



Cisco Unified MobilityManager Installation Guide

Cisco Unified MobilityManager is a Computer Telephony Integration (CTI) application server that integrates with Cisco Unified Communications Manager to provide Mobile Connect features.

Overview

Mobile Connect refers to the set of features that includes the ability to answer incoming calls on the desk phone or cellular phone, to pick up in-progress calls on the desk phone or cellular phone without losing the connection, and to originate enterprise calls from the cellular phone.

These sections describe how to install Cisco Unified MobilityManager, Release 1.2 and obtain additional information:

- [Definitions, page 2](#)
- [Upgrading from Previous Versions, page 3](#)
- [Preparing to Install, page 10](#)
- [Installing Cisco Unified MobilityManager 1.2, page 14](#)
- [Configuring Cisco Unified Communications Manager to Work with Cisco Unified MobilityManager, page 21](#)

Definitions

Table 1 provides definitions of important terms used in this guide.

Table 1 **Terms and Definitions**

Term	Definition
Calling Search Space	Designates the collection of partitions that are searched to determine how an originating number should be routed. See the “Creating the Calling Search Space” section on page 23 .
CTI Port	Designates a virtual phone device within Cisco Unified Communications Manager. The required number of ports will vary according to expected usage patterns and availability of external trunk lines.
CTI Route Point	Designates a virtual device in Cisco Unified Communications Manager that can receive multiple, simultaneous calls and redirect them to the proper destinations. Within Cisco Unified MobilityManager, the CTI route point presents the correct caller ID to the cellular or additional wired telephone numbers that are contacted by Cisco Unified MobilityManager. The outgoing CTI ports also use the CTI route point to place calls to remote destinations. The CTI route point is assigned to a partition that only Cisco Unified MobilityManager can use. You create a CTI route point as part of the initial configuration process. See the “Creating a CTI Route Point” section on page 28 .
CTI Users	Refers to user records defined in Cisco Unified Communications Manager. As part of the Cisco Unified MobilityManager configuration process, you must create two CTI users: one to support the outgoing CTI ports, and the second to control the shared line CTI ports. See the “Adding Cisco Unified MobilityManager CTI Users” section on page 30 .
Mobile Connect	Refers to the set of features that enables users to manage business calls using a single phone number and pick up in-progress calls on the desk phone and cellular phone. Cisco Unified MobilityManager supports Mobile Connect features.
Mobile Voice Access	Refers to the integrated voice response (IVR) system used to initiate Mobile Connect calls and to activate or deactivate Mobile Connect capabilities.

Table 1 **Terms and Definitions (continued)**

Term	Definition
Outgoing CTI Port	Manages the calls that Cisco Unified MobilityManager makes to remote destinations. Cisco recommends that you create at least one outgoing CTI port in Cisco Unified Communications Manager for each five shared-line user CTI ports. See the “Creating a Pool of CTI Ports for Outgoing Calls” section on page 24.
Partition	Designates a structure for managing Mobile Connect inbound calls within Cisco Unified Communications Manager. The partition facilitates call routing by creating logical subsets for inbound calls that are based on organization, location, and call type. Each CTI route point is assigned to the partition that you create during the initial configuration process described in this guide. The partition, in turn, is assigned to a calling search space. See the “Creating a Partition for the Route Point” section on page 22.
Remote Destination	Designates cellular phones that are available for Mobile Connect responses and pickup, plus other phones that are used for system remote access through the Cisco Mobile Voice Access application.
Shared Line CTI Port	Enables a call to be answered by the desk phone or to be directed to a remote destination. To create a shared line, you configure a CTI port in Cisco Unified Communications Manager with a directory number that is identical to the directory number on a physical phone. This permits the physical desk phone or the CTI port to answer the same call. When the CTI port answers the call, it is automatically redirected to the remote destination. See the “Creating a CTI Port for the Shared Line” section on page 26.

Upgrading from Previous Versions

The process for upgrading from Cisco Unified Mobility Manager 1.1 to 1.2 depends on the type of DNS server being used. The following DNS options are supported:

- Microsoft DNS server
- UNIX or LINUX-based DNS server
- No DNS server

Refer to [Table 2](#) for an overview of the required steps.

