been synchronized, navigate to **User Management > End User**, and then click **Find**.

Verify the number of users equals the number you expect. If not, please repeat this step until the remaining users have been synchronized before continuing.

Step 5: Navigate to **System > LDAP > LDAP Authentication**, enter the following information, and then click **Save**:

- LDAP Password–**[password]**
- Confirm Password–**[password]**



Tech Tip

LDAP authentication is used for features such as Extension Mobility in order to validate the user credentials with the LDAP database.

Step 6: In the Status section, verify that the message "Update successful" appears. If not, enter the correct information on this page until the update is successful.

Procedure 3 Change host names to IP addresses

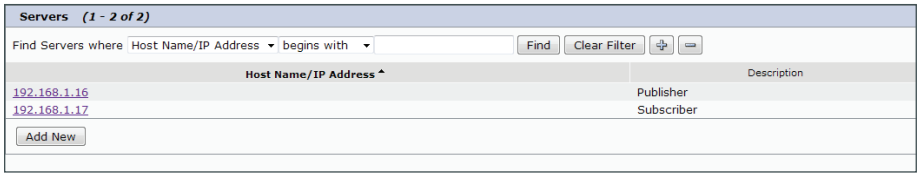
The next set of steps changes the Cisco Unified CM publisher, subscriber, and TFTP server host names to IP addresses, which removes the dependency on DNS for day-to-day operation of the phones.

Step 1: Navigate to **System > Server**, and then click **Find**.

Step 2: Select **CUCM-Pub**, change the **Host Name/IP Address** to **CUCM-Pub.cisco.local** and the **Description** to **Publisher**, click **Save**, and on the dialog box that appears, click **OK**.

Step 3: In the **Related Links** list, choose **Back to Find/List**, and then click **Go**.

Step 4: Select **CUCM-Sub**, change the **Host Name/IP Address** to **CUCM-Pub.cisco.local** and the **Description** to **Subscriber**, click **Save**, and on the dialog box that appears, click **OK**.



Step 5: Return to the CUCC program, click **Continue**, and then click **Finish**.

This completes the first phase of the CUCC program.

PROCESS

Configuring Users, Device Profiles, and IP Phones

1. Configure user and device profiles
2. Deploy IP phones

After the Cisco Unified CM and Cisco Unity Connection servers are configured, the next set of steps updates the users with Unified CM specific information and creates their user device profiles for extension mobility. Since the users have already been synchronized with LDAP, you will use the Modify section of the CUCC tool in order to update their information.

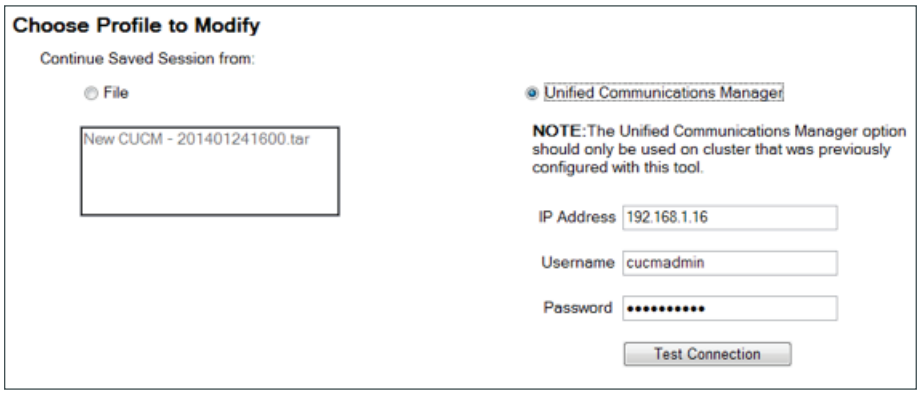
After updating the users and device profiles, the IP phones must have extension mobility enabled. They will also be updated with the correct home device pool and calling search space for their specific location. To log in to the phone, the users will enter their LDAP User ID and the default PIN of **112233**

Procedure 1 Configure user and device profiles

Step 1: On the CUCC main page, click **Modify User and Device Profiles**.

Step 2: On the Choose Profile to modify page, Choose Unified Communications Manager, enter the following information click the Test Connection, if the connection is successful, click **Next**.

- IP Address–**192.168.1.16**
- Username–**CUCMAdmin**
- Password–**[password]**

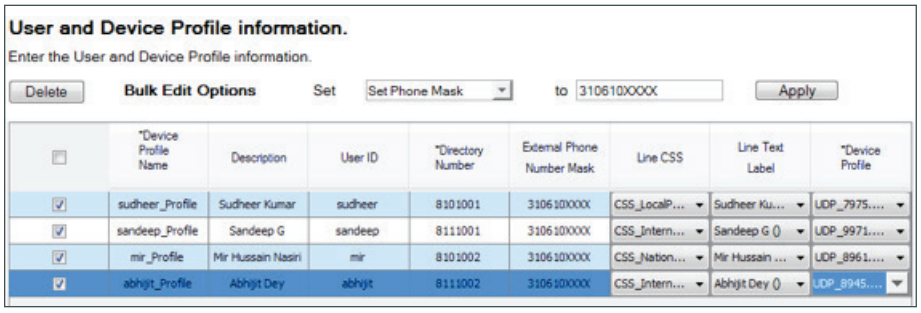


Step 3: For each user device profile, populate the **Directory Number, External Phone Number Mask, Line CSS, Line Text Label** and **Device Profile** fields as follows, and then click **Next**:

- **Directory Number**–This is the number that was synchronized from the ipPhone field in the LDAP directory. (Required)
- **External Phone Number Mask**–This value is used to create the direct inward-dialing number for the user or a main office number. This also appears on the black stripe at the top of the IP phone's display. Enter the phone number mask (for example, 311611XXXX) into the text box at the top of the column, and then click **Set Phone Mask.**
- **Line CSS**–This defines the class of restriction, or type of numbers, the user is allowed to call. The calling search spaces (CSS) defined during the import process is viewed in Cisco Unified CM Administration, under **Call Routing > Class of Control > Calling Search Space**. In the list at the top of the column, select the **Line CSS**, and then click **Set Line CSS**.
- **Line Text Label**–This is the label that is displayed on the phone. Although any alphanumeric string is allowed, it is recommended that you use **FirstName, LastName**. In the list at the top of the column, select a text label format option, and then click **Set Line Text**.
- **Device Profile**–This is the device profile associated with the user device profile. In the list at the top of the column, select the device profile, and then click **Set Device Profile**. (Required)

Tech Tip

Bulk Edit Options allows you to configure the Line CSS, Line Text Label, Device Profiles and External Phone number mask to all the users in the list.



Step 4: Some user IDs that were exported may not need user device profiles. If you want to remove them from the list, select those **User IDs**, and then click **Delete button**.

Step 5: In the Save/Apply Configuration page for Unified Communications Manager, enter the following information for Unified Communications Manager

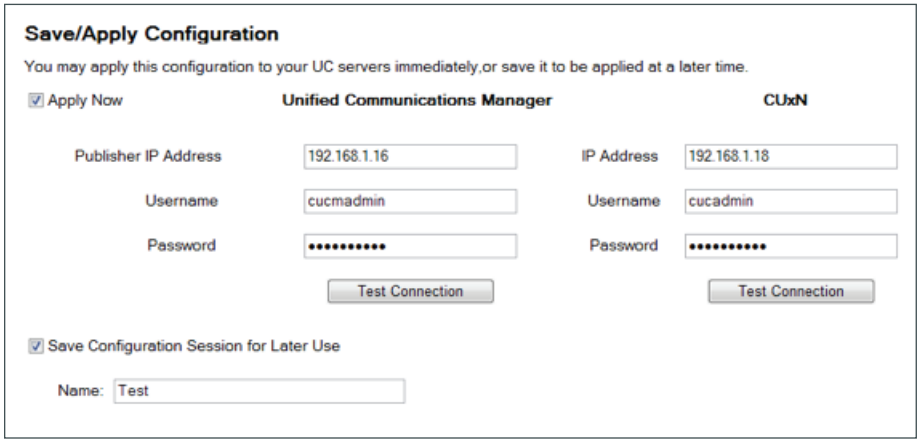
- IP Address–**192.168.1.16 (publisher)**
- Username–**cucmadmin**
- Password–**[password]**

Step 6: On the Save/apply Configuration Page for CUxN (Unity Connection), enter the following information:

- IP Address–**192.168.1.18**
- Username–**cucadmin**
- Password–**[password]**

Step 7: Click Te**st Connection for both Unified Communication Manager and Unity Connection**. This verifies connectivity to the Cisco Unified CM server and Unity Connection and confirms the credentials entered are valid click **OK**.

Step 8: If you want to Save Configuration for later use, choose Save Configuration for Later Use option and then provide the Name.



Step 9: If the test is successful, click **Finish**

If the test is not successful, repeat Step 3 with the correct information.

After CUCC is done reading the user information from Cisco Unified CM, the first five users are displayed. The first three columns are auto-generated from the source data, and the information they contain cannot be changed.

The tool displays its progress on the Update Information page and a log file called modify_user.log with date/time stamps is created in the .\log directory.

CUCC updates approximately 850 users per hour. This means an installation with 1000 users will take seventy minutes to complete.

This completes the second phase of the CUCC program.

Procedure 2 Deploy IP phones

This procedure enables extension mobility on the list of phones. It also updates the phones with the proper home device pool and default calling search space, based on their IP address in the network. The home device pool defines the Cisco Unified Communications Manager redundancy group, local route group, region, media resource group list, location, SRST reference, and physical location for each phone.

Within the network services layer, DHCP option 150 instructs the IP phones to connect to the Cisco Unified CM TFTP server for its initial configuration file and to auto-register with the default pair of Unified CM subscriber servers. Do not proceed with this procedure until all IP phones have registered.

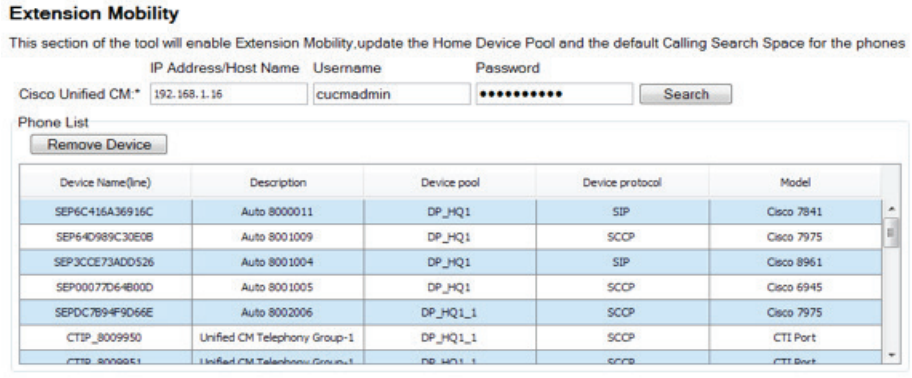
Step 1: Connect the IP phones to the network so they begin the automatic registration process. Depending on the size of your installation and the number of remote sites, this can take several hours to complete.

Please wait for the phones to register before continuing.

Step 2: From the CUCC main page, navigate to **Update Endpoint with Extension Mobility**, enter the following information, and then click **Search**:

- IP Address/Host Name–**192.168.1.16 (publisher)**
- Username–**cucmadmin**
- Password–**[password]**

Step 3: If there are any phones that do not need to be updated, select them, and then click **Remove Device**.



Step 4: After removing the unwanted phones, click **Configure**.

Step 5: In the message window, click **Yes**.

CUCC displays its progress in a blue message window and a log file called phone.log with date/time stamps is created in the .\log directory.

CUCC updates and restarts approximately 30 phones a minute. This means an installation with 1000 phones will take thirty-five minutes.

Wait for the phone configuration to complete before continuing.

Step 6: In the message window at the end of the configuration step, click **OK**.

Step 7: Exit out of the CUCC program by clicking the **X** on the right side of the title bar. On the "Do you really want to quit" message, click **Yes**.

This completes the third phase of the CUCC program. Allow several minutes for the remaining phones to finish restarting with the Cisco Unified CM cluster.

After the users and IP phones are updated in Cisco Unified CM, the configuration of the gateways, conference bridges, public switched telephone network (PSTN) interfaces and Survivable Remote Site Telephony (SRST) services can begin.

PROCESS

Configuring Conference Bridges and SRST

1. Configure conference bridges
2. Configure SRST for SCCP phones
3. Configure SRST for SIP phones
4. Block voice traffic on WAN links

The procedures in this process are required for all voice routers.

If you chose to create the gateway templates in the first phase of the CUCC tool, the files must be modified for your hardware interfaces, server IP address and carrier parameters before you copy them into the voice gateway routers. Unless the location was changed by the user, the individual gateway files are located in the **.\packet\ gateway directory** using a naming format of: **SIP_[Site_Name]_GWY.txt**. Please follow the steps in this process to understand what site-specific information is required in each section of the gateway template files.

