# • **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1**

# **Newer Cisco SBA for Government Guides Available**

This guide is part of an older series of Cisco Smart Business Architecture for Government. To access the latest Cisco SBA for Government Guides, go to http://www.cisco.com/go/govsba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.



cisco.

SBA FOR GOVT

MIDSIZE

COLLABORATION

# Unified Communications Rapid Deployment Guide

🔵 🛑 SBA FOR GOVERNMENT

Revision: H2CY10

# The Purpose of This Guide

This guide provides step-by-step instructions for configuring Cisco Unified Communications Manager and Cisco UnityConnection in the Cisc SBA for Midsize Agencies.

This guide is a companion document to the *Cisco SBA for Midsize Agencies—Borderless Networks Foundation Design Overview* and *Foundation Deployment Guide*.

#### **Who Should Read This Guide**

This guide is intended for the reader who:

- Will be configuring and deploying Cisco Collaboration solutions at customer locations
- Wants to reduce cost by optimizing connectivity solutions and improve employee productivity
- Has 100–1000 connected employees
- Has some technical background with Cisco Unified Communications Manager and Cisco UnityConnection<sup>®</sup>.

#### **Related Document**

Before reading this guide



Design Overview



# Table of Contents

SBA Overview
Introduction
Rapid Deployment Method Overview         4           Auto-Registration         4
Active Directory Integration5
Dial Plan5
Class of Service
Local Route Groups6
Survivable Remote Site Telephony (SRST)6
Device Mobility7
Extension Mobility7
Media Resources7
Unified CM Reference Architecture7
Call Admission Control7

The Rapid Deployment Method	8
Appendix A: Configuration Notes	<b>32</b> .32
Cisco Unity Connection	.33
Appendix B: SBA for Midsize Agencies Document System	35

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITA-TION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental. Cisco Unified Communications SRND (Based on Cisco Unified Communications Manager 7.x)

© 2011 Cisco Systems, Inc. All rights reserved.

# SBA Overview

The Cisco® Smart Business Architecture (SBA) for Government is a comprehensive design for networks with up to 1000 users. This out-of-the-box design is simple, fast, affordable, scalable, and flexible.

The Cisco SBA for Midsize Agencies incorporates LAN, WAN, wireless, security, WAN optimization, and unified communication technologies tested together as a solution. This solution-level approach simplifies the system integration normally associated with multiple technologies, allowing you to select the modules that solve your agency's problems rather than worrying about the technical details.

We have designed the Cisco SBA to be easy to configure, deploy, and manage. This architecture:

- Provides a solid network foundation
- · Makes deployment fast and easy
- · Accelerates ability to easily deploy additional services
- · Avoids the need for re-engineering of the core network

By deploying the Cisco SBA, your agency can gain:

- A standardized design, tested and supported by Cisco
- Optimized architecture for midsize agencies with up to 1000 users and up to 20 remote sites
- · Flexible architecture to help ensure easy migration as the agency grows
- Seamless support for quick deployment of wired and wireless network
   access for data, voice, teleworker, and wireless guest
- Security and high availability for agency information resources, servers, and Internet-facing applications
- Improved WAN performance and cost reduction through the use of WAN
   optimization
- Simplified deployment and operation by IT workers with CCNA<sup>®</sup> certification or equivalent experience
- Cisco enterprise-class reliability in products designed for midsize agencies

#### **Guiding Principles**

We divided the deployment process into modules according to the following principles:

- Ease of use: A top requirement of Cisco SBA was to develop a design that could be deployed with the minimal amount of configuration and day-two management.
- **Cost-effective:** Another critical requirement as we selected products was to meet the budget guidelines for midsize agencies.
- Flexibility and scalability: As the agency grows, so too must its infrastructure. Products selected must have the ability to grow or be repurposed within the architecture.
- Reuse: We strived, when possible, to reuse the same products throughout the various modules to minimize the number of products required for spares.



The Cisco SBA can be broken down into the following three primary, modular yet interdependent components for the midsize agency.

- Network Foundation: A network that supports the architecture
- Network Services: Features that operate in the background to improve and enable the user experience without direct user awareness
- · User Services: Applications with which a user interacts directly

# Introduction

Unified Communications (UC) Rapid Deployment Method (RDM) is a procedural method for installing, configuring, and deploying UC for basic telephony and simple voice messaging. This turnkey solution is constructed to be easy and quick while providing a solid foundation for further configuration and deployment of advanced UC features without the need to redesign or reengineer when a new feature or service is added.

RDM is part of the SBA for Midsize Agencies (100–1000 connected users), which utilizes Cisco Unified Communications Manager cluster for call processing and a Cisco Unity<sup>®</sup> Connection for voice messaging.

The UC module of SBA consists of a headquarters and up to twenty remote sites. The two Unified Communications Manager appliances and the Cisco Unity Connection appliance are placed at the main site to handle all of the call processing for up to 1000 telephony users with voice messaging. Each remote site takes advantage of the Integrated Service Router (ISR) that was deployed as part of the WAN module, and is configured for Survivable Remote Site Telephony in the event of service interruptions.

The RDM includes:

- Two Unified Communication Manager appliances configured for 1:1 call processing redundancy
- One Unity Connection server configured for simple voice messaging
- One headquarters Site and up to 20 remote sites

The Cisco SBA for Midsize Agencies is a prescriptive architecture that delivers an easy-to-use, flexible and scalable network with wired, wireless, security, WAN optimization, and unified communication components. It eliminates the challenges of integrating the various network components by using a standardized design that is reliable with comprehensive support offerings.

The Cisco SBA for Midsize Agencies is designed to address the basic dial tone and simple voice messaging requirements of agencies with 100 to 1000 employees.

# 🔵 Tech Tip

Certain information such as IP addresses, usernames, passwords, and specific command responses are used for example only and may not be appropriate for your specific deployment.

The products and priorities for this design were based on requirements from customers, partners, and Cisco field personnel. The specific end-customer agency 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 changes to this design that you plan to deploy.

Figure 1 illustrates the complete SBA foundation design with all of the modules deployed.

Figure 1. Network Architecture Baseline



# Rapid Deployment Method Overview

The Rapid Deployment Method (RDM) includes step-by-step instructions for installing, configuring and deploying Unified Communications (UC) for basic telephony and simple voice messaging, including:

- Platform Installation
- Server and Site Configuration
- User and Device Configuration
- Unity Connection Deployment
- IP Phone Deployment

#### RDM:

- Uses auto-registration for quick and easy deployment of phones
- Uses the Active Directory integration feature in both Unified Communications Manager and Unity Connection for deployments that require a single source for User Management.
- Is provisioned to utilize the Device Mobility feature, which enables Unified Communications Manager to determine the physical locations of devices. Unified Communications Manager uses the device's IP subnet to determine the exact location of the IP phone. By enabling device mobility within a cluster, mobile users, such as those on wireless, can roam from one site to another, thus acquiring the site-specific settings. Unified Communications Manager then uses these dynamically allocated settings for call routing, codec section, media resource selection, and so forth.
- Is provisioned to use the Cisco Extension Mobility (EM) feature, which enables users to assign a Cisco Unified IP phone as their own. The EM feature dynamically configures a phone according to the authenticated user's device profile. Allowing a user to log into a phone alleviates the need for device-to-user association during user provisioning.
- · Provisions individual media resources for every sit.
- Provisions Session Initiation Protocol (SIP) gateways for all sites.

- Automatically provisions the Unified Communications Manager for Voice Messaging integration and the procedure within RDM documents the Unity Connection configuration
- Uses Endpoint Addressing that consists of a uniform on-net dial plan containing an access code, site codes, and 4-digit extensions
- Automatically configures a North American Dial Plan as part of the path selection for public switched telephone network (PSTN) destinations

#### **Auto-Registration**

Auto-registration allows Unified Communications Manager to automatically assign a directory number to new phones as they are deployed in your network. In UC RDM, auto-registration is enabled by default to allow for quick and easy deployment of phones. Once the phones are registered and the RDM Deployment Guide has been followed completely, users configured in the system can log into the auto-registered phones with Extension Mobility.

By default, auto-registered phones in RDM are able to dial any on-net directory number as well as off-net emergency 911 calls. They are not, however, able to dial any other off-net numbers other than emergency dialing.

### 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.

#### **Active Directory Integration**

Active Directory integration allows you to provision users automatically from the agency directory into the Unified Communications Manager 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 Communications Manager each time a change occurs in the agency directory. The other advantage is that end users are able to authenticate to Unified Communications Manager and Unity Connections using the same credentials in Active Directory, which reduces the number of passwords across the network because the applications share a common directory.