Table 2 **Overview of Upgrading Process**

Task	Purpose	For More Information
DNS Server—Microsoft DNS Server		
1. Verify that the ISM devices mount properly.	Ensures that DNS is functioning properly before starting the install process.	See the “ Verifying ISM Device Status ” section on page 6.
2. Download and run scripts.	Ensures integrity of DNS configuration and database manager.	See the “ Downloading and Running Scripts ” section on page 7.
3. Perform two data backups using Cisco Unified MobilityManager 1.1.	Retains your existing Mobile Connect data.	See the “ Backing Up Data Before Installing ” section on page 8.
4. Verify requirements for installation and gather necessary information.	Enables you to progress through the installation process more smoothly.	See the “ Preparing to Install ” section on page 10.
5. Install Cisco Unified MobilityManager 1.2.	Installs updated software on the MCS server. For an upgrade, you must install on the same MCS server or a different one with the same hostname, IP address, and domain name (if DNS is enabled) used for Cisco MobilityManager 1.1.	See the “ Installing Cisco Unified MobilityManager 1.2 ” section on page 14.
6. Restore data from Cisco Unified MobilityManager.	Restores your existing Mobile Connect data.	See the “ Restoring Data After Installing ” section on page 9.
7. Restart Cisco Unified MobilityManager.	Forces the configuration to be read from the restored data.	See the “ Restoring Data After Installing ” section on page 9.

Table 2 **Overview of Upgrading Process (continued)**

Task	Purpose	For More Information
DNS Server—UNIX, Linux, or none		
1. Backup data using Cisco Unified MobilityManager 1.1.	Retains your existing Mobile Connect data.	See the “Backing Up Data Before Installing” section on page 8.
2. Verify requirements for installation and gather necessary information.	Enables you to progress through the installation process more smoothly.	See the “Preparing to Install” section on page 10.
3. Install Cisco Unified MobilityManager 1.2.	Installs updated software on the MCS server. For an upgrade, you must install on the same MCS server or a different one with the same hostname and IP address used for Cisco MobilityManager 1.1.	See the “Installing Cisco Unified MobilityManager 1.2” section on page 14.
4. Restore data from Cisco Unified MobilityManager.	Restores your existing Mobile Connect data.	See the “Restoring Data After Installing” section on page 9.
5. Restart MobilityManager.	Forces the configuration to be read from the restored data.	See the “Restoring Data After Installing” section on page 9.

Verifying ISM Device Status

Before running the upgrade script, you should verify whether the ISM devices are mounting properly.

To verify ISM device status, follow these steps:

Procedure

-
- Step 1** To display the mounted devices using Cisco MobilityManager 1.1, enter the **ism_show -devices** command:
- ```
ism_show -devices
file disk 1 mounted on /opt/informix/database/device/ism_arc, write
enabled
file disk 2 mounted on /opt/informix/database/device/ism_logs, write
enabled
```
- Step 2** If the devices do not mount properly, run the **cmm\_fixupgrade.sh -fix** script.
- Step 3** Using Secure File Transfer Protocol (SFTP), download the **cmm\_fixupgrade.sh** script to the MCS server from Cisco at this URL:  
<http://www.cisco.com/cgi-bin/tablebuild.pl/mobmgr>
- Step 4** To verify that the devices properly mount after running the script, enter the **ism\_show-devices** command again.
- 



### Note

If you need to reinstall Cisco Unified MobilityManager 1.2 after upgrading, you can use a CLI command to verify the ISM device status. Choose **Serviceability > Service Status** and verify that the Database Storage Manager is running. If it is not running, run **cli utils dsm status/start**. Choose **System > System Parameters** and click **Restart Cisco Unified MobilityManager**.

---

## Downloading and Running Scripts

If you are using a Microsoft DNS Server with Cisco Unified MobilityManager 1.2, you must download and run these scripts to ensure the integrity of your DNS configuration and database manager.