Procedure 1 Configure conference bridges

All routers need a minimum of a packet voice digital signal processor (DSP) module (PVDM3-64) in order to create five 8-party conference bridge resources along with the DSPs needed for voice gateway services. If your organization needs more gateway or conference resources, you will need additional DSPs. The router requires additional DSPs and configuration if hardware-based transcoding is needed. By default, calls to Cisco Unity Connection are transcoded in the server.

The router at the main site can provide unified communications gateway functions. Therefore, it should be configured with sufficient DSPs and a T1/E1 voice/WAN interface card (VWIC) for the PSTN primary rate interface (PRI) configurations.

The Cisco 3945 and 3925 Integrated Services Routers with voice security (VSEC) ship with a PVDM3-64, so they have enough DSPs to handle one voice T1 and five 8-party conferences. If the remote site uses E1, they will have enough DSPs for only four 8-party conferences. The Cisco 2911 Integrated Services Router (ISR) with VSEC ships with a PVDM3-16, and the 2921 ISR with VSEC and 2951 ISR with VSEC ship with a PVDM3-32. The Cisco 2900 Series ISRs have to be upgraded to a single PVDM3-64 DSP in order to allow sufficient resources for a single voice T1 and at least five 8-party conferences.

Apply the following configuration in the HQ router in order to register the five conference-bridge resources as the highest priority on the primary subscriber and as the second priority on the backup subscriber. The same configuration is used in the remote-site routers if conferencing resources are needed.

Tech Tip

The IOS commands are listed under the **Conference Bridge** section in the template file for each voice gateway.

The hardware and IP address-specific information in square brackets must be modified in the gateway template file before the commands can be successfully copied into the router. Use the examples in this section to help you understand what is needed in each area of the configuration.

Step 1: Configure the DSP services on the voice card.

```
voice-card 0
  dspfarm
  dsp services dspfarm
```

Step 2: Configure the dspfarm profile for a conference bridge with a maximum of **5** sessions and a list of the acceptable codecs.

```
dspfarm profile 1 conference
  description HQ Conference Bridges
  codec g711ulaw
  codec g711alaw
  codec g729ar8
  codec g729abr8
  codec g729r8
  codec g729br8
  codec g722-64
  codec ilbc
  maximum sessions 5
  associate application SCCP
  no shutdown
```

Step 3: Configure which interface is used to register to the Cisco Unified CM. If you are adding voice configuration to an existing router, use the Loopback 0 interface.

```
ccm-manager sccp local loopback 0
```

If you are using a standalone voice router, use the interface connecting to the LAN.

```
ccm-manager sccp local [interface type][number]
```

Step 4: Configure the SCCP gateway interface to connect to the Cisco Unified CM servers used for subscription. If a large number of conference bridges are implemented, the priority of the subscriptions should be balanced appropriately by alternating the IP addresses of the Unified CM subscribers in the cluster. Set the version to 7.0 and above.

```
sccp local [interface type][number]
sccp ccm 192.168.1.17 identifier 1 priority 1 version 7.0
sccp ccm 192.168.1.16 identifier 2 priority 2 version 7.0
sccp
```

Step 5: Bind the interface for the conference bridge to the one used by the SCCP applications. Group the servers created in Step 4 and associate them with the profile for the conference bridge. Again if a large number of conference bridges are implemented, the priority should be balanced appropriately. Register the conference bridge with Cisco Unified CM, set the switchback method to graceful, and then wait 60 seconds.

```
sccp ccm group 1
  bind interface [interface type][number]
  associate ccm 1 priority 1
  associate ccm 2 priority 2
  associate profile 1 register CFB1HQ1
  switchback method graceful
  switchback interval 60
```

Tech Tip

The Cisco Unified CM configuration for the conference bridge was completed with CUCC, so the registration name must match the name uploaded into the cluster by the tool. The names are always CFB1<*Site Name*> and CFB2<*Site name*>, if there are two. For example, if the headquarters site is HQ1, the conference bridge names are CFB1HQ1 and CFB2HQ1.

Procedure 2 Configure SRST for SCCP phones

The procedure configures SRST for SCCP phones. If you do not have SCCP phones at remote sites, please skip this section.

If sites codes are used for this installation, the **dialplan-pattern** command transforms the 10-digit E164 PSTN number into the unique 7-digit directory number on the phone. The **extension-length** and **extension-pattern** keywords allow you to identify the last four digits of the E164 number. You create additional dial peers in order to maintain 7-digit dialing between sites with site codes.

The dial plan consists of the following:

- One digit as an inter-site access code
- Two digits for the site code to accommodate up to 90 sites
- Four digits for the site extension

The format is 8 + SS + XXXX, where 8 is the on-net access code, SS is a 2-digit site code from 10-99, and XXXX is a 4-digit extension number, giving a total of seven digits.

To allow the users to maintain 4-digit dialing between the phones at each remote site, a voice translation rule and profile are associated with incoming calls. The voice translation profile is only active when the phones are in SRST mode.

If sites codes are not used for this installation, the **dialplan-pattern** command transforms the 10-digit E164 PSTN number into the unique 4-digit directory number on the phone. The **extension-length** and **extension-pattern** keywords allow you to identify the last four digits of the E164 number. Voice translation rules and profiles are not needed for installations that do not use site codes.

Tech Tip

The IOS commands are listed under the **SRST voice translation commands** section in the template file for each voice gateway. These commands are only needed if site codes are used in your installation.

Step 1: If site codes are used, create a voice translation rule and a voice translation profile in the global area of the router. The first part of the translation rule—between the first set of forward slashes—matches a 4-digit number that starts with a 1 through 7. The second part of the rule—between the second set of forward slashes—prepends the unique site code to the 4-digit dialed number. The translation-profile called SRST-4-Digit applies the translation rule to the number called by the user. The example given is for 7-digit directory numbers starting with 811.

```
voice translation-rule 1
rule 1 /^[1-7]...$/ /811\0/
voice translation-profile SRST-4-Digit
translate called 1

voice translation-rule 800
 rule 2 /^800\(.*)//1310610\1/

voice translation-profile SRST-7-Digit
 translate called 800
```

Tech Tip

The IOS commands are listed under the **SRST for SCCP** section in the template file for each voice gateway.

The carrier and SRST license-specific information in square brackets must be modified in the gateway template file before the commands can be successfully copied into the router. Use the examples in this section to help you understand what is needed in each area of the configuration.

Step 2: Assign the SRST interface to the source address of the router closest to the phones using the default SCCP port of 2000. Allow 50 phones to register, and use dual-line support to allow transfers and conferencing. These are the four basic commands to enable SCCP SRST.

If you are integrating SRST features into a preexisting router, use the IP address of the gateway's Loopback 0 interface.

```
call-manager-fallback
  ip source-address 192.168.2.1 port 2000
  max-ephones 50
  max-dn 35 dual-line
```

Tech Tip

When the command **max-ephones 50** is executed, a license agreement appears. To activate this feature, you must accept the agreement. Be aware of this when copy and pasting or scripting the deployment of these features, as configuration cannot continue until this agreement is accepted.

Step 3: Enhance the user experience in SCCP fallback mode by adding a secondary dial tone when the number 9 is pressed, and then allow the user to perform a supervised transfer (full consultation). Configure eight 3-way conference calls for ad hoc conferencing.

```
secondary-dialtone 9
transfer-system full-consult
max-conferences 8 gain -6
```

Step 4: If site codes are used for this installation, translate the inbound number to the directory number for the phone. When a call arrives from the PSTN carrier, the call is directed to the correct phone, based on the access code, site code, and the last four digits. Apply the translation profile for incoming calls when phones are in SRST mode. The example given is for 2-digit site codes, 7-digit directory numbers, and 10-digit inbound numbers from the PSTN.

```
dialplan-pattern 1 311611.... extension-length 7 extension-pattern 811....
translation-profile incoming SRST-4-Digit
```

If site codes are not used for this installation, configure the translated number to match the 4-digit directory number for the phone. When a call arrives from the PSTN carrier, the call is directed to the correct phone, based on the last four digits. The example given is for 4-digit directory numbers and 10-digit inbound numbers from the PSTN.

```
dialplan-pattern 1 311611.... extension-length 4 extension-pattern ....
```

Step 5: If site codes are used for this installation, add IOS POTS dial peers in order to maintain dialing between sites in SRST mode. The examples given are for 2-digit site codes, 7-digit directory numbers, and 11-digit outbound PSTN numbers.

Example: Headquarters Site

```
dial-peer voice 810 voip
 description 7-DIGIT DIAL to HQ in SRST
 translation-profile outgoing SRST-7-Digit
 destination-pattern 810....
 session protocol sipv2
 session target ipv4:192.168.8.26
 dtmf-relay rtp-nte
 codec g711ulaw
 no vad
```

Repeat this step for each additional remote site. Use an appropriate dial-peer number, description, destination pattern, and prefix.

Procedure 3 Configure SRST for SIP phones

The procedure will configure SRST for SIP phones. If you are not using SIP phones at remote sites, please skip this section.

If sites codes are used for this installation, the **dialplan-pattern** command transforms the 10-digit E164 PSTN number into the unique 7-digit directory number on the phone. The **extension-length** and **extension-pattern** keywords allow you to identify the last four digits of the E164 number. You create additional dial peers in order to maintain 7-digit dialing between sites with site codes.

For networks with 90 sites or less, the dial plan consists of the following:

- One digit as an inter-site access code
- Two digits for the site code to accommodate up to 90 sites
- Four digits for the site extension

The format is 8 + SS + XXXX, where 8 is the on-net access code, SS is a 2-digit site code from 10-99, and XXXX is a 4-digit extension number, giving a total of seven digits.

To allow the users to maintain 4-digit dialing between the phones at each remote site, a voice translation rule and profile are associated with incoming calls. The voice translation profile is only active when the phones are in SRST mode.

If sites codes are not used for this installation, the **dialplan-pattern** command transforms the 10-digit E164 PSTN number into the unique 4-digit directory number on the phone. The **extension-length** and **extension-pattern** keywords allow you to identify the last four digits of the E164 number. Voice translation rules and profiles are not needed for installations that do not use site codes.

Tech Tip

The IOS commands are listed under the **SRST voice translation commands** section in the template file for each voice gateway. These commands are only needed if site codes are used in your installation.

Step 1: If site codes are used, create a voice translation rule and a voice translation profile in the global area of the router. The first part of the translation rule—between the first set of forward slashes—matches a 4-digit number that starts with a 1 through 7. The second part of the rule—between the second set of forward slashes—prepends the unique site code to the 4-digit dialed number. The translation-profile called SRST-4-Digit applies the translation rule to the number called by the user. The example given is for 7-digit directory numbers starting with 820.

```
voice translation-rule 1
rule 1 /^[1-7]...$/ /811\0/
voice translation-profile SRST-4-Digit
translate called 1

voice translation-rule 800
 rule 2 /^800\(.*)//1310610\1/

voice translation-profile SRST-7-Digit
 translate called 800
```

Tech Tip

The IOS commands are listed under the **SRST** section in the template file for each voice gateway.

The carrier, IP address and SRST license-specific information in square brackets must be modified in the gateway template file before the commands can be successfully copied into the router. Use the examples in this section to help you understand what is needed in each area of the configuration.

Step 2: Create the SIP back-to-back user agent and SIP registrar functionality. Change the SIP registrar expiration timer to 600 seconds.

```
voice service voip
 allow-connections sip to sip
 sip
  registrar server expires max 600 min 60
```

Step 3: Assign the following characteristics to SIP phones globally: the system message on the bottom of certain phones, the maximum directory numbers, and the maximum number of pools allowed on the SRST router.

```
voice register global
 system message "SIP SRST Service"
 max-dn 200
 max-pool 50
```

Tech Tip

When the command **max-pool 50** is executed, a license agreement appears. To activate this feature, you must accept the agreement. Be aware of this when copy and pasting or scripting the deployment of these features, as configuration cannot continue until this agreement is accepted.

Step 4: If 2-digit site codes are used for this installation, translate the inbound number to the 7-digit directory number for the phone. When a 10-digit call arrives from the PSTN carrier, the call is directed to the correct phone, based on the access code, 2-digit site code, and the last four digits. This configuration is done under call-manager-fallback

```
call-manager-fallback
 dialplan-pattern 1 311611.... extension-length 7
 extension-pattern 811....
```

If site codes are not used for this installation, configure the translated number to match the 4-digit directory number for the phone. When a 10-digit call arrives from the PSTN carrier, the call is directed to the correct phone, based on the last four digits.

```
call-manager-fallback
  dialplan-pattern 1 311611.... extension-length 4 extension-pattern
  ....
```

Step 5: If site codes are used for this installation, add IOS POTS dial peers in order to maintain dialing between sites in SRST mode. The examples given are for the access code, 2-digit site codes, 7-digit directory numbers, and 10-digit outbound PSTN numbers.