Figure 2. Directory Integration



#### **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. UC RDM configures a North American Dial Plan as part of the path selection for PSTN destinations. You can modify this to meet your specific needs, but by default, it is configured with the North American Numbering Plan and contains the following patterns:

#### Figure 3. Dial Plan

ROUTE PATTERN	ROUTE PARTITION	_
9.911	PAR_Base	
911	PAR_Base	Emergency Dialing
9.[2-9]XXXXX#	PAR_PSTN_Local	
9.[2-9]XXXXXX	PAR_PSTN_Local	Local Dialing
9.1[2-9]XX[2-9]XXXXXX	PAR_PSTN_National	National Dialing
9.1[2-9]XX[2-9]XXXXXX#	PAR_PSTN_National	National Dialing
9.011!	PAR_PSTN_Intl	International Dialing
9.011!#	PAR_PSTN_Intl	

For Local, National, and International route patterns, there are two configured, one to route dinaled digits of that specific length and one configured similarly with a pound (octothorpe) to allow users to bypass interdigit timeout.

With regards to Endpoint Addressing, the recommendation for UC RDM deployments for less than 1000 users is to 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 that could otherwise overlap if a uniform abbreviated dial plan were implemented.

RDM consists of:

- · One digit as an intersite access code
- Two digits for the site code to accommodate the 20 sites
- Four digits for the sites extension
- As such, UC RDM requires a format of 8 + SS + XXXX, where 8 is the on-net access code, SS is a two-digit site code, and XXXX is a four-digit extension number, giving a total of seven digits.

Figure 4. Digit Breakdown



#### **Class of Service**

Class of Service is configured in Unified Communications Manager utilizing Calling Search Spaces and Partitions. There are four classes of service and they relate to providing PSTN access for emergency, local (7-digit), national, and international dialing.

Figure 5. Relationship of Calling Search Spaces to Partitions

Calling Search Space	Route Partition 1	Route Partition 2	<b>Route Partition 3</b>		
CSS_Base	PAR_Base			7	Emergency Dialing
CSS_LocalPSTN	PAR_PSTN_Local			7	Local Dialing
CSS_NationalPSTN	PAR_PSTN_Local	PAR_PSTN_National		7	National Dialing
CSS_InternationalPSTN	PAR_PSTN_Local	PAR_PSTN_National	PAR_PSTN_Intl	7	International Dialing

With RDM, all of the devices are configured with the CSS\_Base Calling Search Space through auto-registration. 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, national, and international dialing capabilities.

#### Figure 6. Calling Search Space



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 all on-net numbers.

#### **Local Route Groups**

The Local Route Group feature in Unified Com¬munications Manager provides decoupling of the PSTN gateway location from the route patterns that are used to access the gateway. This allows a "Local Route Group" to be bound to a provisioned route group differently based on the Local Route Group device pool setting of the originating device. Therefore, devices such as phones from different locales can use identical route lists and route patterns, but Cisco Unified Communications Manager selects the correct gateway(s) for their local end. UC RDM uses this feature to assign a specific route group to each device pool of each site such that each site is configured with a single SIP Gateway that is configured in a Route Group (one for each site). The Route Group is then associated with the Device Pool (one for each site) via the Local Route Group setting. This simplifies the process of provisioning where a single set of route patterns are configured all pointing to the "Local Route Group," which instead of using a specific route group, redi¬rects Unified Communications Manager to use the Local Route Group setting from the Device Pool of the calling device. When a call is made from a device that matches the route pattern, Unified Communications Manager uses the Local Route Group device pool to set that device to determine the actual route group, and this will always select the local SIP Gateway by default.

#### Figure 7. Route Assignment



#### Survivable Remote Site Telephony (SRST)

In a centralized Cisco Unified Communications Manager environment, when IP phones lose connectivity to Cisco Unified Communications Manager because the WAN is down or the application is unreachable, IP phones in remote branch offices or teleworker homes lose call-processing capabilities. The SRST feature provides basic IP telephony backup services so that IP phones can fall back to the local router at the remote site when connectivity is lost to make calls within the site and out the local IOS gateway to the PSTN.

In UC RDM, Survivable Remote Site Telephony (SRST) is used to backup the remote sites in case of WAN outage.

#### **Device Mobility**

UC RDM uses a feature called Device Mobility which allows Unified Communications Manager to determine if the IP phone is at its home or a roaming location. Unified Communications Manager 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 Communications Manager then uses these dynamically allocated settings for call routing, codec section, media resource selection, and so forth.

In RDM, this feature is used primarily to reduce the configuration on the devices themselves by not requiring device-specific configuration of many parameters that are instead configured at a site level and dynamically applied based on the subnet the device is attached to. This allows for a quick and less error-prone deployment because the Administrator does not have to configure each phone individually based on their site/location or ensure the phone is at the correct location.

#### **Extension Mobility**

RDM is provisioned utilizing the Cisco Extension Mobility (EM) feature, enabling users to configure a Cisco Unified IP phone as their own, either temporarily or permanently based on the agency requirements. The EM feature dynamically configures a phone according to the authenticated user's device profile. The Rapid Deployment Method provisions users with User Device Profiles that are part of EM enablement. Users then log into an IP phone using their username and PIN and their profile gets uploaded to the IP phone. Allowing a user to log into a phone alleviates the need for device-to-user association during user provisioning. This saves time in user provisioning and deployment while simultaneously allowing the benefit of Extension Mobility.

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. This can be enabled so that EM is used uniquely for IP phone deployment, but not as a feature to be used in the deployment. By default, the RDM configuration allows for users to log out of the IP phone, which enables EM for both IP phone deployment and user feature functionality.

#### **Media Resources**

Media Resources have been provisioned as part of the procedure for every site to ensure branch sites utilize their local conference bridges and avoid unnecessary voice traffic over the WAN circuit. The naming of the conference bridges within the ISR needs to match those provisioned by RDM.

#### **Unified CM Reference Architecture**

The Unified CM architecture includes:

- Two Unified Communications Manager appliances configured for 1:1 call processing redundancy allowing a single Unified Communications Manager to assume the call processing load in case of a Unified Communication Manager appliance failure or system maintenance.
- One Unity Connection server configured for simple voice messaging without redundancy. Another Unity Connection server can be configured for voice messaging application redundancy as an added advanced feature; however, this is not part of the Rapid Deployment Method architecture.

#### **Call Admission Control**

The default design is provisioned for a hub-and-spoke topology where each remote site is connected to the HQ over a bandwidth-constrained widearea network. The RDM design has been set to use locations-based Call Admission Control and each site (or location) is configured to allow for up to two calls to or from the remote site. Between sites, devices are configured to use g.729 as the default voice codec running at 24 KB per call and each site (location) will allow up to two such intersite calls (48 KB total) to/from remote each site. Call Admission Control is not calculated for calls to/from the central site (HQ). It's expected that as long as the spokes are provisioned for Call Admission Control, the hub will not be oversubscribed. This is the case for hub-and-spoke topologies; however, for MPLS-based networks, the HQ site configuration will need to be modified to provide correct Call Admission Control.

### 🔵 Tech Tip

Intrasite calls are configured to use g.722 (80 Kbps) and are configured to allow an unlimited number of calls within the site (location).

Please see <u>www.cisco.com</u> for further information on Unity Connection Active/Active High Availability.

Further details can be found in the Unified Communications SRNDs on <u>www.cisco.com</u>.

# The Rapid Deployment Method

The following procedures allow for the parallel installation of both Cisco Unified Communications Manager nodes and Cisco Unity Connection.

Please note, however, that at certain points of the installation process, some steps must occur prior to proceeding with others. In order to save time, the software installation can also proceed in parallel with running the Rapid Deployment Method Customization Tool (RDMCT) but certain RDMCT steps require access to the CUCM admin.

#### Process

Configuring the Cisco Unified Communications Manager

- 1. Install the Platform
- 2. Configure the Server and the Site
- 3. Configure User and Device Profiles
- 4. Deploy Unity Connection
- 5. Deploy Phones

Before you begin the configuration procedures, make sure you meet the following prerequisites:

- Configure the Cisco Unified Communications Manager and Cisco Unity Connection host names (cucm1, cucm2, and cuc1) in DNS prior to installation.
- Obtain License Files from the licensing system prior to installation of Cisco Unified Communications Manager and Cisco Unity Connection.
- · Obtain the associated files for this installation method.
- Lightweight Directory Access Protocol (LDAP) integration with Microsoft's Active Directory.
- Manager Distinguished Name (Read Access required)
- Password

- User Search Base (for example: Us¬er's Container in Domain cisco.com is cn=users,dc=cisco,dc=com)
- Host Name or IP address and port number
- 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.
- · Install an archive program for tar files on the PC used for administration.
- DHCP option 150 in the DHCP Scopes have been defined to use the IP addresses of cucm1 (primary) and cucm2 (secondary), or conversely, for redundancy and load balancing.

### 🔵 Tech Tip

Please see <u>www.cisco.com</u> for further information on Unity Connection Active/Active High Availability.

Further details can be found in the Unified Communications SRNDs on <u>www.cisco.com</u>.

The user-provisioning capabilities of this guide require an IP phone that supports IP phone services. All users imported will have the default PIN '12345'

#### Procedure 1

Install the Platform

**Step 1:** Physically install the server and attach the monitor, keyboard, and network.

Step 2: Insert Cisco DVD into the DVD drive.