To download and run the DNS scripts, follow these steps:

Procedure

- 
- Step 1** Using Secure File Transfer Protocol (SFTP), download the `cmm_fixupgrade.sh` script to the MCS server from Cisco at this URL:  
<http://www.cisco.com/cgi-bin/tablebuild.pl/mobmgr>
- Step 2** Run the **`cmm_fixupgrade.sh -check`** command to verify the DNS server.
- ```
cmm_fixupgrade.sh -check
Informix Storage Manager host info:...
name: lax.nl.env.HOSTNAME ;
parallelism: 4;
manual saves: Enabled;
administrator: root<hostname>, informix<server name>;
browse policy: 6 Months;
retention policy: 6 Months;
Dump /etc/hosts :
127.0.0.1 localhost
150.1.1.12 lax.nl.env.<hostname> <server name>
```
- Step 3** Verify that Informix Storage Manager host is identified as: `lax.nl.env.hostname`.
- Step 4** To modify the `/etc/hosts` file, run the **`cmm_fixupgrade.sh -upgrade`** script.
- Step 5** Restart the MCS server.
- Step 6** To verify the fully-qualified hostname, use the **`ism_show -config`** command.
-

Backing Up and Restoring Data

To ensure that you retain the Mobile Connect data currently in the database, you must back up the data before installing, and then restore the data after installing. Refer to these sections for details:

- [Backing Up Data Before Installing, page 8](#)
- [Restoring Data After Installing, page 9](#)

Backing Up Data Before Installing

Prior to upgrading to Cisco Unified MobilityManager 1.2, you must back up your data using Cisco MobilityManager 1.1.



Caution

If you do not properly back up your data before starting the installation process, you will lose all existing Mobile Connect data.

To back up your data, follow these steps:

Procedure

Step 1 From Cisco MobilityManager 1.1, choose **System > Backup and Restore**.



Note Be sure to use the backup program in Cisco MobilityManager for this step. Do not use Cisco Disaster Recovery Services.

Step 2 In the Host Name or IP Address field, enter the appropriate information to identify the backup server.



Note You must use an SFTP server, and it cannot be the same MCS server on which you are installing Cisco Unified MobilityManager.

Step 3 Enter the User ID and Password for the backup server.

Step 4 Enter the password again in the Confirm Password field.

Step 5 In the File Path field, enter the location to store or retrieve the backup files.

- Step 6** To begin backing up the database to the specified location, click Start Backup Now.

**Caution**

If you are using Microsoft DNS Server, perform two backups to ensure the integrity of the data.

- Step 7** When the backup completes, navigate to the location where you stored the backup and verify that these two files are present and that you can unzip them to view their contents:

- ciscoSNRdb.tgz
- ciscoSNRsnmp.tgz

- Step 8** Install Cisco MobilityManager 1.2 before restoring data. See the [“Preparing to Install” section on page 10](#) for details.

Restoring Data After Installing

After installing Cisco Unified MobilityManager 1.2, you must then restore your data from Cisco MobilityManager 1.1.

To restore data after installing, follow these steps:

Procedure

- Step 1** From Cisco MobilityManager 1.2, choose **System > Backup and Restore**.

**Note**

Be sure to use the restore program in Cisco MobilityManager for this step. Do not use Cisco Disaster Recovery Services.

- Step 2** In the Host Name or IP Address field, enter the appropriate information to identify the backup server you used to back up the data.
- Step 3** Enter the User ID and Password for the backup server.
- Step 4** Enter the password again in the Confirm Password field.
- Step 5** In the File Path field, enter the location to store or retrieve the backup files.

- Step 6** Click **Start Restore Now** to begin backing up the database to the specified location.
- Step 7** After completing the restore process, choose **System > System Parameters** and click **Restart Cisco Unified MobilityManager**.
-

Preparing to Install

Before upgrading or installing Cisco Unified MobilityManager 1.2, you must first verify the hardware and software requirements and gather necessary information. These sections provide details about these requirements:

- [Hardware and Software Requirements, page 10](#)
- [Gathering Installation Information, page 12](#)

Hardware and Software Requirements

This section describes hardware and software requirements for installing and operating Cisco Unified MobilityManager:

- [Hardware Requirements, page 10](#)
- [Software and Browser Requirements, page 11](#)

Hardware Requirements

Verify that you have the following required hardware:

- One of the following MCS servers:
 - MCS-7815-I1 (3.0 GHz)
 - MCS-7825-H1 (3.4 GHz)
 - MCS-7835-H1 (3.4 GHz)
 - MCS-7835-H2 (3.4 GHz)
 - MCS-7835-I1 (3.4 GHz)
 - MCS-7835-I2 (3.4 GHz)

- MCS-7845-H1 (3.4 GHz dual processor)
- MCS-7845-H2 (3.4 GHz dual processor)
- MCS-7845-I1 (3.4 GHz dual processor)

**Note**

Additional servers may be added. Consult the latest release notes or product data sheet for the most up-to-date information.