Example: Headquarters Site

```
dial-peer voice 810 voip
 description 7-DIGIT DIAL to HQ in SRST
 translation-profile outgoing SRST-7-Digit
 destination-pattern 810....
 session protocol sipv2
 session target ipv4:192.168.8.26
 dtmf-relay rtp-nte
 codec g711ulaw
 no vad
```

Repeat this step for each additional remote site. Use an appropriate dial-peer number, description, destination pattern, and prefix.

Step 6: Configure the voice register pool for the defined IP address range. If your IP address ranges are not contiguous, you may create multiple pools. The id network is the IP subnet for the voice VLAN. Create a voice pool for each voice subnet implemented at the remote site. In this example, we are using two voice subnets. Use **rtp-nte sip-notify** for the **dtmf-relay** parameter, and use the G711 ulaw codec for all calls.

```
voice register pool  1
 id network 192.168.2.1 mask 255.255.255.0
 dtmf-relay rtp-nte sip-notify
 codec g711ulaw
```

Step 7: Identify the IP address of the Cisco Unified CM subscriber 1 and subscriber 2 as the external registrars, using the default expiration of 3600 seconds that is defined in the cluster.

```
sip-ua
 registrar ipv4:192.168.1.16 expires 3600
 registrar ipv4:192.168.1.17 expires 3600 secondary
```

Procedure 4 Block voice traffic on WAN links

(Optional)

In some cases, an administrator may want to force IP phones into SRST mode when a failover to a backup WAN link occurs. Implementing this blocking avoids transmitting voice over a lossy link, and it decreases the cost of a failure by reducing data usage while maintaining the dial tone that end-users expect. This configuration can be applied to the backup router of a dual router design or to the secondary link of a single router design. This configuration can also be used on any WAN interface when centralized voice registrations are not wanted at a particular remote site.

Tech Tip

The IOS commands are listed under the **Optional - Block Voice on WAN** section in the template file for each voice gateway.

The hardware-specific information in square brackets must be modified in the gateway template file before the commands can be successfully copied into the router. Use the examples in this section to help you understand what is needed in each area of the configuration.

Step 1: Configure the access list that blocks SIP: 5060 (TCP/UDP), Secure SIP: 5061 (TCP/UDP), SCCP: 2000 (TCP), Secure SCCP: 2443 (TCP), standard RTP ports: 16384-32767 (UDP), and allow all other traffic.

```
ip access-list extended ACL-VOIP-CONTROL
 deny tcp any any eq 5060
 deny udp any any eq 5060
 deny tcp any any eq 5061
 deny udp any any eq 5061
 deny tcp any any eq 2000
 deny tcp any any eq 2443
 deny udp any any range 16384 32767
 permit ip any any
```

Step 2: Apply the access control list to the WAN interface to which the administrator wishes to block voice traffic.

```
interface Tunnel10
 ip access-group ACL-VOIP-CONTROL in
 ip access-group ACL-VOIP-CONTROL out
```

The Cisco Unified CM system installation is now complete.

PROCESS

Configuring Extend and Connect

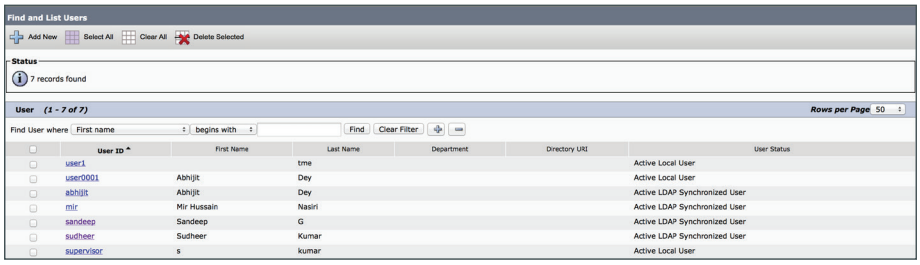
1. Configure the extend and connect
2. Using Jabber for Extend and Connect

The procedures below are required to enable extend and connect for the users.

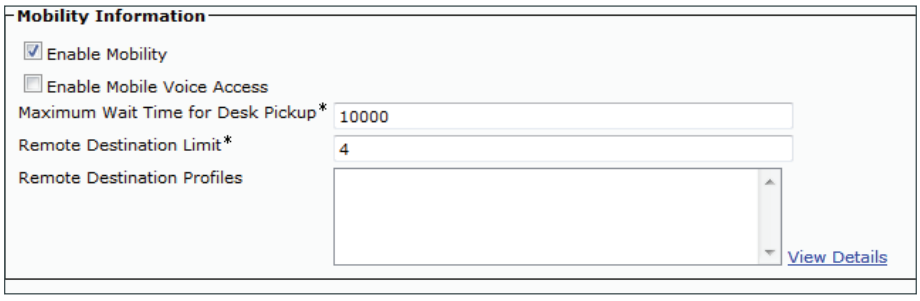
Procedure 1 Configure the extend and connect

This procedure configures the extend and connect for the users.

Step 1: For a new or existing user in Unified CM, enable user mobility to provision CTI remote devices. On the Unified CM administration page, select User Management and click Add New for a new user or click Find to find the existing user.

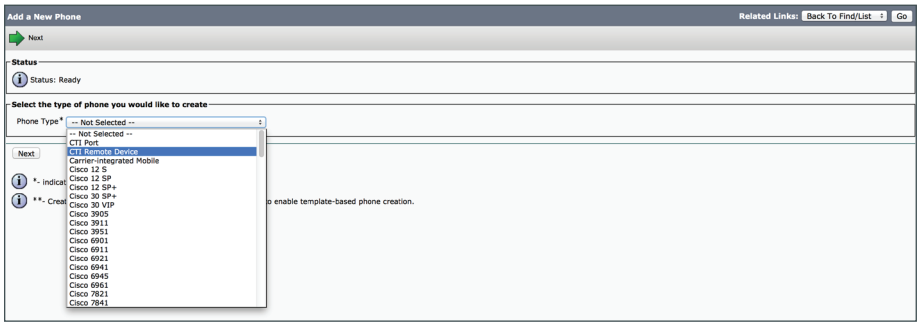


Step 2: On the End User Configuration page of unified CM administration, scroll to Mobility Information section and check the Enable Mobility Checkbox



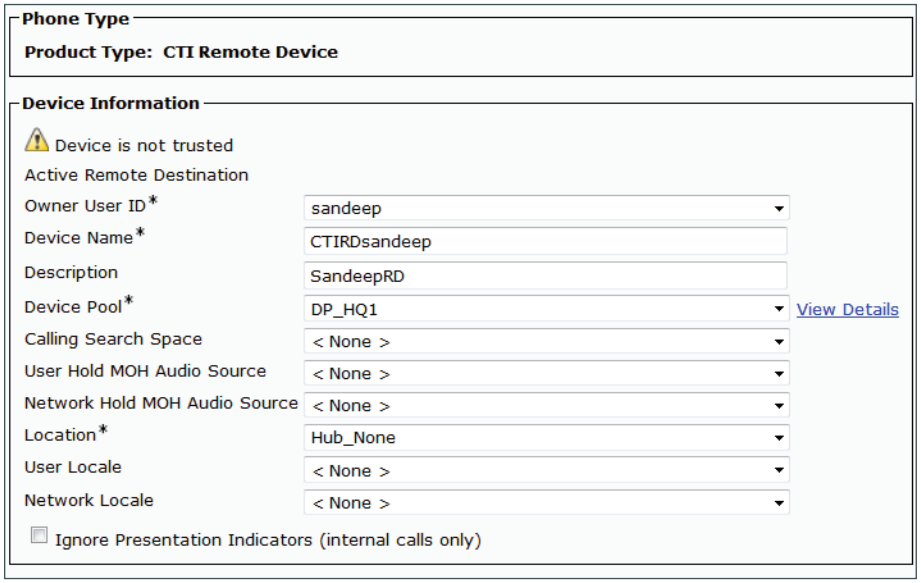
Step 3: On the End User Configuration page of Unified CM administration, select the user and add access control group permissions for the end users. Add Standard CTI Enabled to the access control group, and then click **Save**.

Step 4: Create a CTI remote device that represents off-cluster phones that users can use for UC applications. On the Unified CM Administration page, select Device and then Phone and Add New. Select CTI Remote Device from the drop down and click **Next**

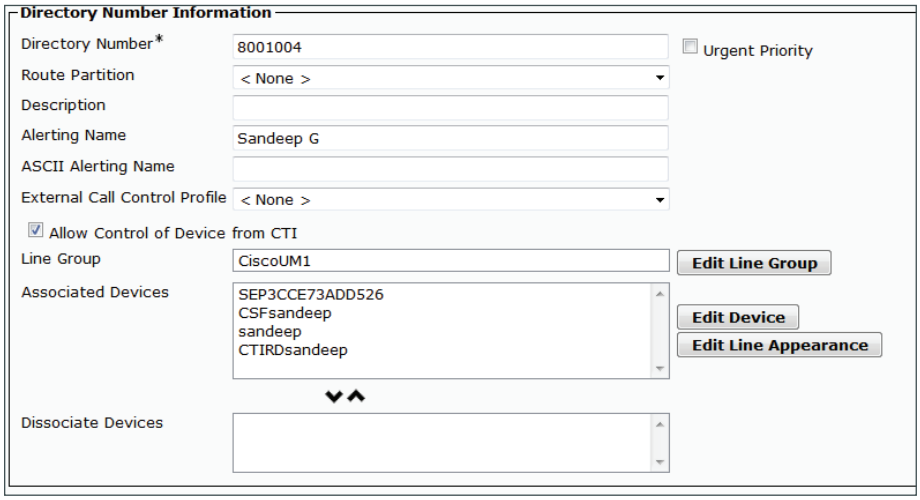


Step 5: In the **Owner User ID** field, select the user that was enabled for mobility. Unified CM populates the Device Name field with the user ID and a CTRID prefix.

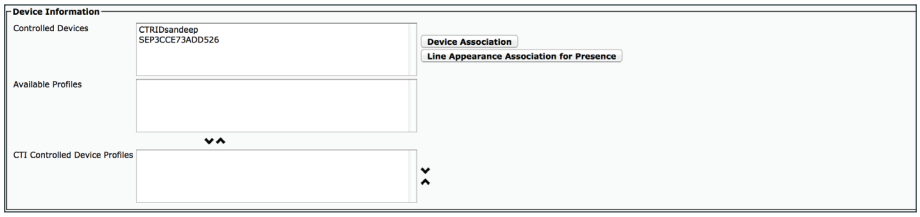
Step 6: Assign a device pool and ensure the selection of the appropriate rerouting calling search space. (The rerouting calling search space is needed for rerouting the calls and ensuring that users can send and receive calls from the CTI remote device.) Click **Save**.



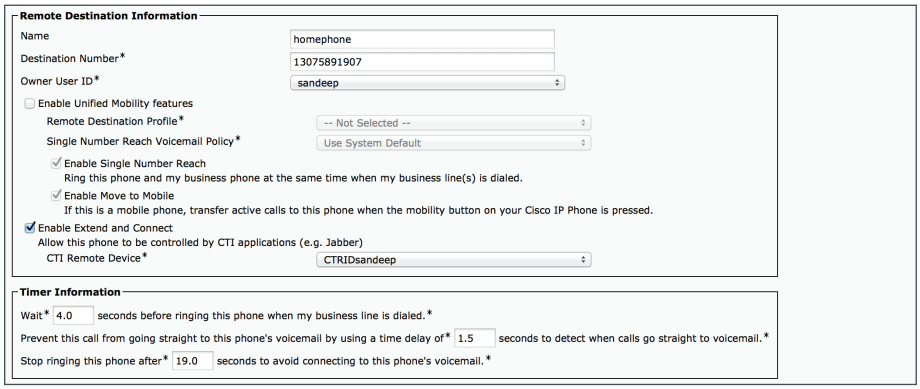
Step 7: Add the directory number. On the CTI remote device page, click **Add a New DN**, and then add the directory number that is shared with user's physical phone. The remaining fields are updated when the shared directory number is selected. Click **Save**.



Step 8: Associate the user to the CTI device that was created in Steps 4 and 5. On the Cisco UCM administration page, select User Management, select end user, and find the user that was enabled for mobility. Click the **Device Association** tab and select the CTI remote device, and then save.



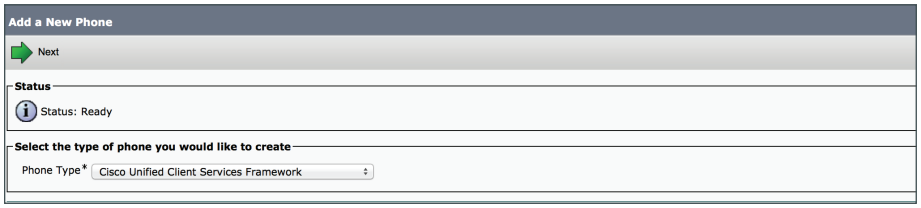
Step 9: Add the remote destination–the address that represents other phones that the user owns, which may be a home phone or PBX phone. This can be an off-cluster device. On the Unified CM administration page, select **Device** and the remote destination and add new. Enter the name and the destination number (the home phone number), select the owner user id, and select **Enable Extend and Connect**.