Step 3: Power the server ON and it will boot from DVD.

**Step 4:** The option for Media Check will be presented, press **OK** if this is the first time this DVD has been used or to ensure its integrity.

**Step 5:** After the Media Check has completed and it passes, it will allow you to select **OK** to continue installation. If not, it will prompt for another DVD.

Step 6: Setup will ask to Continue installation, select Continue.

Step 7: The license agreement is displayed. If you agree to the terms, select Agree to continue installation.

**Step 8:** Depending on the MCS platform, two or three products are presented for deployment. Choose the first option for both Cisco Unified Communications Managers servers and select **OK**.

	Product Deployment Selection
Selec	t the product or product suite to be installed:
( ) (	isco Unified Communications Manager
()	isco Unity Connection
()	isco Unified Communications Manager Business Edition
	OK

Step 9: Select Yes to proceed with installation on the Proceed with Install page.

Step 10: Select Proceed on the Platform Installation Wizard page.

Step 11: Select No on the Apply Patch page.

Step 12: Select No on the Import Windows Data page.

Step 13: Select Continue on the Basic Install page.

Step 14: Select the time zone in which the appliance is installed and select OK.



**Step 15:** Select **Yes** on the Auto Negotiation Configuration page to enable Auto NIC speed and duplex.

**Step 16:** Select **No** on the MTU Configuration unless specifically required to change.

Step 17: Select No on the DHCP Configuration page.

**Step 18:** Enter the required host name, IP address, IP mask, and GW address on the Static Network Configuration page.

- CUCM1 for the First Node (Publisher)
- CUCM2 for the Second Node (Subscriber)

	Static Network Configuration
Host Name	cucm1
IP Address	192.168.28.28
IP Mask	255.255.255.8
GW Address	192.168.28.1

Step 19: Select Yes on the DNS Client Configuration page.

**Step 20:** Enter the primary and optional secondary DNS server IP addresses and the domain, then select **OK**.

	nt Configuration
Primary DNS	192.168.28.10
Secondary DNS (optional)	
Doma i n	cisco.com
ОК	Back

**Step 21:** Enter the username and password that will be used for the Platform Administration account on the Administrator Login Configuration page and then select **OK**.



The password must start with an alphabetic character, be at least 6

characters long, and contain alphanumeric characters, hyphens, or underscores. Step 22: Complete the details on the Certificate Information page that will be used to generate the certificate used for secure communications, then select OK.

	- Certificate Information
Enter informati generate securi	on about your organization. This is used to ity certificates for this mode.
Organization	Clsco Systems Inc
Unit	Unified Communications Group
Location	San Jose
State	California
Country	Ukraine United Arab Emirates #
	United States
	Dack He 1p

**Step 23:** If this is the first node (Publisher) installation, select **Yes** on the First Node Configuration page and skip to Step 28.

**Step 24:** For the second node (Subscriber) installation, select **No** on the First Node Configuration page.



**Step 25:** Select **OK** on the First Node Configuration warning page to acknowledge this as the second node installation.

Step 26: Select Yes on the Network Connectivity Test Configuration page.

**Step 27:** Enter the host name, IP address, and security password details (entered previously on the Database Access Security Configuration page) for the first node (Publisher) installation and select **OK**.

First	Node Access Configu	ration
Connectivity to Fi	rst Node:	
Host Name	cucm1	
IP Address	192.168.28.20	
Security Password	****	
Confirm Password	******	
OK	Back	Help

<Tab>/<Alt-Tab> to move between elements. <Space> or <Enter> to select.

**Step 28:** On the Network Time Protocol Client Configuration page, select either:

- Yes, and then enter the IP address or host names for up to 5 NTP servers and select OK. NTP is the recommended option or
- No, and set the Hardware Clock Configuration to the correct time and date, then select OK.

**Step 29:** If this is the first node (Publisher), enter a security password in the Database Access Security Configuration page, then select OK. This password will be used during the second node installation process. If this is the second node (Subscriber), this step will be skipped.

**Step 30:** Select **No** on the SMTP Host Configuration page. Mail notifications can be configured at a later stage if desired.

**Step 31.** Enter the username and password you wish to use for the Cisco Unified Communications Manager Administration account on the Application User Configuration page, and then select **OK**. For example: CUCMAdmin

## **Tech Tip**

The Application User Name is case sensitive when authenticating against the Cisco Unified Communications Manager Administration pages.



**Step 32:** Select **OK** on the Platform Configuration Confirmation page to install the software.

**Step 33:** After the software has finished loading, the following screen will appear:

If this is the second node installation, skip to Step 45.

Cisco Unified Communications Manager 7.1.1.39161-9 cucm1 login: \_

**Step 34:** Using another computer, access the Cisco Unified Communications Manager Administration Interface at <u>http://cucm1</u>. Select the **Cisco Unified Communications Manager Administration** link in the center of the page.

**Step 35:** Enter the username and password you entered for the Application User Configuration earlier and select the **Login** button.

## **Tech Tip**

You may receive a warning about the website's security certificate, ignore and continue to the page.

Step 36: Select System > Licensing > License File Upload.



Step 37: Select the Upload License File button, browse to the license file obtained prior to installation, then select the Upload button. This may take a few minutes to complete.

**Step 38:** Log in to the Cisco Unified Serviceability Interface using the **Navigation** drop-down list and select the **Go** button.



Step 39: Select Tools > Service Activation.

Step 40: Select CUCM1 from the drop-down list and click the Go button.

Step 41: Select the check box Check All Services and select Save. Select OK on any warning pop-up. Activating services may take a few minutes to complete.



You may safely disable the following services if they are not planned for utilization:

- Cisco Messaging Interface
- Cisco DHCP Monitor Service
- Cisco TAPS Service
- Cisco Dialed Number Analyzer

		CUCMAdmin About Logo
Marm	- Iraca - Togis - Samo - Haip -	
ervio	ce Activation	Related Links: Control Center - Feature Services 👻 🛛
	Save 🧬 Set to Default 🔇 Refresh	
Stat	us date Operation Successful	
Sele	et Server	
Го	heck All Services	
CM S	ervices	
	Service Name	Activation Status
P	Cisco CallManager	Activated
M	Cisco Intp	Activated
	Cisco Messaging Interface	Deactivated
P	Cisco Onined Mobile Voice Access Service	Activated
5	Cisco CTIManager	Activated
D.	Cisco Extension Mobility	Activated
R	Cisco Extended Functions	Activated
Г	Cisco Dialed Number Analyzer	Deactivated
Г	Cisco DHCP Monitor Service	Deactivated
сті 5	iervices	
	Service Name	Activation Status
M	Cisco CallManager Attendant Console Server	Activated
R	Cisco IP Manager Assistant	Activated
A	Cisco WebDialer Web Service	Activated
CDR	Services	
	Service Name	Activation Status
M	Cisco SOAP - CDRonDemand Service	Activated
R	Cisco CAR Web Service	Activated
Data	base and Admin Services	
	Service Name	Activation Status
P	Cisco AXL Web Service	Activated
M	Cisco UXL Web Service	Activated
M	Cisco Bulk Provisioning Service	Activated
Г	Cisco TAPS Service	Deactivated
Perfo	rmance and Monitoring Services	
	Service Name	Activation Status
R	Cisco Serviceability Reporter Cisco CaliMananer SNMP Service	Activated
Secu	rity Services	Artivation Status
V	Cisco CTL Provider	Activated
7	Cisco Certificate Authority Proxy Function	Activated
Direc	tory Services	
	Service Name	Activation Status
	Ciara DirCiara	1 diaman d
¥	CISCO DI SYIK	ACLIVACEC

Step 42: Log in to the Cisco Unified CM Administration using the Navigation drop-down list and select Go.

abab	Cisco Unified CM Administration				Navigation	Cisco Unified CM Administration	٠	Go
CISCO	For Cisco	Unified Communic	ations Solut	ions		Cisco Unified Serviceability		out
System •	Call Routing 👻	Media Resources 👻	Voice Mail 🔻	Device -	Application -	Disaster Recovery System		n 🕶
						Cisco Unified Reporting		

Step 43: Select System > Server and select Add New.

cisco	Cisco Unified CM Administration For Cisco Unified Communications Solutions		Navigation	Cisco Unified CM Administration - Go CUCMAdmin About Logout
System -	Call Routing  Media Reso	urces 👻 Voice Mail 👻 Device 👻	Application -	User Management 👻 Bulk Administration 👻
Cisco L Cisco L Phone I Date/Ti	Jnified CM Jnified CM Group NTP Reference me Group	Administration		

Step 44: Enter the host name (CUCM2) of the Subscriber and select Save. When the Subscriber has been added, continue the second node installation from Step 24.

cisco Unified CM Administration For Cisco Unified Communications Solutions				Navigatio	vigation Cisco Unified CM Administration - Go				
System -	Call Routing +	Media Resources 👻	Voice Mail 👻	Device -	Application +	User Management 👻	Bulk Administration +	Help -	
Server Co	onfiguration					R	elated Links: Bad	k To Find/List	- G0
Save									
- Status -	is: Ready								
- Server I	Information - e/IP Address*	cucm2							
IPv6 Nam	e				1				
MAC Addr Descriptio	n ess	Communications Ma	anager 2						
- Save									
(i) ×- in	dicates require	ed item.							