- For system remote access, a gateway that can support H.323. For configuration information, see the “[Configuring H.323 Gateways for Mobile Voice Access](#)” section on page 38.
- Cisco Unified IP phones that support XML and HTTP for the cellular phone pickup feature, which enables a user to change from the desk phone to cellular phone without disconnecting from a call.
- Existing cellular phones devices and other remote phone endpoints.

Software and Browser Requirements

Ensure you have the following required software:

- Voice-enabled IP network, including LAN and PSTN voice gateways
- Working Cisco Unified Communications Manager installation, Release 4.0.2a or higher—For detailed compatibility information, see the Cisco Unified Communications Manager Compatibility Matrix at this URL: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm.
- Operating system and other software required for Cisco Unified MobilityManager, included on the software installation DVD
- Supported web browser:
 - Microsoft Internet Explorer, version 6.0 or later
 - Netscape Navigator version, 7.2 or later
- Use Cisco Unified Communications Manager Administration to set up the initial computer telephone interface (CTI) information—See the “[Configuring Cisco Unified Communications Manager to Work with Cisco Unified MobilityManager](#)” section on page 21.

Gathering Installation Information

[Table 3](#) lists the configuration data required to install Cisco Unified MobilityManager. Use the middle column record your system and network configuration information.

**Note**

Some fields are optional and may not be appropriate for your installation. For example, if you plan to use DHCP, you will not need to enter other network settings.

**Caution**

You cannot change some fields after installation without reinstalling the software. Refer to the last column in [Table 3](#) to determine whether a field can be changed after installation.

Table 3 **Configuration Data**

Configuration Data	System and Network Configuration Values	Can Entry Be Changed After Installation?
Domain Name Service (DNS) Enable		No
Primary DNS Server IP address (if applicable)		No
Secondary DNS Server IP Address (if applicable)		No
DHCP		Yes CLI> set network dhcp eth0 ena CLI> set network dhcp eth0 dis
Host Name		No

Table 3 **Configuration Data (continued)**

Configuration Data	System and Network Configuration Values	Can Entry Be Changed After Installation?
IP Address of Server (if DHCP is not used)		Yes Note If you are upgrading from Cisco MobilityManager 1.1, you must install Cisco Unified MobilityManager 1.2 on a server with the same hostname, IP address, and domain (if using DNS). You cannot change these values during installation. Note If you change the IP address after installation, you must open Cisco IPT Platform Administration and verify that the host settings reflect the new IP address. If the host settings do not reflect the new IP address, you must perform these tasks: 1. Update the host IP address in Platform Administration and restart Cisco Unified MobilityManager. See the “Platform Administration” chapter in the <i>Cisco Unified MobilityManager Administration Guide</i>. 2. In the H.323 gateway configuration, reload the Cisco Unified MobilityManager application using the command: <pre>CLI> call application voice load <application name>.</pre>
IP Netmask (if DHCP is not used)		Yes Note You can change the netmask, but the value is not saved during upgrade. <pre>CLI > set network ip eth 0 <addr> <mask></pre>

Table 3 **Configuration Data (continued)**

Configuration Data	System and Network Configuration Values	Can Entry Be Changed After Installation?
Gateway IP Address (if DHCP is not used)		Yes CLI > set network gateway <IPaddress> Note You can change the address, but the value is not saved during upgrade.
Time Zone		No
Domain Name		No
Administrator ID		No
Administrator Password		Yes CLI > set password Note The cmmadmin password can be reset using the utils reset_ui_administrator_password command.

Installing Cisco Unified MobilityManager 1.2

This section describes how to install and configure the operating system and Cisco Unified MobilityManager on a server using the installation DVD.

Before You Begin

Before you begin, review these topics:

- [Upgrading from Previous Versions, page 3](#)—To upgrade from a previous version of Cisco MobilityManager.
- [Gathering Installation Information, page 12](#)—To review the configuration data that you have entered.
- [Connecting the Server Hardware, page 15](#)—To connect the server for the first time.