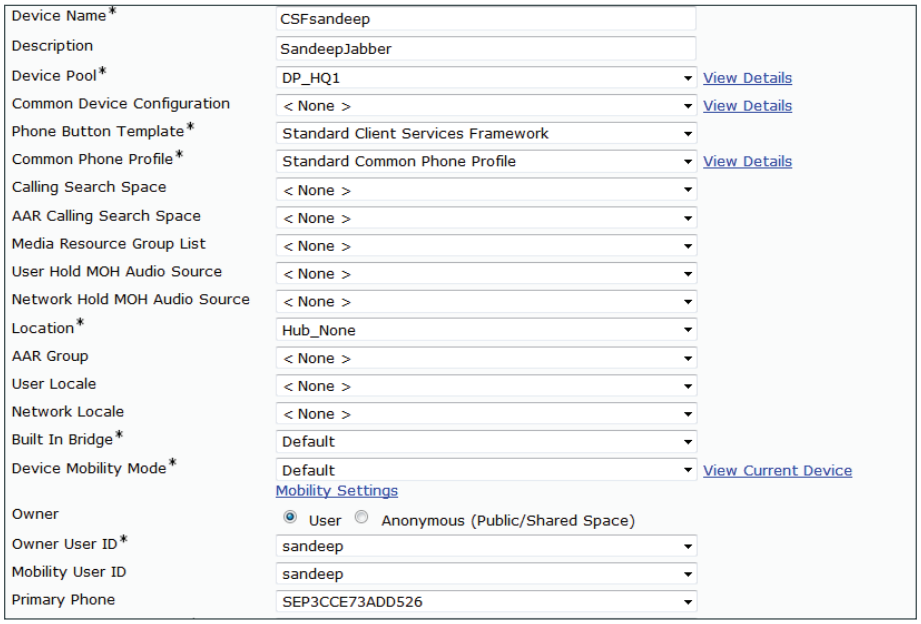
Procedure 2 Using Jabber for Extend and Connect

This procedure configures Jabber for extend and connect.

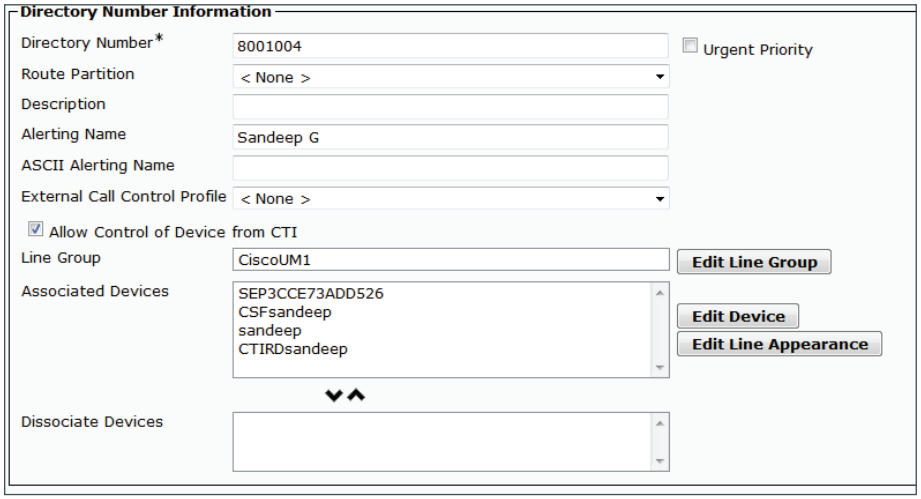
Step 1: Enable the user to use Jabber. Add the user's Cisco Unified Services framework device in the Unified CM. In the Unified CM Administration page, select the device, add new, and select **Cisco Unified Client Services Framework**. Click **Next.**



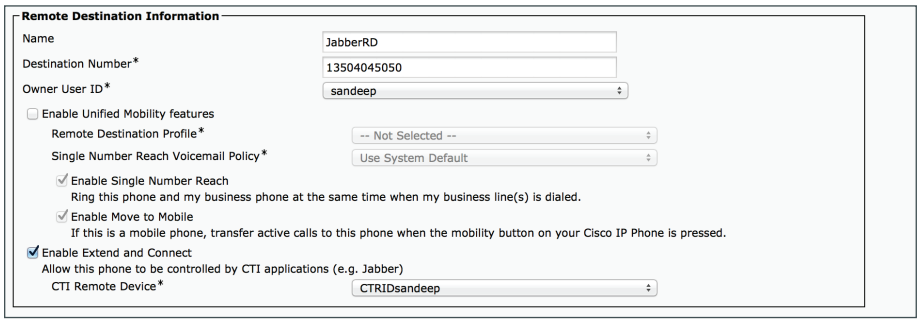
Step 2: In the **Device Name** field, enter **CSF** plus the username, as shown. Specify other fields—**Device Pool**, **Owner User ID**, and **Mobility User ID**. Add the device.



Step 3: Click **Add a New DN** and add the directory number (the number that is assigned to user's physical phone).

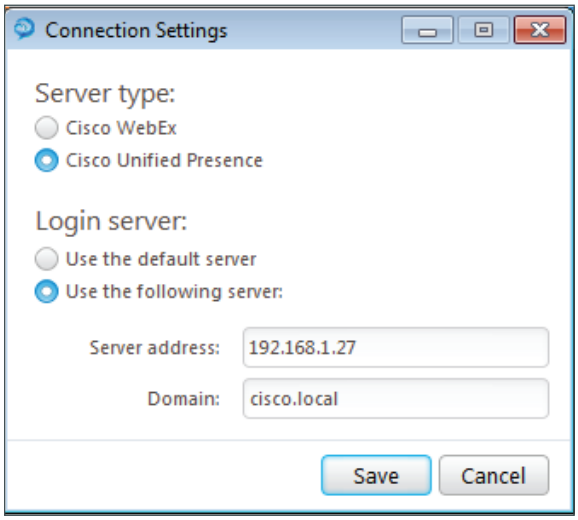


Step 4: Create a new remote destination, with either the home phone or external number. Click **Save**.



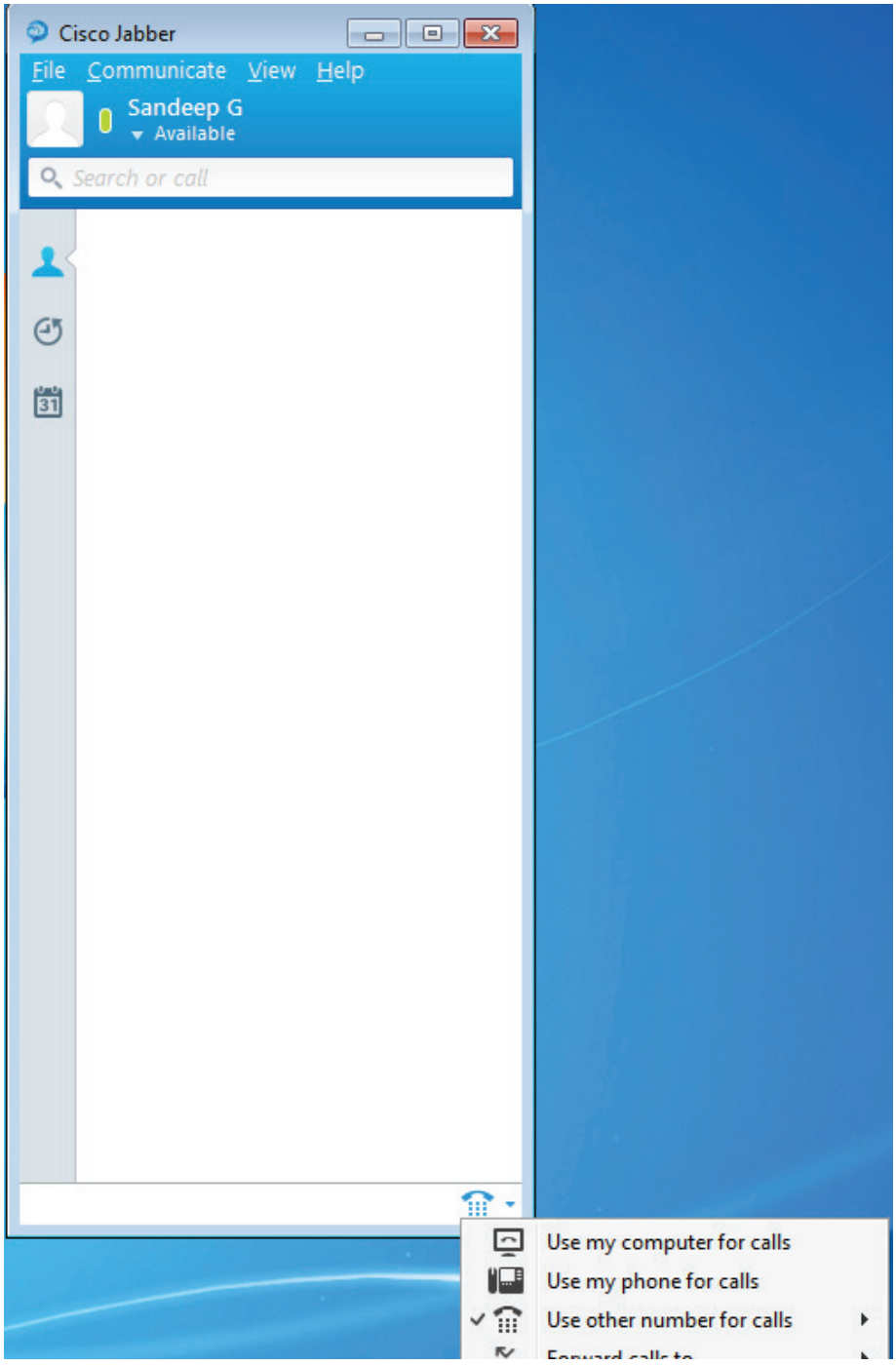
Step 5: Download and install the latest Jabber client for Windows or Macintosh from cisco.com and run the .exe or .dmg file on Windows or Macintosh.

Step 6: After the installation is complete, open the Jabber client and in the settings or Preferences tab, Select **Cisco Unified Presence** and enter the Unified Presence Server IP address and the domain. Click **Save**.



Step 7: Login with the user credentials.

Step 8: In the lower-right corner, select **Use other number for calls** and specify the number to call (the home number). This ensures that when the call is made to user's internal extensions, it will get connected the user's external number or the number that is specified in the remote destination.



PROCESS

Preparing the Platform for Cisco Unified CM IM and Presence

1. Prepare the server for IM and Presence

This guide covers the details for installing Cisco Jabber for Windows. The first two 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.

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://software.cisco.com/download/release.html?mdfid=286269517&flowid=50462&softwareid=283757588&release=10.5&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=286269517&flowid=50462&softwareid=282074312&release=10.5(1)&relind=AVAILABLE&rellifecycle=&reltype=latest

Procedure 1 Prepare the server for IM and Presence

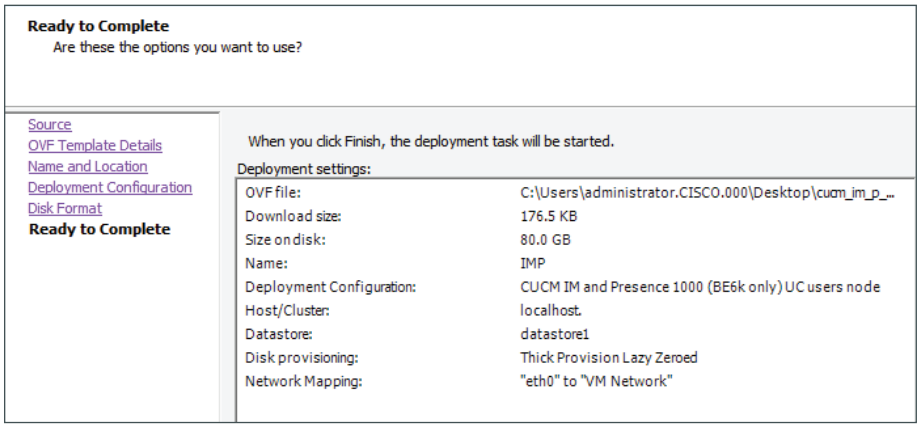
Follow the steps below to deploy an OVA file in order to define the virtual machine requirements. You use the Open Virtualization Format (OVF) support of VMware in order to import and deploy the OVA file.

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 the following option for the number of Cisco UC users, and then click **Next**:

  CUCM IM and Presence 1000 (BE6k only)—For a cluster of up to 1000 Full UC users per node
- 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 the server name (**Example: CUCM-IMP**), 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: On the Getting Started tab, click **Power on the virtual machine**.

Step 7: Click the Console tab, and then watch the server boot.

Step 8: The virtual machine is prepared for installation.