Step 45: After the second node (Subscriber) has completed the software installation, log in to the Cisco Unified Serviceability Interface using the **Navigation** drop-down list and select the **Go** button.



Step 46: Select Tools > Service Activation.

Step 47: Select CUCM2 from the drop-down list and click the Go button.

Step 48: Select the checkbox Check All Services and select Save. Select OK on any warning pop-up. Activating services may take a few minutes to complete.

### Tech Tip

You may safely disable the following services if they are not planned for utilization:

- Cisco Messaging Interface
- Cisco DHCP Monitor Service
- Cisco AXL Web Service
- Cisco UXL Web Service
- Cisco Dialed Number Analyzer

Cisco Unified Serviceability	Navigation Cisco Unified Serviceability +
For Cisco Unified Communications Solutions	CUCMAdmin About Logo
sterm • Irace • Topts • Samp • Help •	
ervice Activation	Related Links: Control Center - Feature Services 👻 🕴
🔜 Save 🤣 Set to Default 🔇 Refresh	
Status Status : Ready	
Select Server erver* cucm2 • Go	
Check All Services	
CM Services	
Service Name	Activation Status
Cisco CallManager	Activated
<ul> <li>Cisco Tftp</li> </ul>	Activated
Cisco Messaging Interface	Deactivated
Cisco IP Voice Media Streaming App	Activated
Cisco CTIManager	Activated
Cisco Extension Mobility	Activated
Cisco Extended Functions	Activated
Cisco Dialed Number Analyzer	Deactivated
Cisco DHCP Monitor Service	Deactivated
CTI Services	
Service Name	Activation Status
Cisco CallManager Attendant Console Server	Activated
Cisco IP Manager Assistant	Activated
Cisco WebDialer Web Service	Activated
Database and Admin Services	
Service Name	Activation Status
Cisco AXL Web Service	Deactivated
Cisco UXL Web 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
Save Set to Default Refresh	
Sare Verto Delaut	

#### Procedure 2

**Configure the Server and the Site** 

**Step 1:** Unzip RDMCT Package to a folder and double click on **RDMCT** (RDMCT.exe) provided as part of this package.

**Step 2:** If you agree to the Terms of Use, select **Accept** to move ahead. Otherwise, select Cancel to exit.

Step 3: Are you configuring for Cisco Unified CM Business Edition? Select No.

Step 4: In "Select the configuration phases you would like to perform" section, uncheck the configuration phase you would like to skip and select Next.

Are you configuring for Cisco Unified CM Business Edition?*	No
Select the configuration phases you would like to perform (Mu	res No Isconouse acceascone)
Cisco Unified CM - User Device Profile Configuration Phase	ie in the second se
Cisco Unified CM - User Configuration Phase	

**Step 5:** Enter the server name of the Publisher and Subscriber configured during the installation.

- CUCM1 for the first node (Publisher)
- CUCM2 for the second node (Subscriber)



Server names need to be exactly the same (including case) as configured during installation without the domain name.

**Step 6:** Enter the name of the headquarter/central site (up to 6 alphanumeric characters) where all the servers are hosted.

**Step 7:** Enter the number of remote sites that you will have in your deployment (between 0 and 20).

Step 8: Check the Active Directory check box and select Next.

#### **General Information**

What is the server name of the first CUCM node? *	CI ICM1
What is the server name of the second CUCM node? $\ensuremath{^*}$	CUCM2
What would you like to call the headquarters site?*	HQ
How many remote sites are you supporting?	1
Check if you have an integrated Active Directory	<b>~</b>

**Step 9:** To change the site name, highlight the **Site Name** cell and type in the desired name (up to 6 alphanumeric characters). Enter the subnet information for each site along with the IP Address of the SIP gateway, which is connected to the PSTN and select **Next**.

#### Site Information

Enter the following site information for each site:

	Site Name:		S	ubnet:		Subnet Mask:		IP Addre G	ess of the ateway:	e SIP
1	HQ	10	. 64	. 89	. 0	27	10	. 64	. 89	. 10
2	Site01	10	. 64	. 89	. 33	27	10	. 64	. 89	. 40

Step 10: Enter the LDAP Directory Configuration and then select Next.

- · LDAP Manager Distinguished Name Example: Administrator@cisco.com
- LDAP User Search Base Example: cn=users,dc=cisco,dc=com
- · Select an attribute from the Phone Number drop-down list
- Host name or IP address for server of the LDAP server
- In the case where a backup of the LDAP server is required, add up to 2 servers or IP addresses.

### Tech Tip

If configured, the phone number field populates the user's Telephone Number field in the Unified CM directory. This field is synchronized from Active Directory from either the ipPhone attribute or the telephoneNumber attribute, whichever is selected. Typically the telephone-Number attribute contains the user's E.164 formatted number while 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.

#### LDAP Directory Configuration

LDAP	<sup>,</sup> Directory Information P manager distinguished name: *	Administrator@cisco.com
LDA	P user search base: *	CN=Users, DC=cisco, DC=com
Phor	ne number: *	telephoneNumber 🛛 😪
	a the import operation is complete you must go to the P password 2 Sorver Information	telephoneNumber DAF <mark>ipPhone</mark> ion page in CUCM to configure the
	Host name or IP address for server (up to 3):*	LDAP Port.*
1)*	AD cisco com	389
2)	backupAD.cisco.com	389
3)		209

**Step 11:** Select the check box next to **Use LDAP Directory Configuration** to use the same settings for LDAP authentication as provided in the LDAP Directory configuration screen and select **Next**. This will enable the authentication of users through LDA.P

# Tech Tip

Once the import operation is complete you must configure the password in the CUCM admin page (System > LDAP > LDAP Authentication). This is performed in Step 30 of this process.

#### LDAP Authentication Configuration

☑ Use LDAP directory information

Step 12: In the Unified CM Dial-Plan screen leave the default settings, and select Next.

**Step 13:** The Overview page will provide a summary of all inputs entered into RDMCT up to this point. If all information shown is correct select **Configure**, otherwise, select **Back** to correct the information

**Step 14:** After **Configure** is selected a popup message confirming the creation of the CUCM user device profile configuration files will be displayed, select **OK**.

**Step 15:** The Server and Site Configuration Phase Complete page will provide path details to the location of configuration files.

The CUCM Server and Site Configuration Phase of RDMCT is now complete and if you have selected the Show Configuration Files check box, RDMCT will open the output directory where the output files are stored. The procedure will continue with importing these configuration files into CUCM.

#### Server and Site Configuration Phase Complete

Creating the Bulk Administration Import file for the Server and Site configuration Phase was successful.

```
The configuration file can be found at

- C:\ I EMP\RDMC I \Output\ConfigurationExport tar
```

A summary of your configuration can be found at: - C:\TEMP\RDMCT\Output\DeviceConfigSummary.txt

Press next to continue to the User and Device Profile Configuration Phase

**Step 16:** Go to http://cucm1.yourdomain.com/ccmadmin (substituting yourdomain. com) and log into Cisco Unified CM Administration on the Publisher using the **Navigation** drop-down. Select **Go**.

dialo	Cisco l	Unified CM A	dministr	ation	Navigation	Cisco Unified CM Administration	Go
System •	Call Routing -	Media Resources -	Voice Mail -	Device -	Application -	Cisco Unified Serviceability Cisco Unified OS Administration Disaster Recovery System	n 🕶
						Cisco Unified Reporting	

Step 17: Select Bulk Administration > Upload/Download Files.

Cisco Unified CM Administration For Cisco Unified Communications Solutions	Navigation Cisco Unified CM Administration V GO CUCMAdmin About Logout
System - Call Routing - Media Resources - Voice Mail - Device	▼ Application ▼ User Management ▼ Bulk Administration ▼ Help ▼
Find and List Files	
Add New	
File	
Find File where Name   begins with    Select item or enter s	Using AND V Find
No active query. Please enter your	r search criteria using the options above.
Add New	

Step 18: Select Add New.

**Step 19:** Browse to the Output folder in the directory where RDMCT is located and select ConfigurationExport\_date and time.tar (Do not extract the tar file).