- [Navigating Within the Installation Wizards, page 15](#)—To learn about the installation wizards.
- [Installation Process, page 17](#)—To get a high-level overview of the installation process.

Connecting the Server Hardware

Before powering the server for the first time, you must connect a monitor, a keyboard, and network cable.

To connect the server hardware, follow these steps:

Procedure

-
- | | |
|---------------|--|
| Step 1 | Plug the mouse and keyboard into the standard mouse and keyboard connectors that are marked on the back of the server. |
| Step 2 | Plug the monitor cable into the monitor connector on the back of the server. |
| Step 3 | Connect the network cable from the server to the network. |
-

Navigating Within the Installation Wizards

The following installation wizards guide you through the installation and configuration process:

- Server Installation Wizard—Common to all Cisco IPT appliances
- Cisco Unified MobilityManager Installation Wizard—Specific installation and configuration for Cisco Unified MobilityManager

For information on how to navigate within the installation wizards, see [Table 4](#).



Note

Keep in mind that all fields in the installation wizards are case-sensitive.

Table 4 *Navigating Within the Installation Wizards*

If you want to...	Then...
Move to the next field	Press Tab . Note When you press Tab to move to a field with a drop-down menu, the menu opens.
Move to the previous field	Press Shift-Tab . Note Shift-tab may move you past the previous field if the entry in the previous field depends on a prior field.
Choose an option in a drop-down menu	Press Tab .
Complete a window	Press Enter .
Get help information on a window	Press ? .
Close a help window	Press Tab .
Scroll up or down in a help pop-up window or drop-down box (A '#' displays on the left margin when additional text exists in a help window or options in a drop-down box.)	Press the Up or Down arrows.
Go to the previous page in a wizard	Press P if you are at the bottom of a page. Press Shift-Tab until you move to the top of the previous page. Note You cannot use P and Shift-Tab to navigate between the Server Installation Wizard and the Cisco Unified MobilityManager Installation Wizard.

Installation Process

To install the operating system and Cisco Unified MobilityManager, follow these steps:

Procedure

Step 1 Verify that a DNS server is running in your network.



Note

To use DNS, ensure that the IP address of the DNS server is correct and the Cisco Unified MobilityManager server hostname is configured in the DNS server. If DNS is not used, you should verify that the Cisco Unified MobilityManager hostname settings are correct in Cisco IPT Platform Administration.

Step 2 Power up the server.

Step 3 While the server is booting, insert the DVD. After inserting the DVD, recycle the power on the server.

The server reboots from the DVD and displays all installed software version.

Step 4 Enter **yes** and press **Enter** to overwrite the hard drive.

The operating system installation begins and may take approximately 20-30 minutes to complete.

Step 5 When the OS installation is complete, the DVD slot automatically slides open. Remove the DVD.

Step 6 To restart the system, press **Enter**.

The computer reboots and a menu displays booting options. If you do not select an option, the system will auto-select after 10 seconds. If you press any key on the keyboard, the window continues to display until you select an option.

Step 7 At the **>** prompt, press **Enter** to continue the installation process without preconfigured data.

The Server Installation Wizard opens.

Step 8 Enter **yes** and press **Enter** to respond to the installation questions, as shown in [Table 5](#). When responding, use the information that you recorded in [Table 3](#).

- Step 9** After you answer the installation questions, a summary screen displays that shows all the configuration parameters. To accept the settings and start installation, press **Enter**.

The system installs and configures Cisco Unified MobilityManager.



Note This process takes approximately 30-40 minutes. During this time, the monitor might go into a screen saver mode.

During this installation, you might be prompted to respond to multiple “DVD Found/Media Check” messages. At the first prompt, press **Yes** to ensure the integrity of the DVD, and press **No** to subsequent prompts to continue the installation.

When the installation and configuration process completes, Cisco Unified MobilityManager starts automatically, and a login window displays. Next, configure settings in Cisco Unified Communications Manager, according to the instructions in the [“Configuring Cisco Unified Communications Manager to Work with Cisco Unified MobilityManager”](#) section on page 21.

For information about how to use Cisco Unified MobilityManager to set up and administer Mobile Connect capabilities, see the *Cisco Unified MobilityManager Administration Guide*.