PROCESS

Installing Cisco Unified CM IM and Presence

1. Install Cisco Unified CM IM and Presence
2. Install the redundant server
3. Configure Unified CM IM and Presence
4. Configure the second node of the cluster

Make sure you have the following information:

- Time zone for the server
- Host name, IP address, network mask, and default gateway
- DNS server IP addresses
- Administrator ID and password
- Organization, unit, location, state, and country
- 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**.

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

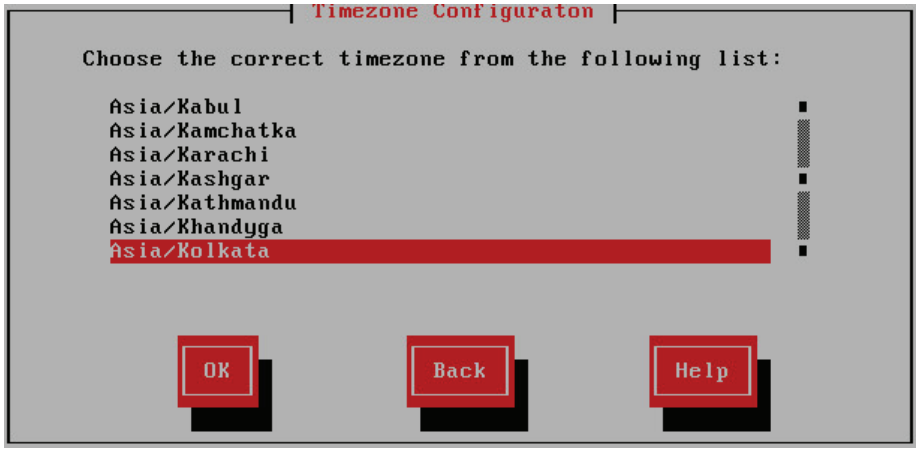
Step 5: On the **Platform Installation Wizard** page, choose **Proceed**.

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**.



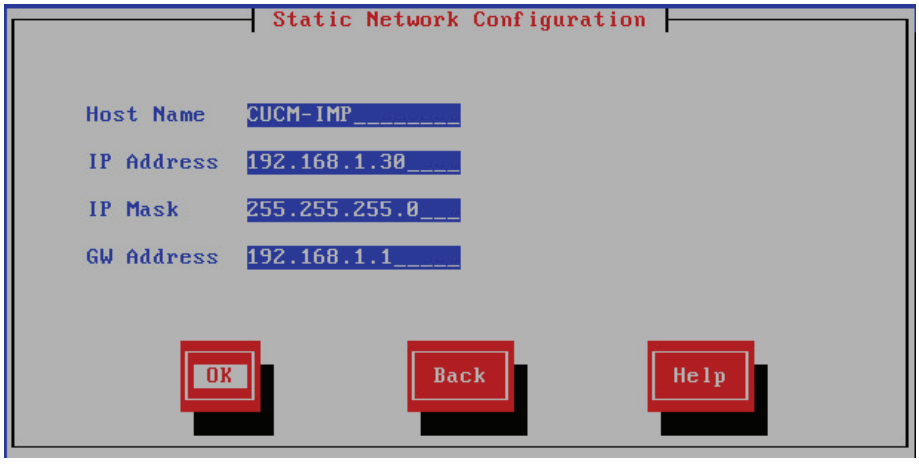
Step 9: On the Auto Negotiation Configuration page, choose **Continue**.

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**:

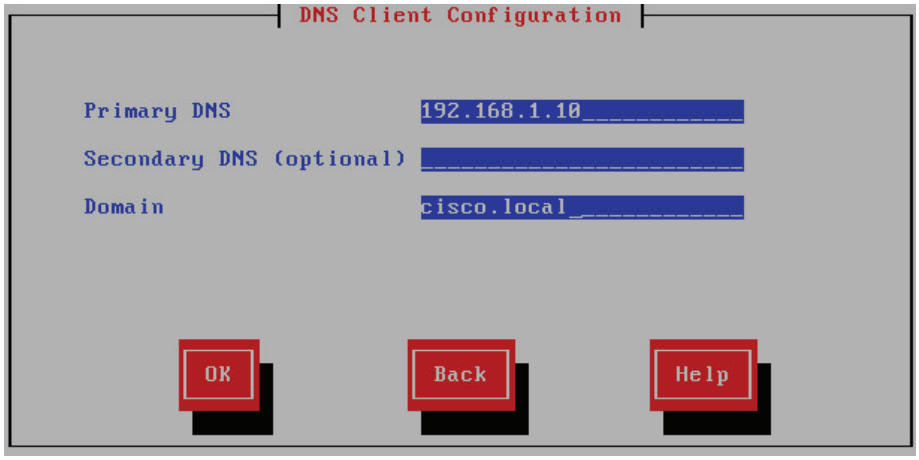
- Host Name–**CUCM-IMP**
- IP Address–**192.168.1.30**
- IP Mask–**255.255.255.0**
- GW Address–**192.168.1.1**



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

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

- Primary DNS –**192.168.1.10**
- 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]**

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

- Organization–**CISCO**
- Unit–**CTG**
- Location–**Bangalore**
- State–**Karnataka**
- Country–**India**

Step 17: On the First Node Configuration page, choose **NO**

Tech Tip

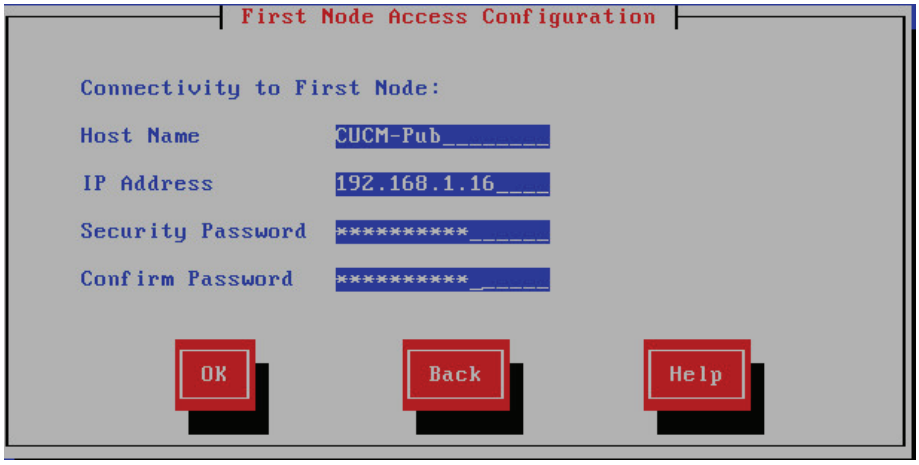
Before proceeding with the remaining nodes installation, ensure that the first node has finished installing and the subscribers have been added under the publisher's **System > Server** menu using the Cisco Unified CM administration interface.

Step 18: On the First Node Configuration page, read the warning, and then choose **OK** to acknowledge you have installed the first node and verified that it is reachable from the network.

Step 19: On the Network Connectivity Test Configuration page, choose **No.**

Step 20: On the First Node Access Configuration page, enter the following information, and then choose **OK**:

- Host Name–**CUCM-Pub** (name of publisher)
- IP Address–**192.168.1.16** (IP address of publisher)
- Security Password–**[password]** (from publisher)
- Confirm Password–**[password]**



Step 21: On the SMTP Host Configuration page, choose **No**.

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**.

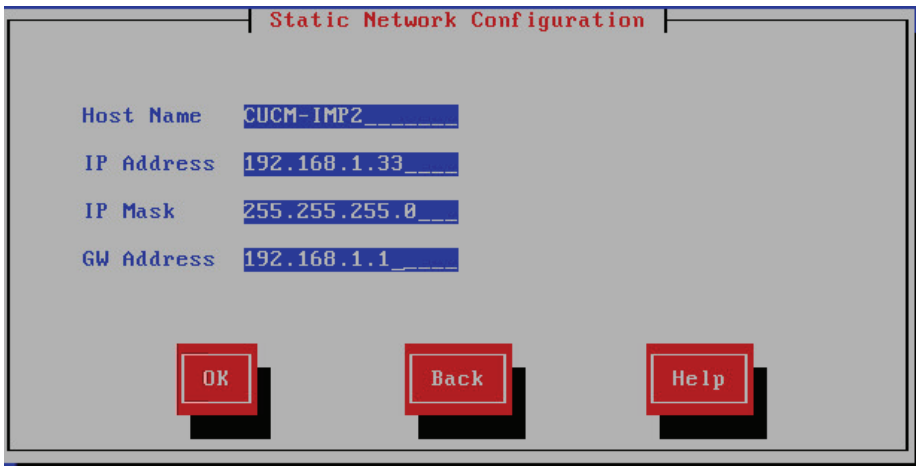
Step 25: Clear **Connect at power on**, and then click **OK**

Procedure 2 Install the redundant server

Step 1: Install an additional node of the cluster by repeating steps 1 to 12 in the previous procedure.

Step 2: On the Static Network Configuration page, enter the following information, and then choose **OK**:

- Host Name–**CUCM-IMP2**
- IP Address–**192.168.1.33**
- IP Mask–**255.255.255.0**
- GW Address–**192.168.1.1**



Step 3: Repeat steps 13 to 25. This finishes the installation of the next node.

Procedure 3 Configure Unified CM IM and Presence

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

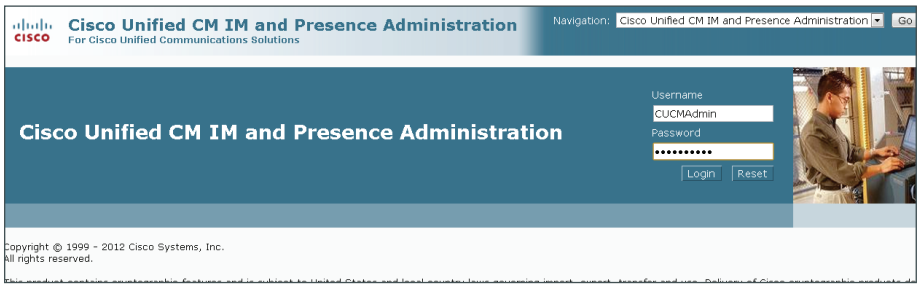
Step 1: In a web browser, access the IP address or hostname of the Cisco Unified CM IM and Presence server, and then in the center of the page under Administrative Applications, click **Cisco Unified Communications Manager IM and Presence**.

Tech Tip

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

Step 2: In the **Navigation** list, click **Cisco Unified IM and Presence administration**, and then click **Go**

Step 3: Enter the username and password of the CUCM admin.



Step 4: 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

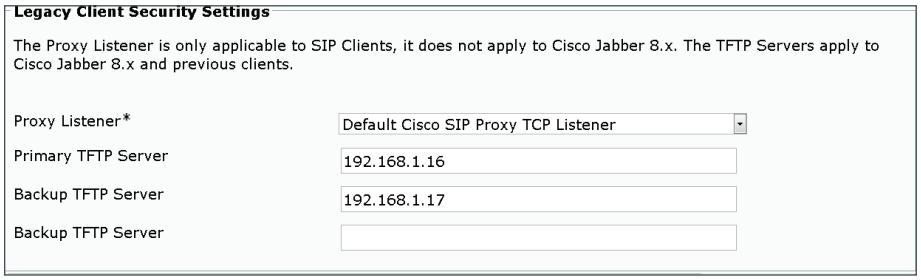
	Service Name	Activation Status

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

Step 6: In the Navigation list at the top right of the page, choose **Cisco Unified CM IM and Presence Administration**, and then click **Go**.

Step 7: Navigate to **Application > Legacy Clients > Settings**, enter the following information, and then click **Save**:

- Primary TFTP Server—**192.168.1.16**
- Backup TFTP Server—**192.168.1.17**



The initial application administration setup is now complete.

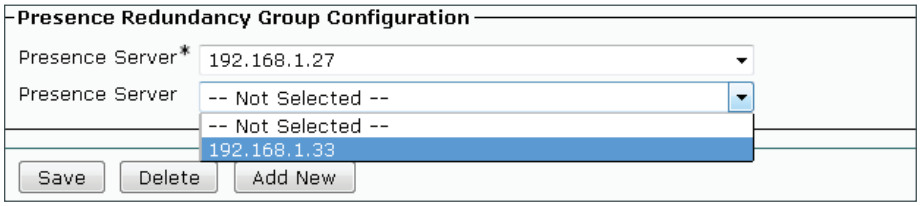
Procedure 4 Configure the second node of the cluster

Step 1: In the previous procedure, repeat steps 1-6 for the second node.

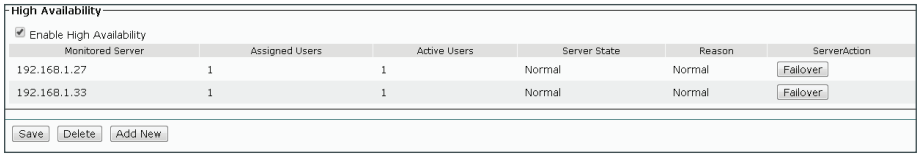
Step 2: For adding the second node of the cluster to the presence redundancy group, In a web browser, access the IP address or hostname of the Cisco Unified CM publisher, and then in the center of the page, under Installed Applications, click Cisco Unified Communications Manager

Step 3: Navigate to **Systems > Presence Redundancy Groups**, and then click **Find**.