- Set Select the Target as Import/Export.
- Set Select Transaction Type as Import Configuration.
- Select Overwrite File check box, if it exists.
- · Select Save.

ahah. Cisco Un	ified CM Ad	Iministra	ation	Nav	vigation Cisco Unifie	d CM Administration	₹ G0
CISCO For Cisco Un	nified Communica	tions Soluti	ions		CUCMA	dmin About	Logout
System - Call Routing - I	Media Resources 👻	Voice Mail 🔻	Device •	Application •	User Management 👻	Bulk Administration +	Help 🔻
File Upload Configuratio	'n				Related Links:	Back To Find/List	▼ Go
Save							
Status Status: Ready							
File: *	C:\Users\nobody\	Desktop\Con	figurationE:	kport.tar		Browse	
Select The Target *	Import/Export				-		
Select Transaction Type *	Import Configurat	tion 👻					
Save							

()\*\* If you are trying to upload a file which is already present for a particular transaction, it will be overwritten.

Step 20: Select Bulk Administration > Import/Export > Import.

Cisco Un For Cisco Un	ified CM Adminis	stration olutions	Na	vigation	Cisco Unifie	d CM Administrat	tion 👻 🧕
System - Call Routing - M	ledia Resources 👻 Voice Ma	il - Device -	Application -	User Mar	nagement <del>+</del>	Bulk Administration	Help
File Upload Configuration  Save  Status  Upload successful  Upload the CSV file  File: *  Select The Target *  Select Transaction Type *  Overwrite File if it exist  Save	n Not Selected Not Selected Not Selected •			R	Upload/Dov Phones Users Phones & U Managers// User Devic Gateways Forced Au Client Matte Call Pickup Mobility Region Mat	wrload Files Jsers Assistants er Profiles thorization Codes er Codes Group	•
	_	Export			Import/Exp	ort	+
*- indicates required iten	n.	Import			CUP		
₩** If you are trying to up	load a file which is alrea	Validate Import	t File		TAPS Job Sched Phone Migr	uler aton	,

Step 21: Select the file uploaded in step 19 from the File Name drop-down list and select Next.

abab	Cisco Unified CM Ad	dministra	ation	Navigation Cisco Unified CM Administration 👻 GO					
cisco	For Cisco Unified Communic	ations Soluti	ons	CUCMAdmin About Logout					
System -	Call Routing 👻 Media Resources 👻	Voice Mail -	Device -	Application -	User Management 👻	Bulk Administration	· → Help →		
Import Co	nfiguration								
Next									
- Status - i Statu	s: Ready								
- Select F	ile —								
File Name	Not Selected		-						
- Next	Not Selected ConfigurationExport.tar								
(i) *- in	dicates required item.								

Step 22: Select Select All and select the Override the existing configuration check box and the Run Immediately radio button. Then select Submit.

stem - Call Routing - Media Resources - Voic	e Mail - Device - Application -	User Management 👻 Bulk A	Administration - Help -
port Configuration			
Submt Select Al Clear Al			
Status			
i) Status: Ready			
Archive Information			
ile Name: ConfigurationExport.tar			
Import Configuration			
System Data			
Cisco Unified Communications Manager Group	Device Pool	☑ Location	Phone NTP Reference
Region	SRST	Physical Location	Device Mobility group
LDAP System	Device Mobility Info		
Call Routing Data			
CSS (Class of Control)	Partitions (Class of Control)	Line Group	Route Group
V Hunt List	Route List	I Hunt Pilot	Route Pattern
Media Resources			
Conference Bridge	Media Resource Group	Media Resource Group Li	st
User Data			
Credential Policy Default	Credential Policy		
Device Data			
V Trunk	Phone Services		
Voice Mail Data	CAG 11 11 11 11 11 11 11 11 11 11 11 11 11		
Message Waiting Numbers	Voice Mail Pilot	Voice Mail Profile	Voice Mail Port
Override the existing configuration			
Job Information			
Job Description Import Confid	guration		
Run Immediately     O Run Later	(To schedule and activate this jo	b, use Job Scheduler page.)	

Step 23: Select Bulk Administration > Job Scheduler.

**Step 24:** Select **Find** to list the status of the scheduled jobs. When the status is Completed, select the Job Id link to check details.

- Refresh the page if the job is still running and not yet complete.
- The Job Result Status should be Success for all. Once the Status displays as Completed go to the next step.

Step 25: Select System > Server and select Find.

Step 26: Select CUCM1 and change the host name/IP address from the hostname to the IP address and select Save.

Step 27: Select CUCM2 and change the host name/IP address from the hostname to the IP address and select Save.

Step 28: Select System > LDAP > LDAP Directory and click Find. Select the active directory configured, modify the LDAP password and confirm password, then select Save.

**Step 29:** Select **Perform Full Sync Now** to start the user import process from the directory. Click **OK** on the Pop-up warning window.

Note: Go to User Management > End User and select Find to confirm that all users have been synced from active directory. This process may take a few minutes to complete depending on the number of users synchronized.

**Step 30:** Select **System > LDAP > LDAP Authentication**, modify the LDAP password and confirm password, then select **Save**.

aluda Cisco Unified C	M Administration	Navig	ation Cise	o Unified CM A	dministrat	ion 👻 G
CISCO For Cisco Unified Con	nmunications Solutions			CUCMAdmin	About	Logou
System - Call Routing - Media Resou	urces • Voice Mail • Device •	Application - User M	anagement ·	Bulk Administ	ration 👻 🛛	Help 🔻
LDAP Authentication						
Save						
- Status						
j Status: Ready						
I DAD Authentication for End Up						
Use I DAP Authentication for End Us	lisers					
LDAP Manager Distinguished Name*	Administrator@cisco.com					
LDAP Password*						
Confirm Password*						
LDAP User Search Base*	cn=users,dc=cisco,dc=com		1			
- LDAP Server Information			*	line FEI		
ad.cisco.com	3	89	E SSL			
Add Another Redundant L	DAP Server					
	,					
Save						
*- indicates required item						

Procedure 3

**Configure User and Device Profiles** 

Step 1: Select Bulk Administration > Import/Export > Export.

**Step 2:** Enter a tar file name such as DirectoryUsers and select the **End User** check box within the User Data section.

Step 3: Select the Run Immediately button and select Submit and OK on any warning pop-up window.

Step 4: Select Bulk Administration > Job Scheduler and check the status of the export job submitted.

Step 5: After the Job Status indicates successful completion, select Bulk Administration > Upload/Download Files.

**Step 6:** Select the exported file name (DirectoryUsers\_date and time.tar) created by the export operation and then select **Download Selected**. Save the file.

Include Cisco Unified CM Administration			Navi	Navigation Cisco Unified CM Administr			
cisco	For Cisco Unified Commun	ications Solutions			СИСМА	dmin About	Logout
System - Ca	I Routing - Media Resources -	Voice Mail - Device - Ap	pplication -	User Management	+ Bulk Administrati	ion - Help -	
Find and List	Files						
Add New	Select All Clear All	Delete Selected 🗿 Do	wnload Selec	cted			
- Status							
i 3 record	s found						
-							
File (1	3 of 3)					Rows per Page	100 💌
File (1 -	s of s) e Name + begins with +	Using	a AND 👻	Find		Rows per Page	100 👻
File (1 -	3 of 3) e Name → begins with →	Using Select item or enter search t	g AND 🗸	Find		Rows per Page	100 👻
File (1 -	S of S)	Using Select item or enter search t File Name *	g AND 🗸	Find	Fu	Rows per Page	100 🔻
File (1 -	S of S)	Using Select item or enter search t File Name <sup>*</sup>	g AND 🗸	Find)	Fu nport Configuratio	Rows per Page	100 -
File (1 -	s of 3) e Name v begins with v ConfigurationExport.tar DirectoryUsers_05082009173	Using Select item or enter search t File Name * 3612.tar	g AND - text -	Find In E	Fui nport Configuration xport Configuration	Rows per Page	100 -

**Step 7:** Open the downloaded tar file using an archive program that supports tar format and extract the enduser.csv file for use later.

Step 8: Select Bulk Administration > User Device Profiles > UDP Template and select Add New.

There are 2 options for deploying User Device Profiles. You can either:

- Create a single User Device Profile Template such as a 7975 to deploy for all User Device Profiles.
- Create a User Device Profile Template for each device type (phone model) deployed.

## Tech Tip

Refer to the following documentation describing the phone behavior for a user logging into a device with a User Device Profile that does not match the device type: <u>http://www.cisco.com/en/US/docs/voice\_ip\_comm/cucm/admin/7\_1\_2/ccmfeat/fsem.html#wp1146344</u>.

Step 9: Select the correct phone model from the Device Profile Type dropdown box and select Next.

**Step 10:** Select the Device Protocol as **SCCP** if the Device Protocol dropdown is presented.

**Step 11:** Enter a User Device Profile Template Name (i.e. 7975 Standard Template), select a Phone Button Template from the drop-down and select **Save**.

Step 12: Select Line [1] - Add a New DN.

**Step 13:** Enter a name in the Line Template Name field (i.e. Default Line Template) and for Route Partition select **PAR\_Base**. Also check the **Voice Mail** check boxes for the items in the following figure, to enable forwarding to voice mail correctly, and then select **Save**.