Table 5 **Installation Questions**

Windows and Fields	Description
Timezone Configuration	The default is Pacific Standard Time. To change timezones, press Tab .
Set hardware clock?	Press Tab to choose hours, minutes, seconds, day, week, and year, and use arrows to set the desired value. To save the clock settings, press Enter .
DHCP select	To use DHCP to automatically configure the network settings on your server, choose Yes . If you choose Yes , the IP address fields are crossed out. If you choose No , you must enter the required field information described in the following “Static Network Configuration” row.
Static Network Configuration	
Hostname	Enter a host name that is unique to your network. The host name can comprise up to 64 characters and can contain alphanumeric characters and hyphens.
IP Address	Enter the IP address in the form <i>d.d.d.d</i> , where <i>d</i> can have a value between 0 and 255 (except 0.0.0.0).
IP Mask	Enter the IP mask in the form <i>d.d.d.d</i> , where <i>d</i> can have a value between 0 and 255 (except 0.0.0.0).
Gateway address (GW address)	Enter the IP address of the gateway in the format <i>d.d.d.d</i> , where <i>d</i> can have a value between 0 and 255 (except 0.0.0.0). If you do not have a gateway, you must still populate this field by setting it to 255.255.255.255. Not having a gateway may limit you to only being able to communicate with devices on your subnet.
DNS Enabled	Make sure DNS is properly configured and choose Yes to enable DNS. If you choose No , the system cannot resolve any domain names.
DNS Client Configuration	
Primary DNS	Enter the IP address of the DNS server that you want to specify as the primary DNS server in the format <i>d.d.d.d</i> , where <i>d</i> can have a value between 0 and 255 (except 0.0.0.0). Consider this field required if DNS is set to Yes .
Secondary DNS	In this optional field, enter the IP address of the secondary DNS. Enter the IP address in dotted decimal format as <i>d.d.d.d</i> , where <i>d</i> can have a value between 0 and 255 (except 0.0.0.0).
Domain	Enter the DNS domain suffix for the server (<i>xxx.com</i>).

Table 5 **Installation Questions (continued)**

Windows and Fields	Description
GW Address	Enter the IP address of the gateway in the format <i>d.d.d.d</i> , where <i>d</i> can have a value between 0 and 255 (except 0.0.0.0).
Administrator Login Configuration	
Administrator ID	Use this ID for access to the server console and platform administration pages. Ensure the ID is unique, and it can contain lowercase, alphanumeric characters, hyphens, and underscores. It must start with a lowercase, alphanumeric character. Record this required field for use when you log in to the CLI on the server. You cannot change this field after installation.
Password	Enter the password and reenter it in the Confirm Password field. The password, which must be at least 6 characters long can contain alphanumeric characters, hyphens, and underscore. The password is used with the administrator ID for access to the server console. The password checking is similar to that used with <i>passwd</i> on Linux, including requirements for different character types. This field is required, and you should record it for use when logging in to Cisco Unified MobilityManager. Note If you need to change the administrator password during installation, or if you notice character scrambling, go back to the previous window and then return to the current window. You will now be able to modify the password.
Certificate Signing Request Configuration	
Organization	Enter these fields as appropriate for your organization.
Unit	
Location	
State	
Country	
Network Time Protocol Client Configuration	
Network Time Protocol Client Configuration	To use a Network Time Protocol (NTP) server, choose Yes . If you choose Yes , the IP address fields are crossed out.
NTP Server 1-2	Enter the IP address of the NTP server(s).

Table 5 **Installation Questions (continued)**

Windows and Fields	Description
Database Access Security Configuration	
Security Password	Enter the password and reenter it in the Confirm Password field. The password, which must be at least 6 characters long can contain alphanumeric characters, hyphens, and underscore.

Configuring Cisco Unified Communications Manager to Work with Cisco Unified MobilityManager

Before you can use Cisco Unified MobilityManager to set up Mobile Connect, you must configure settings in the Cisco Unified Communications Manager system. This section describes how to configure the required settings in Cisco Unified Communications Manager.

To get started, log in to the Cisco Unified Communications Manager administrative interface and verify that the following services are running:

- Cisco Communications Manager
- Cisco CTIManager

**Note**

You can use Serviceability to verify that the services are activated and running. For more information, refer to the *Cisco Unified Communications Manager Serviceability Administration Guide* and the *Cisco Unified Communications Manager Administration Guide*.