Step 4: Under Presence Redundancy Group configuration, click **DefaultCUPSubcluster**, select the second node of the cluster, and then click **Save**.



Step 5: Select **Enable the High Availability**, and then click **Save**.



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 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.

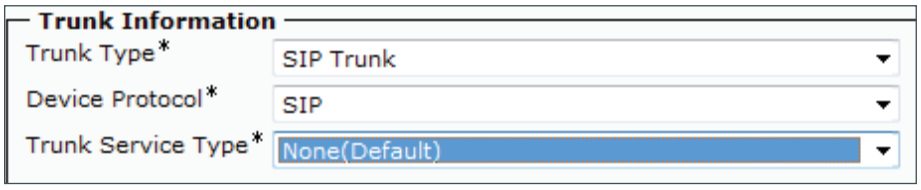
Step 1: In a web browser, access the IP address or hostname of the Cisco Unified CM publisher, and then in the center of the page, under Installed Applications, click **Cisco Unified Communications Manager**.

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

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

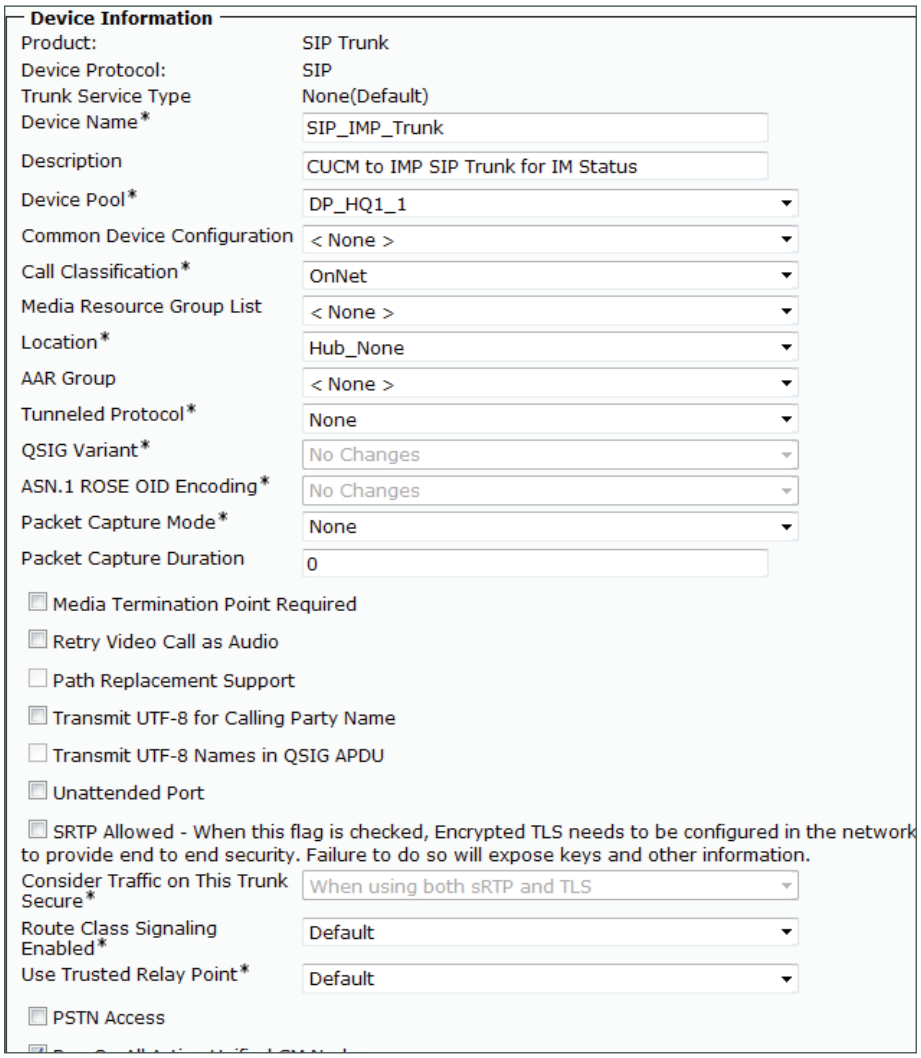
Step 4: On the Trunk Configuration page, enter the following values, and then click **Next**:

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



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**



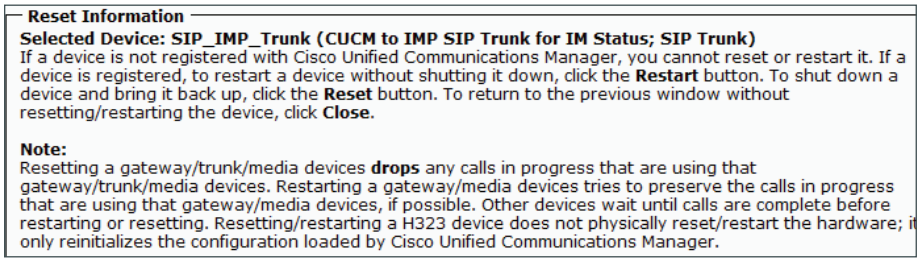
Step 6: In the SIP Information section, enter the following values, and then click **Save**:

- Destination Address 1—**192.168.1.27**
- Destination Port 1—**5060**
- SIP Trunk Security Profile—**Non Secure SIP Trunk Profile**
- SIP Profile—**Standard SIP Profile**

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**.

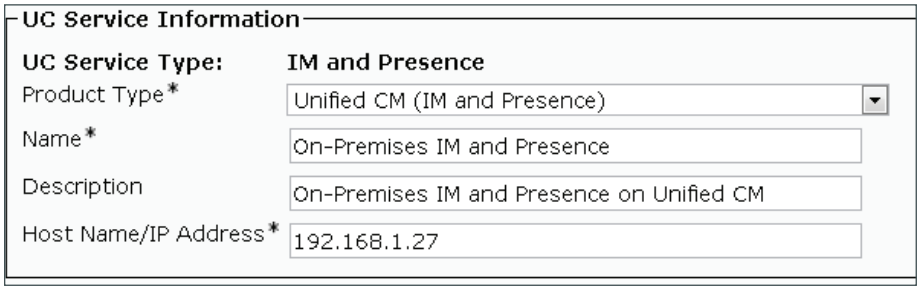


Step 10: Navigate to **User Management > User Settings > UC Service**, and then click **Add New**.

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—**192.168.1.27**

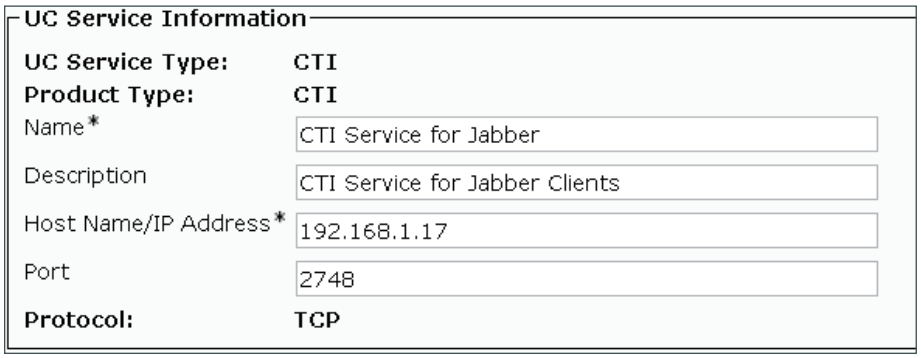


Step 13: Navigate to **User Management > User Settings > UC Service**, and then click **Add New**.

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–**192.168.1.17 (Subscriber 1)**
- Port–**2748**

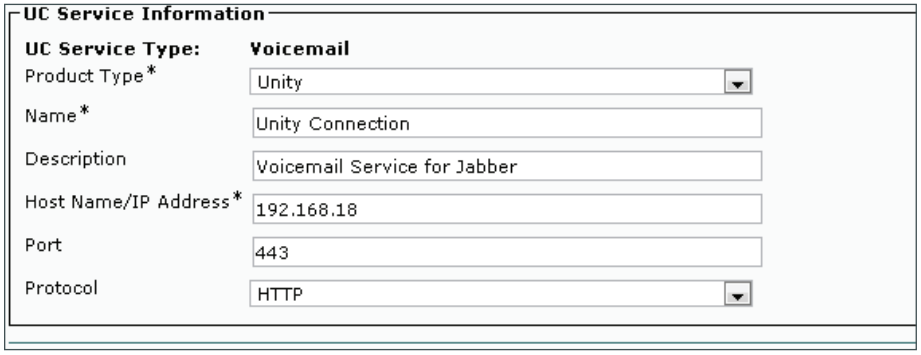


Step 16: Navigate to **User Management > User Settings > UC Service**, and then click **Add New**.

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–**192.168.1.18**
- Port–**443**
- Protocol–**HTTP**



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

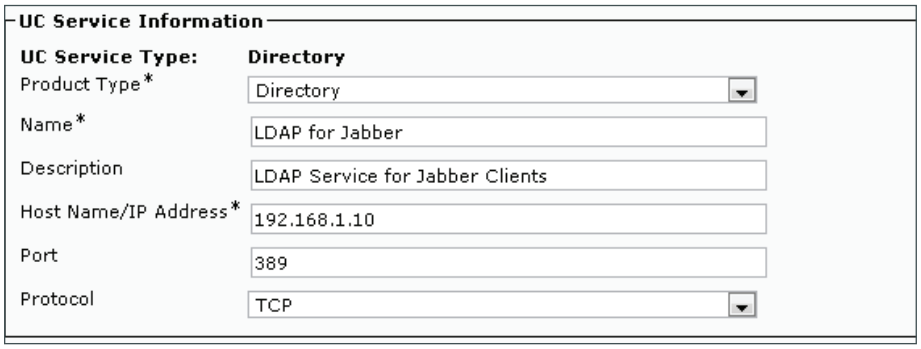
Step 20: On the UC Service Configuration page, in the UC Service Type list, select **Directory**, and then click **Next**.

Tech Tip

When using an LDAP directory service, the Cisco Jabber client's click-to-call phone number 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.

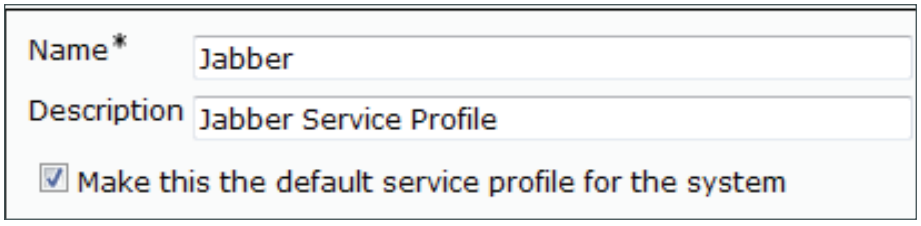
Step 21: In the Add a UC Service section, enter the following information, and then click **Save**:

- Product Type–**Directory**
- Name–**LDAP for Jabber**
- Description–**LDAP Service for Jabber Clients**
- Host Name/IP Address–**192.168.1.10**
- Port–**389**
- Protocol–**TCP**



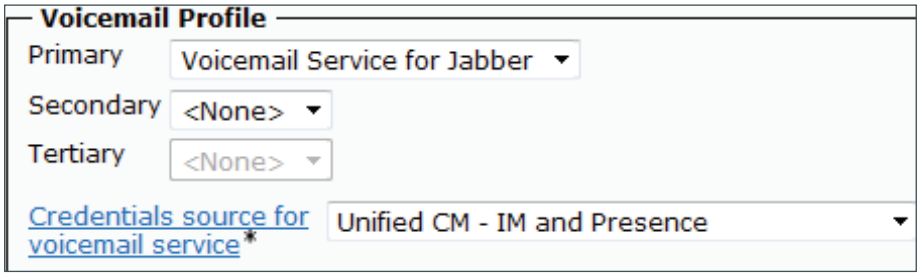
Step 22: Navigate to **User Management > User Settings > Service Profile**, click **Add New**, and then enter the following information:

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



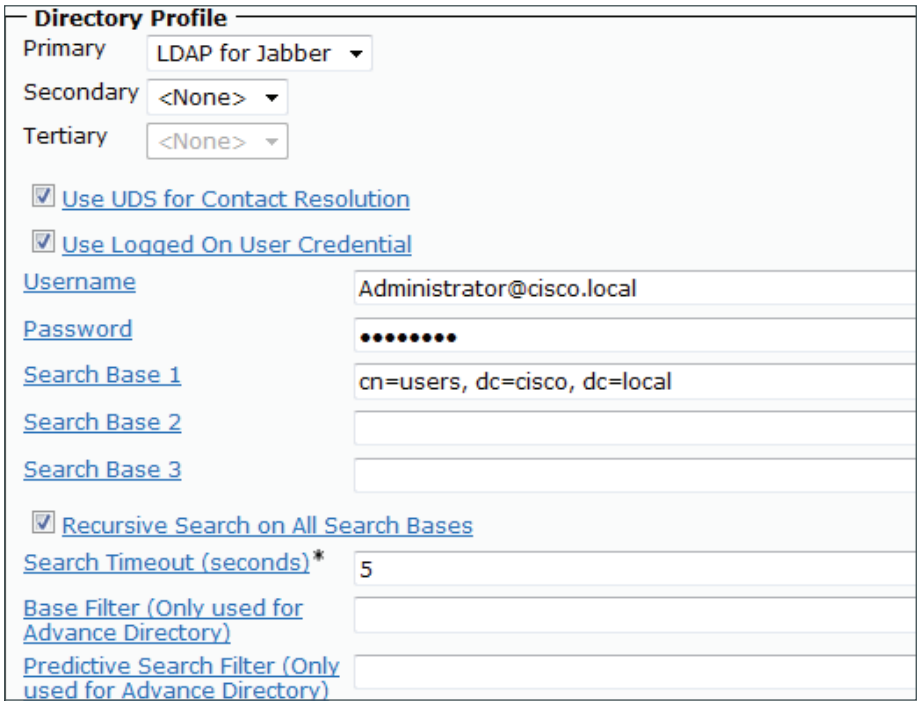
Step 23: In the Voicemail Profile section, enter the following information:

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

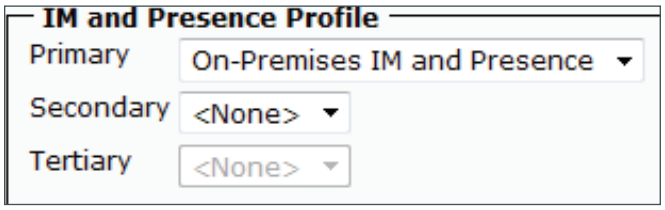


Step 24: In the Directory Profile section, enter the following information:

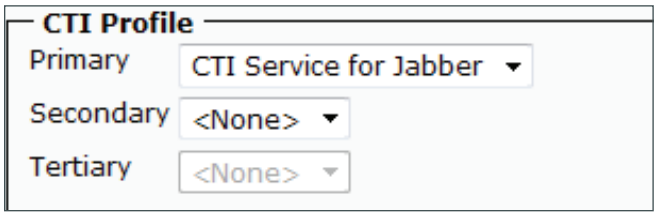
- Primary–**LDAP for Jabber**
- Use UDS for Contact Resolution–**Select**
- Use Logged On User Credential–**Select**
- Username–**Administrator@cisco.local**
- Password–**[password]**
- Search Base 1–**cn=users, dc=cisco, dc=local**



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



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



Procedure 2 Configure Unity Connection for Jabber

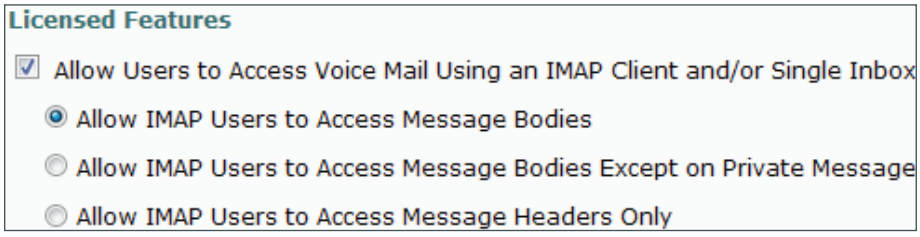
The next set of steps will configure Cisco Unity Connection for use with Jabber.

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**.



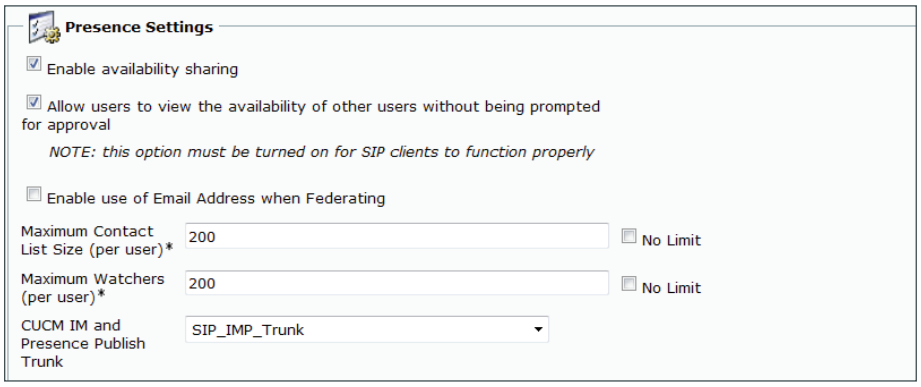
Procedure 3 Configure IM and Presence services

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**.

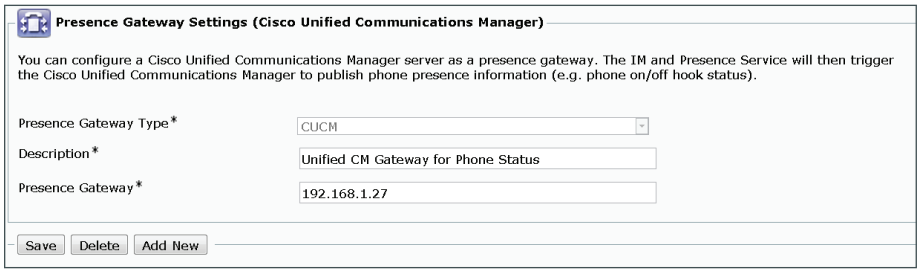
Step 3: Navigate to **Presence > Settings**, and in the CUCM IM and Presence Publish Trunk list, choose **SIP_IMP_Trunk**, and then click Save.



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**:

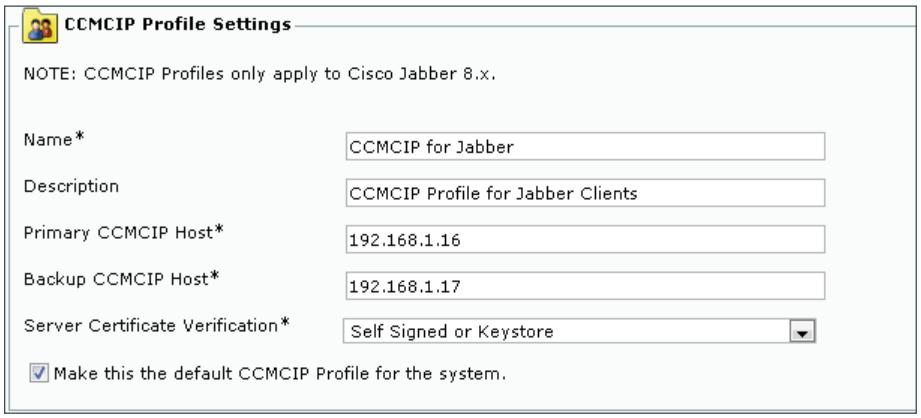
- Presence Gateway Type—**CUCM**
- Description—**Unified CM Gateway for Phone Status**
- Presence Gateway—**192.168.1.27 (publisher)**



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–**192.168.1.16 (subscriber 1)**
- Backup CCMCIP Host–**192.168.1.17 (subscriber 2)**
- Server Certificate Verification–**Self Sígned or Keystore**
- Make this the default CCMCIP Profile for the system–**Select**



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**.

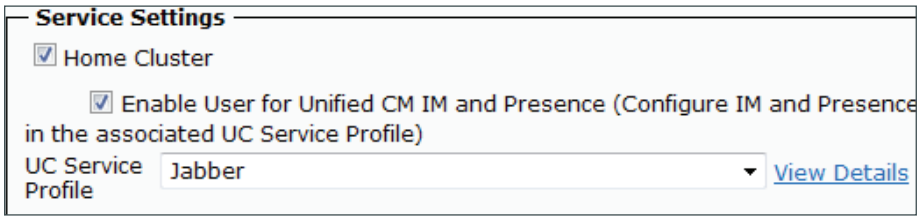
Step 2: Enter the Unified CM application username and password, and then click **Login**.

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**



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:

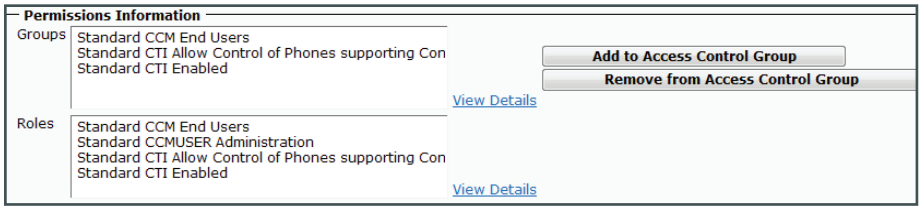
- Access Control Group—**Standard CCM End users (existing)**
- Access Control Group—**Standard CTI Enabled**

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**.



Step 11: Repeat steps 3-10 for each additional Cisco Jabber for Windows.

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.

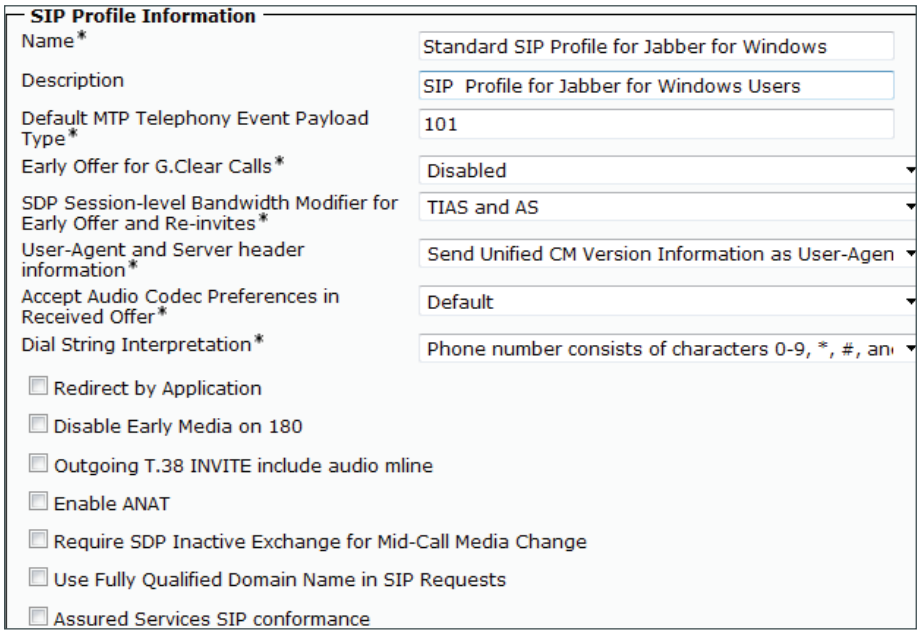
You also modify the default standard common phone profile in order to enable **Real-time Transport Control Protocol (RTCP)**.

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

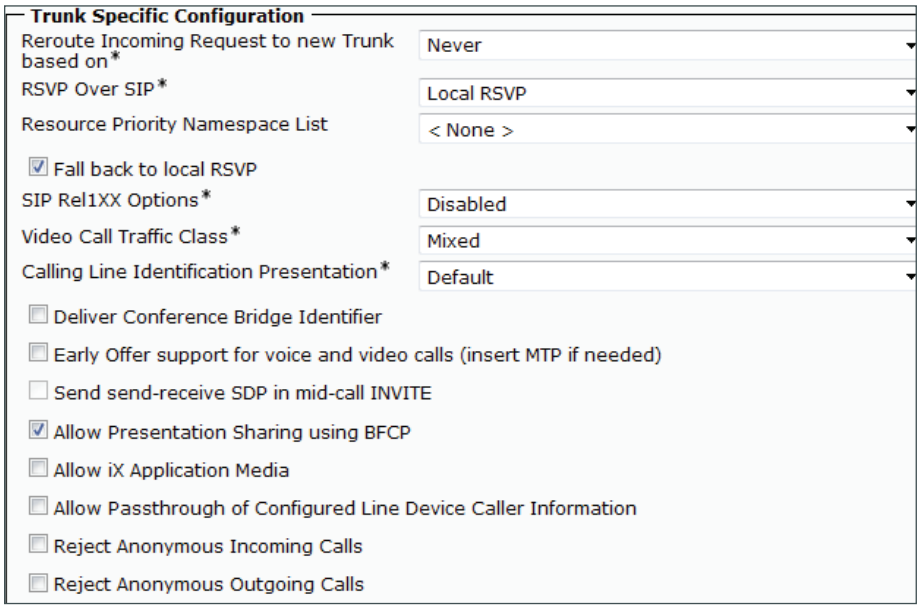
Step 2: Locate Standard SIP Profile, and then on the right side of the page in line with the profile, click the **Copy** icon.

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**



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



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**.