	Voice Mail	Destination	Calling Search Space	•
Calling Search S	pace Activation Polic	Y	Use System Default	-
Forward All	🖾 or		< None >	
Secondary Callir	ng Search Space for I	Forward All	< None >	•
Forward Busy Internal	🗹 or		< None >	•
Forward Busy External	V or		< None >	•
Forward No Answer Internal	♥ or		< None >	•
Forward No Answer External	V or		< None >	•
Forward No Coverage Internal	♥ or		< None >	•
Forward No Coverage External	☑ or		< None >	•
Forward on CTI Failure	🗖 or		< None >	•
Forward Unregistered Internal	☑ or		< None >	•
Forward Unregistered External	☑ or		< None >	•
lo Answer Ring D	ouration (seconds)			
all Pickup Group		None >		

**Step 14:** Select the **Go** button to return to the UDP Template Configuration page, then select **Save**.

• The procedure will now return to the RDMCT to continue with the configuration.



Step 15: From the RDMCT, check only User and Device Profile Configuration Phase and click Next.

Step 16: Assign one or more extension ranges to the headquarters site and each remote site. Enter a 4 digit starting extension in Reserved Extension Range Start and a 4 digit ending extension in Reserved Extension Range End. Click + to add additional start/end extension ranges or click – to remove the unwanted extension ranges. Click Next when complete.

#### **Basic Site Information: Site Directory Number Ranges**

How many remote sites are you supporting?

	Site *	Reserved Extension Range Start	Reserved Extension Range End	Add/Remove Site Extension Range
1	HQ	51000	51199	+
		62050	62099	-
9 2	Sile01	37000	37099	+

Step 17: Click Browse to locate endusers.csv extracted in step 7.



**Step 18:** For each User Device Profile (UDP), populate the Directory Number, External Phone Number Mask, Line CSS, and Line Text Label. Click **Configure**.

#### **User Information**

Path	n of the	e exported 'enduser.r	csv' file: * C:\C	Cisco\RDM-CT\	enduser.csv				Browse
					Import from C ⊻	408555	CSS_Nation 💙	~	7975 🗸 🗸
		Remove User			Set Directory #	Set Phone Mask	Set Line CSS	Set Line Text	Set Device Type
		Device Profile Name *	Description	User ID	Directory Number *	External Phone Number Mask	Line CSS	Line Text Label	Device Туре
	1	User1	User One	User1	3201	408555	CSS_Internati	User One (32	7975
	2	Usei2	Usei Two	Usei2	3202	408555	CSS_Internati	Usei Twu (32	7975
	3	User3	User Three	User3	3203	408555	CSS LocalP	User Three (3	7975
	4	User4	User Four	User4	3204	408555****	CSS_LocalP	User Four (32	7975
•	5	User5	User Five	User5	3205	408555	CSS_National	User Five (32	7975

**Step 19:** After Configure is selected the system will display a confirmation dialog box, click **OK** to generate the list of files that will be used for the rest of the procedure.

### Tech Tip

There are user ID's exported as part of the list which may not need to be configured for User Device Profiles, select those UserIDs from the list and click **Remove Users** to remove them from the list.

Directory Number is made up of the number 8 followed by a two-digit site code, followed by a 4-digit extension (for example, 8001000 pr 8[site] [extension], where 00 is the site code and 1000 is the extension).

External Phone Number Mask is the direct inward dialing (DID) number for the user or a Main Office Number, This will also appear on the Black Stripe at the top of the IP phones display. Enter the phone number mask (eg. 408555XXXX) into the text box and select **Set Phone Mask**.

If you specify a mask of 408555XXXX, an external call from extension 8001234 displays a caller ID number of 4085551234.

Line CSS defines the Class of Restriction or type of numbers the user is allowed to call. The Calling Sear Spaces (CSS) defined during the import process can be viewed under Call Routing > Class of Control > Calling Search Space in the Cisco Unified CM. Administration. Select the Line CSS from the drop-down and click **Set Line CSS**.

Line Text Label is the label that will be displayed on the phone and although it can be any alphanumeric string, it is recommended to have FirstName, LastName, and extension number in parentheses. Select a text label option from the drop-down and click **Set Line Text**. The default is: Description (DirectoryNumber), see below.

Select device type, which is the phone model type (eg. 7975) that will be associated with UDP from the drop-down and click **Set Device Type**.

For each phone model type, there will be a UserDeviceProfiles-xxxx. csv created. For example: UserDeviceProfiles-7975.csv will contain all UDP that use 7975 phones. For UDP that don't have any device type set, they will be put into UserDeviceProfiles.csv. Step 20: Click Finish to close the RDMCT.

 CUCM User and Device Profile Configuration Phase is now completed with RDMCT. If you select Show Configuration Files, RDMCT will open the output folder where the files are stored. Select **Finish** to exit from RDMCT application.

#### **Configuration Complete**

The configuration files can be found at: Z:\CiscoDocs\VSE\_Projects\EOU\wizard\Output

 Use the following file(s) to create UDP in CUCM Device Configuration Phase: - UserDeviceProfiles.csv - UserDeviceProfiles-7960.csv - UserDeviceProfiles-7975.csv

2) Use 'AddUsersToStdCCMGroup.csv' to add users to standard CCM End Users group in CUCM Device Configuration Phase

3) Use 'CUCVoicemailUsers.csv' to update users with 7 digit extensions in Unity Connectoin Deployment Phase

Press finish to exit.

**Step 21:** Go to http://cucm1.yourdomain.com/ccmadmin (substituting yourdomain.com). Log into the Cisco Unified CM Administration page.

# Step 22: Select Bulk Administration > Upload/Download Files and select Add New.

Step 23: Repeat for each UserDeviceProfiles.csv file created by RDMCT:

 Browse to the Output folder in the directory where RDMCT is located and select the corresponding UserDeviceProfiles.csv. Set Select The Target to UDP and Select Transaction Type to Insert UDP – Specific Details. Select Overwrite File check box, if it exists. Then select Save.

Step 24: Repeat for each UDP Template created in step 8.

- Select Bulk Administration > User Device Profiles > Insert UDP.
- Select Insert User Device Profiles Specific Details and in the File Name drop-down, select the file name uploaded in step 23 and the user device profiles template name previously created and matching the phone type of the users being imported.

Step 25: Select Run Immediately and then select Submit.

**Step 26:** Verify the import completes successfully without errors using Bulk Administration > Job Scheduler.

Step 27: Select Bulk Administration > Upload/Download Files.

- · Select Add New.
- Browse to the Output folder in the directory where RDMCT is located and select AddUsersToStdCCMGroup.csv.
- · Set Select the Target as Users.
- · Set Select Transaction Type as Update Users Custom File.
- · Select Overwrite File check box, if it exists.
- · Select Save.

#### Step 28: Select Bulk Administration > Users > User Template.

- · Select Add New.
- For User Template Name, provide a name (eg. UserTemplate).
- For User Group, select Standard CCM End Users from drop-down list.
- · Select Save.

#### Step 29: Select Bulk Administration > Users > Update Users.

- · Select the file uploaded in step 27 for File Name.
- · Select the user template created in step 28 for User Template Name.
- Select the Run Immediately radio button and click Submit.

**Step 30:** After some time (time might vary depending number of users updating), select **Bulk Administration > Job Scheduler**.

Step 31: Select Find to list the status of the scheduled jobs.

- $\cdot\;$  When the Status is Completed, select the Job Id link to check details.
- The Job Result Status should be Success.

Step 32: Select User Management > End User and select a few users to verify that they have the correct Groups Permission Information (Standard CCM End Users).

Step 33: Select System > Application Server.

- Select Add New.
- · Set Application Server Type as Cisco Unity Connection.
- · Select Next.
- In the Name field enter the name of the Cisco Unity Connection Server (ex: CUC1).
- In the IP address field enter the IP address of the Cisco Unity Connection Server.
- Select the Application User Account that you created during installation of the Unified CM (eg. CUCMAdmin) and move the account from Available Application Users to Selected Application Users using the v character.
- · Save.

#### Procedure 4

#### **Deploy Unity Connection**

Step 1: Physically install the server and attach the monitor and keyboard.

Step 2: Insert the Cisco DVD into the DVD drive.

Step 3: Power the server ON and it will boot from the DVD.

**Step 4:** The option for Media Check will be presented, select **OK** if this is the first time this DVD has been used or to ensure its integrity.

**Step 5:** After the Media Check has completed and it passes, it will allow you to select **OK** to continue installation. If not, it will prompt for another DVD.

Step 6: Setup will ask to continue installation, select Continue.

Step 7: The license agreement is displayed. If you agree to the terms, select Agree to continue installation.

**Step 8:** Depending on the MCS platform, two or three products are presented for deployment. Choose the second option for the Cisco Unity Connection, then select **OK**.

	Product Deployment Selection
Select	the product or product suite to be installed:
() Cis	co Unified Communications Manager
() Cis	co Unity Connection
() Cis	co Unified Communications Manager Business Edition
	ок

 ${\rm (Tab}/{\rm (Alt-Tab})$  to move between elements.  ${\rm (Space)}$  or  ${\rm (Enter)}$  to select.