You must perform these tasks in this section in the indicated order:

1. [Restarting Cisco Unified MobilityManager after Upgrading Cisco Unified Communications Manager, page 22](#)
2. [Creating a Partition for the Route Point, page 22](#)

3. [Creating the Calling Search Space, page 23](#)
4. [Creating a Pool of CTI Ports for Outgoing Calls, page 24](#)
5. [Creating a CTI Port for the Shared Line, page 26](#)
6. [Creating a CTI Route Point, page 28](#)
7. [Adding Cisco Unified MobilityManager CTI Users, page 30](#)
8. [Setting Parameters for the Mobile Connect IP Phone Service in Cisco Unified Communications Manager, page 36](#)
9. [Configuring H.323 Gateways for Mobile Voice Access, page 38](#)
10. [Checking the Desk Phone Configuration, page 43](#)

Restarting Cisco Unified MobilityManager after Upgrading Cisco Unified Communications Manager

To ensure that the common software files are synchronized, you should restart Cisco Unified MobilityManager whenever you upgrade Cisco Unified Communications Manager.

Creating a Partition for the Route Point

A CTI route point in Cisco Unified Communications Manager designates a virtual device that can receive multiple, simultaneous calls and redirect them to the proper destinations. Within Cisco Unified MobilityManager, the CTI route point presents the correct caller ID to the cellular or additional wired telephone numbers that are contacted by Cisco Unified MobilityManager. The outgoing CTI ports also use the CTI route point to place calls to remote destinations.

The [“Creating a CTI Route Point” section on page 28](#) describes how to create the CTI route point. Before doing so, you must create a partition for the CTI route point. The partition facilitates call routing by creating logical subsets for inbound calls that are based on organization, location, and call type. You must also create a calling search space for the partition and set up the CTI ports for outgoing calls and shared lines.

To create the partition, follow the steps in [Table 6](#):

Table 6 *Route Point Partition Settings*

Cisco Communications Manager 4.x	Cisco Unified Communications Manager 5.x
1. Log in to Cisco Communications Manager 4.x.	1. Log in to Cisco Unified Communications Manager.
2. Choose Route Plan > Class of Control > Partition .	
3. Click Add a New Partition .	
4. Enter the partition name and a description.	
5. Click Insert .	5. Click Save .

Creating the Calling Search Space

A calling search space specifies the collection of partitions that are searched to determine how an originating number should be routed. You must create a special calling search space that contains the partition defined in the “[Creating a Partition for the Route Point](#)” section on page 22. The CTI ports must be able to reach the destinations that belong in the <None> partition or the partition defined for the CTI route point.

To create the calling search space, follow the steps in [Table 7](#):

Table 7 *Calling Search Space Settings*

Cisco Communications Manager 4.x	Cisco Unified Communications Manager 5.x
1. Log in to Cisco Communications Manager 4.x.	1. Log in to Cisco Unified Communications Manager.
2. Choose Route Plan > Class of Control > Calling Search Space .	2. Choose Call Routing > Class of Control > Calling Search Space .
3. Enter the name and a description.	3. Enter the name and a description.
4. Choose the partition you created in “ Creating a Partition for the Route Point ” section on page 22 from the list of available partitions, and use the arrow to move the partition to the Selected Partitions area.	
5. Click Insert .	5. Click Save .

Creating a Pool of CTI Ports for Outgoing Calls

You must create a pool of CTI ports to manage all outgoing calls that Cisco Unified MobilityManager makes to cellular phones and other destinations. A CTI port functions as a virtual phone device. The required number of ports will vary according to expected usage patterns and availability of external trunk lines.

You must create a minimum of two CTI ports. However, Cisco recommends that you create at least one outgoing CTI port for each five shared-line user CTI ports. For example, if your installation has 50 users with shared-line CTI ports, you should create a minimum of 10 outgoing CTI ports.



Note

When configuring CTI ports for outgoing calls, make sure the Media Resource group for the CTI ports does not include Music-On-Hold (MOH) servers.