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

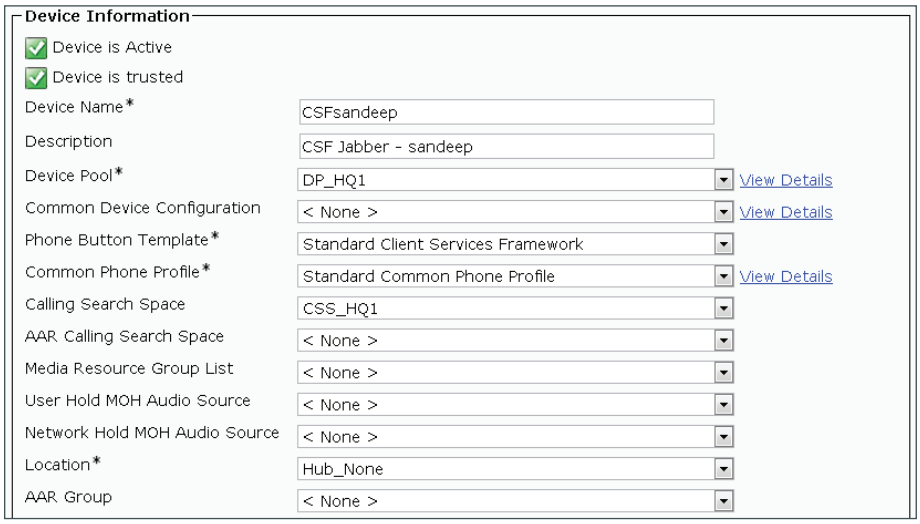
The Client Service Framework (CSF) phone type is used within Cisco Unified CM in order to deploy Cisco Jabber for Windows clients that require unified communications.

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**.

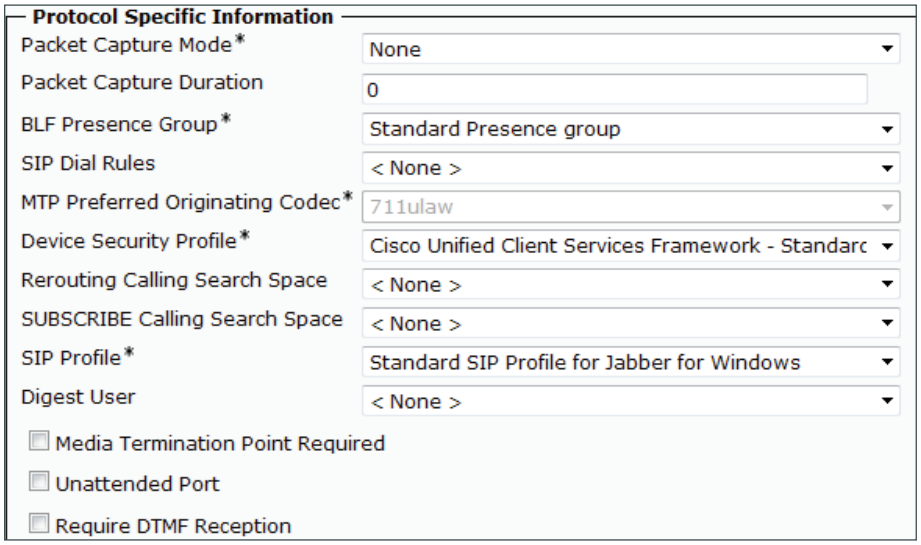
Step 3: On the Phone Configuration page, in the Device Information section, enter the following information:

- Device Name–**CSFsandeep (uppercase CSF plus username)**
- Description–**CSF Jabber - sandeep**
- 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**



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**



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 phone number 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—**8001004**
- Route Partition—**PAR_Base**
- Description—**Jabber CSFsandeep**
- Alerting Name—**Sandeep G**
- ASCII Alerting Name— **Sandeep G**
- External call control profile—**None**
- Allow Control of Device from CTI—**Select**

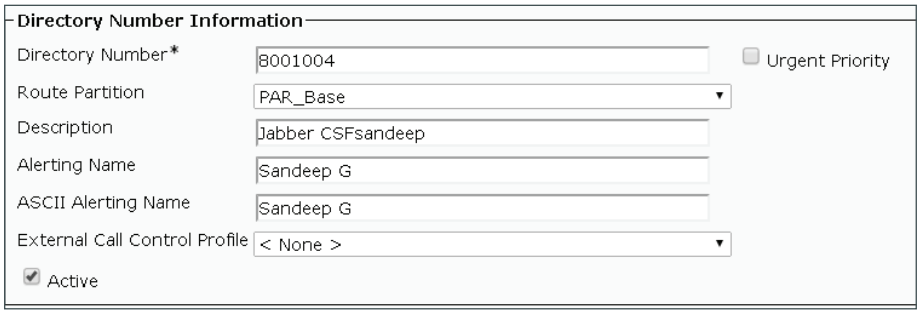
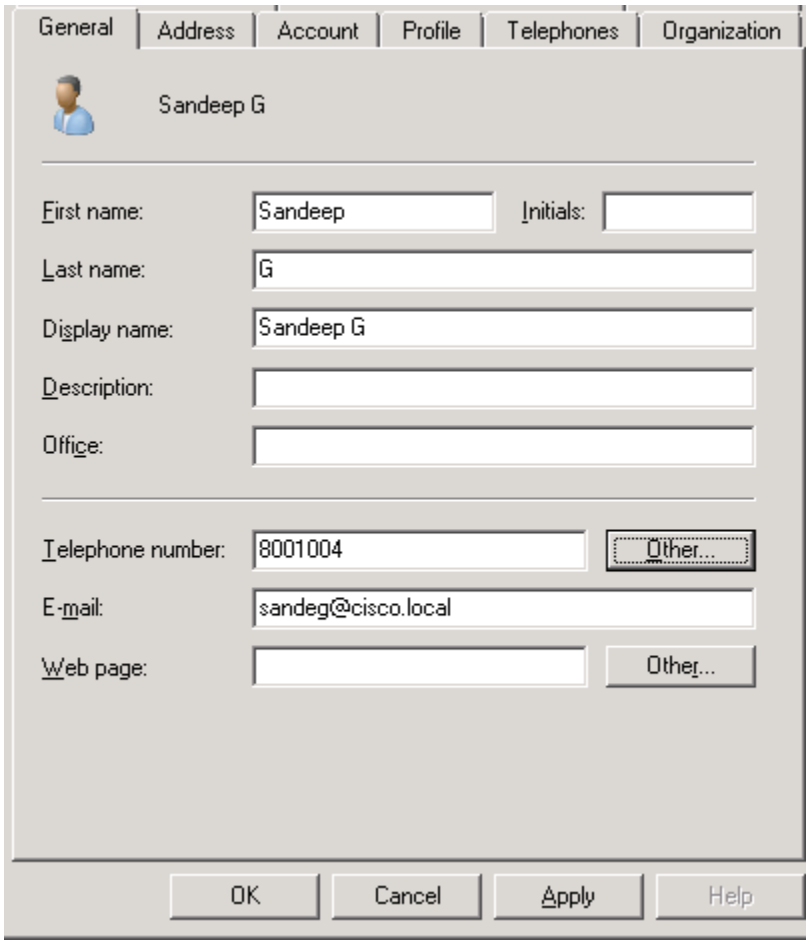
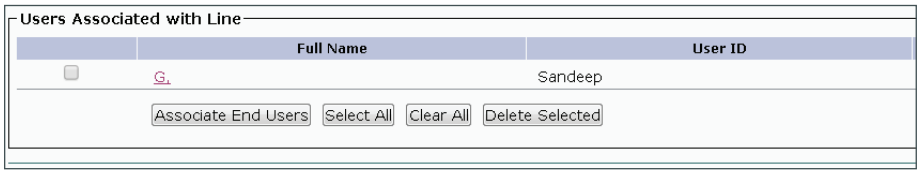


Figure 14 - Example LDAP general information telephone number attribute



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**



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: CSFsandeep), and then click **Save Selected/Changes**.

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

Step 6: Repeat procedures 2-3 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.

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	Size	Packed	Type	Modified	CRC32
..			File folder		
CiscoJabberSetu...	47,587,840	43,052,406	Windows Installer ...	12/12/2013 1:0...	61EA7CE7
README_install....	238	135	Text Document	12/14/2013 6:3...	0DE2096E

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

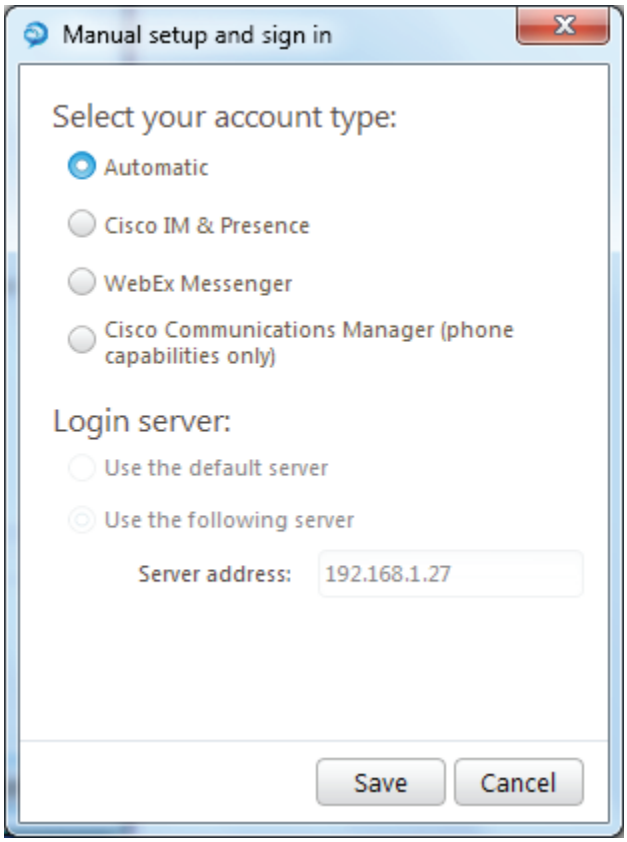
Step 5: Depending on your operating system, you have to accept several security messages as the software installs. After the software installs, click **Finish**.

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 Manual setup and sign in Settings page, enter the following information, and then click **Save**:

- Server type–**Cisco IM and Presence**
- Login server–**Use the following server**
- Server address–**192.168.1.27**



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

Step 10: Add contacts and favorites as needed.

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

Appendix A: Product List

Data Center or Server Room

Component	Product Description	Part Numbers	Software
Call Control	Cisco Business Edition 6000 with up to 1000 users	BE6K-ST-BDL-K9	10.5.1.10000-7

Headquarters Voice

Functional Area	Product Description	Part Numbers	Software
Headquarters Voice Router	Cisco 3945 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3945-VSEC/K9	15.2(4)M5 securityk9 license ipbasek9 license uck9 license
	Security Paper PAK for Cisco 3900 Series	SL-39-SEC-K9	
	IP Base Paper PAK for Cisco 3900 series	SL-39-IPB-K9	
	Unified Communications Paper PAK for Cisco 3900 Series	SL-39-UC-K9	
	2 Port Channelized T1/E1 and ISDN PRI High Speed WAN Interface Card (data only)	HWIC-2CE1T1-PRI	
	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card-T1/E1	VWIC2-2MFT-T1/E1	

Remote Site Voice

Functional Area	Product Description	Part Numbers	Software
Remote Site Voice Router	Cisco 2921 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2921-VSEC/K9	15.2(4)M5 securityk9 license ipbasek9 license uck9 license
	Security Paper PAK for Cisco 2900 Series	SL-29-SEC-K9	
	IP Base Paper PAK for Cisco 2900 series	SL-29-IPB-K9	
	Unified Communications Paper PAK for Cisco 2900 Series	SL-29-UC-K9	
	2 Port Channelized T1/E1 and ISDN PRI High Speed WAN Interface Card (data only)	HWIC-2CE1T1-PRI	
	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card-T1/E1	VWIC2-2MFT-T1/E1	
	SRST For 50 phones	FL-SRST-50	15.2(4)M5

Endpoints

Functional Area	Product Description	Part Numbers	Software
Phones	Unified IP Phone 9900 Series	CP-9971-C-K9	SIP9971.9-4-1-9 SIP9971.9-3-2-10
	Unified IP Phone 8900 Series	CP-8961-C-K9	SIP8961.9-4-1-9
	Unified IP Phone 7800 series	CP-7821-K9 CP-7841-K9 CP-7861-K9	SIP78xx.10-1-1-SR1-4
	Unified IP Phone 7975	CP-7975G	SCCP75.9-3-1SR4-1S
	Unified IP Phones DX600 series	CP-DX650-K9	SIPdx650.10-1-2-24
Video Endpoints	Cisco TelePresence EX series	CTS-EX90-K9	TC 7.0 .0.dcf48ec
	Cisco TelePresence SX series	CTS-SX20-PHD4X-K9	TC 7.0.0.dcf48ec
Soft Client	Jabber	Cisco Jabber for Windows	Jabber_for_ Windows-9.6.0

Feedback

Please send comments and suggestions about this guide to collab-mm-cvd@external.cisco.com.

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.

1 09/14