**Step 9:** Select **Yes** to proceed with installation on the Proceed with Install page.

Step 10: Select Proceed on the Platform Installation Wizard page.

Step 11: Select No on the Apply Patch page.

Step 12: Select No on the Import Windows Data page.

Step 13: Select Continue on the Basic Install page.

**Step 14:** Select the time zone in which the appliance is installed and select **OK**.



**Step 15:** Select **Yes** on the Auto Negotiation Configuration page to enable Auto NIC speed and duplex.

**Step 16:** Select **No** on the MTU Configuration unless specifically required to change.

Step 17: Select No on the DHCP Configuration page.

**Step 18:** Enter the required host name, IP address, IP mask and GW address on the Static Network Configuration page.

• Select cuc1 for the Unity Connection Server.

	- Static Network (	Configuration  -	
Host Name	cuc1		
IP Address	192.168.28.22		
IP Mask	255.255.255.0		
GW Address	192.168.28.1		
	Baci		e1p

Step 19: Select Yes on the DNS Client Configuration page.

**Step 20:** Enter the primary and optional secondary DNS server IP addresses and the domain, and then select **OK**.

DNS Cli	ent Configuration
Primary DNS	192.168.28.10
Secondary DNS (optional	)
Domain	cisco.com
OK	Back

**Step 21:** Enter the username and password that will be used for the Platform Administration account on the Administrator Login Configuration page and then select **OK**.



The password must start with an alphabetic character, be at least 6 characters long, and contain alphanumeric characters, hyphens, and underscores.

**Step 22:** Complete the details on the Certificate Information page that will be used to generate the certificate used for secure communications, then select **OK**.

generate secu	urity certificates for this mode.	
Organizatio	on Cisco Systems Inc	
Unit	Unified Communications Group	
Location	San Jose	
State	California	
Country	Ukraine	
	United Hrab Emirates United States	

Step 23: If this is the first node that is being installed, select Yes.

Step 24: On the Network Time Protocol Client Configuration page select:

- The recommended option is to select **Yes** and then enter the IP address or host names for up to 5 NTP servers and select **OK**.
- No and set the Hardware Clock Configuration to the correct time and date, then select OK.

**Step 25:** Enter a security password in the Database Access Security Configuration page, and then select **OK**.

• Keep this password safe for the future should another Cisco Unity Connection node be added to this first to form a cluster.

**Step 26:** Select **No** on the SMTP Host Configuration page. You can configure mail notifications at a later stage if desired.

**Step 27:** Enter the username and password you wish to use for the Cisco Unity Connection Administration account on the Application User Configuration page, select **OK**. For example: CUCAdmin.

Cisco Unif	ied Communications M	anager 7.1.1.39161-5 cation User Configur	eation
	The Application Us log into the Applic Application User U Application User P Confirm Application	er username and pass cation administrativ sername CUG assword an n User Password an	sword are used to be webpage(s). CHMdmin HARANA HARANA
		Back	Help

**Step 28:** Select **OK** on the Platform Configuration Confirmation page to install the software.

**Step 29:** After the software has finished loading, the following screen will appear:

cucl login: _	Cisco Unity	Connection	7.1.1.39161-9
	cucl login:	<u> </u>	

**Step 30:** Using another computer, access the **Cisco Unity Connection Administration** Interface. Navigate to http://cuc1.yourdomain.com in a browser (substituting yourdomain.com). Select the Cisco Unity Connection Administration link in the center of the page. **Step 31:** Enter the username and password you entered for the Application User Configuration earlier and select the **Login** button.



Step 32: Select System Settings > Licenses and select Add New.

alula Cisco Unity	Connection Administration	Navigation Cisco Unity Connection Administration - Go		
CISCO For Cisco Unified	Communications Solutions	CUCAdmin Feedback About Logo		
Unity Connection	Licenses	Licenses		
Users		Related Links Kun License Report • Gg		
Class of Service	License Refresh Help			
Templates				
Contacts	Status			
<ul> <li>Distribution Lists</li> </ul>	No licensing warpings or errors exit	iet .		
Call Management				
Message Storage				
Networking	License Files			
Dial Plan	Install Selected Delete Sele	Add New		
System Settings	(			
-General Configuration	I Installed	d File Name		
Cluster	Yes Yes	CUCdemp.lic		
-External Services				
Authentication Rules	Install Selected Delete Sele	acted Add New		
Roles				
Restriction Tables				
Licenses				
Schedules				
Holiday Schedules				
-Global Nicknames				
Subject Line Formats				
-Attachment Descriptions				
Enterprise Parameters				
Service Parameters				
Plugins				
-Fax Server				
E LDAP				
SMTP Configuration				
E Advanced				
Telephony Integrations				
FI Tools				

**Step 33:** Using the **Browse** button, locate the license file obtained prior to installation and select **Add**.

Step 34: Select the check box next to the loaded license file, uncheck the CUCdemo.lic license, and select Install Selected. Close the confirmation pop-up window.

Log in to the Cisco Unified Serviceability Interface using the Navigation drop-down list and select the **Go** button.

ahaha	<b>Cisco Unity Connection Administration</b>	Navigation	Cisco Unified Serviceability	Go
cisco	For Cisco Unified Communications Solutions	α	Cisco Unified Serviceability Cisco Unified OS Administration Cisco Unity Connection Administration Cisco Unity Connection Serviceability Disaster Recovery System	Off

Step 35: Select Tools > Service Activation.

Step 36: Select the Check All Services check box and select Save. Select OK on any warning pop-up.

**Step 37:** Select Cisco Unity Connection Administration from the Navigation drop-down list and select the **Go** button.

Step 38: Select Unity Connection > Telephony Integrations > Phone System.



Step 39: Select the default available phone system—PhoneSystem.

**Step 40:** Select the **Go** button on the Related Links to Add Port Group for phone system.

Cisco Unity	Connection Administration	Navigation Cisco Unity Connection Administration • Go CUCAdmin Feedback About Log Off
Unity Connection	Phone System Basics (PhoneSystem)	Search Phone Systems ) Phone System Basics (PhoneSystem)
Cose of Service     Templates     Contacts     Contacts     Call Management     Massace Scenae	Phone System Edit Refresh Help Save: Delete Previous bext Status At the phone system cannot take calls until a port or	pup is set. Use the Related Links to add a port group.
Networking     Dial Plan     System Settings	Phone System Phone System Name* Phone System	

Step 41: In the New Port Group page, enter the following information, then select Save.

- Device Name Prefix field = CiscoUM1-VI
- MWI On Extension = 8009999
- MWI Off Extension = 8009998
- IP Address or Host Name = IP Address or Host Name of the Subscriber (CUCM2)

#### Step 42: Select Edit > Servers.

cisco Unity Conr Cisco For Cisco Unified Comm	nection Administration unications Solutions	Navigation Cisco Unity Connection Administration 👽 GO unityadmin Feedback About Log Off
Class of the second secon	Port Group Baskes (PhoneSystem-1)         Port Group Edit Refresh Help         Sove Dei         Port Group Daskes (PhoneSystem-1)         Port Group Edit Refresh Help         Sove Dei         Port Group Daskes (PhoneSystem-1)         Port Group Daskes (Phone Network)         Maximum Concurrent Requests (Phone	unityadmin Feedback About Log Off Search Port Groups + Port Group Basics (PhoneSystem-1) Related Links Add Ports 🛛
<ul> <li>□ Tools</li> <li>─ Import Users</li> <li>─ Synch Users</li> <li>─ Task Management</li> <li>─ Bulk Administration Tool</li> </ul>	Fields marked with an astensk (*) are required.	

**Step 43:** Select **Add** in the Cisco Unified Communications Manager Servers section to add a new row. Enter the following information:

• Order = 1

• IP Address or Host Name = cucm1.cisco.com

**Step 44:** Select **Add** in the TFTP Servers section to add a new line. Enter the following information:

- Order = 0
- IP Address or Host Name = Publishers IP address or host name (cucm1)
- Change the existing entry to Order = 1

#### Step 45: Select Save.

dit Servers			Searc	ch Port Groups > Port Group Basics (PhoneSy	stem 1
Port Group	Edit Refresh Help		_	Related Entry entry configuration	
Sava					
Save Cisco Unifi	ed Communications Manager Serv	ers			
Save Cisco Unifi Delete	ed Communications Manager Serv	ers			
Save Cisco Unifi Delete	ed Communications Manager Serv selected Add IP Address or Host Name	Port	TLS Port	Server Type	
Save Cisco Unifi Delete	ed Communications Manager Serv selected Add r IP Address or Host Name cucm2.cisco.com	Port	TLS Port 2443	Server Type Cisco Unified Communications Manager	•

Reconnect to a Higher-order Cisco Unified Communications Manager When Available

		Order		IP Address or Host Name	
1	0		cucm1.cisco.com		
1	1		cucm2.cisco.com		

Save

**Step 46:** Select **Edit > Codec Advertising** and move iLBC from Unadvertised Codecs to Advertised Codecs using ^.

Edit Codec Adverti	sing	Search Port Groups 🕨 Port Group Basics (PhoneSystem-1) Codec Adv	Edit ertising
Port Group Edit	Refresh	Help	
Save			
Status	tem canno	ot take calls if it has no ports. Use the Related Links to add por	rts.
Codec Advertising	3		
Advertised Codecs	G.711 G.729 iLBC	mu-law	
	<u>I</u>	<b>∧ ∨</b>	
Unadvertised Codec	s		
	G.711 ( G.722	a-law	
Save			
Fields marked with	an asteris	k (*) are required.	

Step 47: Select Save.

Step 48: Select Telephony Integrations > Port. Select Add New.

**Step 49:** Enter the licensed number of ports in Number of Ports and select **Save**.



Step 50: Select Telephony Integrations > Port Group and select PhoneSystem-1.

Step 51: If Reset Status is Reset Required, select Reset.

Step 52: Select Templates > User Templates and select the voicemailusertemplate template.

Step 53: Select Edit > Change Password and select Voice Mail in the Choose Password drop-down. Enter a default PIN for accessing voice mail in password and confirm password, then select Save. Step 54: Select System Settings > LDAP > LDAP Setup, select the Enable Synchronizing from LDAP Server check box, and select Save.

DAP Setup		LDAP Setup
LDAP Setup Refresh Hel	p	
– Status –		
<li>Update successful</li>		
Save		
Save	9	
Save – LDAP System Information V Enable Synchronizing fro	m	
Save - LDAP System Information C Enable Synchronizing fro LDAP Server Type*	m m LDAP Server Microsoft Active Directory	

Fields marked with an asterisk (\*) are required.

Step 55: Select System Settings > LDAP > LDAP Directory Configuration, and then select Add New.

- LDAP Configuration Name (for example: Active Directory)
- LDAP Manager Distinguished Name
- LDAP Password
- · LDAP User Search Base
- Host Name or IP Address for Server and LDAP Port of the LDAP server

### 🔵 Tech Tip

Ensure the attribute selected from the Phone Number drop-down list matches the attribute selected from the Phone Number drop-down list inside RDMCT as in step 10 of the Server and Site Configuration Phase.

Step 56: Select Save.

Step 57: Select Perform Full Sync Now and select OK on the pop-up window.

DAP Directory Configuration			Find and List LDA	P Directory Configurations 🕨	LDAP Directory Configurati
DAP Directory Configuration Refre	esh Help				
Save					
Status					
i Status: Ready					
LDAP Directory Information	200			·	
DAP Configuration Name*	Active Direct	ory			
DAP Manager Distinguished Name*	Administrato	r@cisco.com			
LDAP Password*					
Confirm Password*					
LDAP User Search Base*	cn=users,dc	=cisco,dc=com			
LDAP Directory Synchronization	Schedule -				
Perform Sync Just Once					
Perform a Re-sync Every"	7	DAY	•		
Next Re-sync Time (YYYY-MM-DD hh	:mm)* 2009-	05-27 00:00			
	57 57				
User Fields To Be Synchronized Cisco Unified Communications Manag	er User Fields	LDAP User Fields	Cisco Unified Com	munications Manager User Fiel	ds LDAP User Fields
User ID		sAMAccountName	First Name		givenName
Middle Name		middleName 👻	Last Name		sn
Manager ID		manager	Department		department
Phone Number		telephoneNumber +	Mail ID		mail 👻
LDAP Server Information	Server*			LDAP Port* Use SSL	
ad.cisco.com				389	
Add Another Red	undant LDA	PServer		Production and a second second	
annound and a second se					
Envir					

Step 58: Select System Settings > LDAP > LDAP Authentication.

Step 59: Select Use LDAP Authentication for End User check box, and then enter:

- · LDAP Manager Distinguished Name
- LDAP Password
- · LDAP User Search Base
- Host Name or IP Address for Server and LDAP Port of the LDAP server.

#### Step 60: Select Save.

DAP Authentication			LDAP Authenticat
DAP Authentication Refresh He	ip		
Save			
Chabur			
Status: Ready			
LDAP Authentication for End Us	ers		
Use LDAP Authentication for End	Users		
LDAP Manager Distinguished Name*	Administrator@cisco.com		
LDAP Password*	•••••		
Confirm Password*			
LDAP User Search Base*	cn-users,dc-cisco,dc-com		
LDAP Server Information Host Name	e or IP Address for Server*	LDAP Port*	Use SSL
ad.cisco.com		389	
Add Another Redundant Ll	DAP Server		
Save			
Save			
ields marked with an asterisk (*) are	e required.		

Step 61: Select Tools > Import Users and select LDAP Directory in the Find End Users In drop-down list.

#### Step 62: Select Find



**Step 63:** Select **voicemailusertemplate** in the Based on Template dropdown list. **Step 64:** Select the users that require a voice messaging mailbox, and then select **Import Selected**. Do not use Import All.

-Import Users -Synch Users	Based on Template voicemailusertemplate
-Task Management -Bulk Administration Tool	Directory Search Results
-Bulk Edit Utility -Custom Keynad Mapping	Import Selected Import All 25 • Rows Per Page

Step 65:. Go to Tools > Bulk Administration Tool.

**Step 66:** In the right hand pane under Select Operation, select the **Update** radio button.

Step 67: Under Select Object Type, select the Users with Mailbox radio button.

Step 68: Under Select File, CSV File\*, browse to the Output folder in the directory where RDMCT is located and select from the User and Device Profile Configuration Phase.

**Step 69:** Under Failed Objects Filename, add a filename (for example: failed. txt) and select **Submit**.

**Step 70:** Check the status box to ensure all users are updated successfully and no failure.

#### 🗆 Status -

Bulk Administration Tool completed. Number of successes: 5, Number of failures: 0

Procedure 5 Deploy Phones

Step 1: Connect the IP Phone to the network



DHCP option 150 will instruct the IP Phone to connect to the Unified Com-munications manager TFTP server and auto-register. Once all IP Phones have registered proceed to the next step, which can only be accomplished once the phones have registered at least once to Cisco Unified Communications Manager.

Step 2: Select Bulk Administration > Phones > Update Phones > Query and then select Find.

Step 3: Scroll to the end of the list and select Next.

Step 4: Select the Reset Phones radio button at the top of the page.

– Logout/Reset/Restart –			
Logout Users before update			
On't Reset/Restart phones/Apply Config	Reset phones	Restart phones	C Apply Config

**Step 5:** Scroll down to the Extension Information section and select both the check boxes next to Enable Extension Mobility.

<ul> <li>Extension Information</li> </ul>	n ————	
Enable Ex	tension Mobility	
Log Out Profile	Use Current Device Settings	•

Step 6: At the bottom of the page select Run Immediately and then select Submit.

- Job Information		
Job Description	Update Phones - Query	
Run Immediately	$\bigcirc$ Run Later (To schedule and activate this job, use Job Scheduler page.)	

**Step 7:** Allow a few minutes for the phones to reset and reregister with Cisco Unified Communications Manager.

System Installation is now complete.

# Appendix A: Configuration Notes

### **Configuration Notes**

Cisco Unified Communications Managers
Timezone
cucm1 IP address
cucm1 IP Mask
cucm1 IP Gateway address
cucm2 IP address
cucm2 IP Mask
cucm2 IP Gateway address
Primary DNS
Secondary DNS
Domain (DNS)
Platform Administrator Username
Platform Administrator Password
Security Certificate Organization
Security Certificate Unit
Security Certificate Location
Security Certificate State
Security Certificate Country
DB Security Password
NTP Server IP or Hostname
Application User Username
Application User Password

# **Configuration Notes**

LDAP Directory Manager Distinguished Name	
LDAP Directory Manager Password	
LDAP Directory User Search Base	
LDAP Directory Hostname or IP Address	
LDAP Authentication Manager Distinguished Name	
LDAP Authentication Manager Password	
LDAP Authentication User Search Base	
LDAP Authentication Hostname or IP Address	

#### **Cisco Unity Connection**

Timezone
IP Address
IP Mask
IP Gateway Address
Primary DNS
Secondary DNS
Domain (DNS)
Platform Administrator Username
Platform Administrator Password
Security Certificate Organization
Security Certificate Unit
Security Certificate Location
Security Certificate State
Security Certificate Country
NTP Server IP or Hostname
Application User Username
Application User Password

### **Configuration Notes**

LDAP Directory Manager Distinguished Name
LDAP Directory Manager Password
LDAP Directory User Search Base
LDAP Directory Hostname or IP Address
LDAP Authentication Manager Distinguished Name
LDAP Authentication Manager Password
LDAP Authentication User Search Base
LDAP Authentication Hostname or IP Address

# Appendix B: SBA for Midsize Agencies Document System







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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

C07-641153-00 1/11