To create a pool of CTI ports, follow the steps in [Table 8](#):

Table 8 **CTI Port Settings**

Cisco Communications Manager 4.x	Cisco Unified Communications Manager 5.x
1. Log in to Cisco Communications Manager 4.x	1. Log in to Cisco Unified Communications Manager 5.x.
2. Choose Device > Phone .	2. Choose Device > Phone .
3. Click Add a New Phone .	3. Click Add New .
4. In the pull-down list box, find and select CTI Port.	4. In the pull-down list box, find and select CTI Port.
5. To open the Phone Configuration window, click Next .	5. To open the Phone Configuration window, click Next .

Table 8 **CTI Port Settings (continued)**

Cisco Communications Manager 4.x	Cisco Unified Communications Manager 5.x
6. Complete the following fields: • Device Name—Enter an alphanumeric name to identify the CTI port. You should name the CTI ports with a prefix, such as CMM_, that can be easily identified when you search for them in Phone Configuration . The prefix should differ from those that are assigned to other CTI ports that Mobile Connect does not use. For example, the device name CMM_90001 could identify the device as Mobile Connect CTI port 90001. • Description—Enter a description for the port. If this field is left blank, the system uses a default description that matches the device name. • Device Pool—Select one from the pull-down list box. Make sure the Media Resource group for the Device Pool does not include Music-On-Hold (MOH) servers. • Calling Search Space—Enter the calling search space that you previously created in “Creating the Calling Search Space” section on page 23.	
Note You do not need to choose values for any of the other fields in this window.	
7. Click Insert .	7. Click Save .
8. To add a directory number, click OK .	8. To add a directory number, click one of the line links
9. Complete the following fields: • Directory Number—Enter a number that is not normally used by any of your normal desk phones. Consider creating a pool of virtual numbers that differs from the desk phone pool, such as a sequence of numbers beginning with 90001. • Partition—Choose the partition for the outgoing ports. This should not be the partition that was created for the CTI route point.	
Note You do not need to choose values for any of the other fields in this window.	
10. Click Add .	10. Click Save .
Note To create additional CTI ports, use Copy (if fewer than 10 ports) or BAT (10 or more ports).	Note To create additional CTI ports, use Copy (if fewer than 10 ports) or BAT (10 or more ports).

Verifying the CTI Port Configuration

To verify that all CTI ports have been configured properly, perform a search using the Device Name prefix common to the CTI ports.

To perform the search, follow these steps:

Procedure

Step 1 In Cisco Unified Communications Manager, choose **Device > Phones**.

Step 2 Enter the prefix for your CTI device names and click **Find**.

All the device names for the CTI ports that you created should be displayed in the list of devices.

Creating a CTI Port for the Shared Line

To create a shared line, you must configure one CTI port with a directory number that is identical to the directory number on a physical phone. With a shared line, either the physical desk phone or the CTI port can answer the same call.



Note

When configuring CTI ports for the shared lines, make sure the Media Resource group for the CTI ports does not include Music-On-Hold (MOH) servers.



Note

If you want to restrict calling numbers (for example, international dialing), be sure to choose the appropriate calling search space for the CTI device.



Note

To support different types of codecs, a transcoder must be configured in Cisco Unified Communications Manager for shared line CTI ports. Refer to the *Cisco Unified Communications Manager Administration Guide* for transcoder configuration information.

To create a shared line, follow the steps in [Table 9](#):

Table 9 **Shared Line CTI Port Settings**

Cisco Communications Manager 4.x	Cisco Unified Communications Manager 5.x
1. Log in to Cisco Communications Manager 4.x.	1. Log in to Cisco Unified Communications Manager 5.x.
2. Choose Device > Phone .	2. Choose Device > Phone .
3. Click Add a New Phone .	3. Click Add a New Phone .
4. In the pull-down list box, find and select CTI Port.	4. In the pull-down list box, find and select CTI Port.
5. To open the Phone Configuration window, click Next .	5. To open the Phone Configuration window, click Next .
6. Complete the following fields: - Device Name—Enter an alphanumeric name for the shared line. You should name the CTI ports with a prefix, such as CMM_, that can be easily identified when you search for them in Phone Configuration . The prefix should differ from those that are assigned to other CTI ports that Mobile Connect does not use. For example, the device name CMM_2003 could identify the device as the Mobile Connect shared-line CTI port with actual directory number 2003. - Assign the device pool and other parameters for this CTI port to be identical to the parameters of the physical phone that will be used for the shared line.	
7. Click Insert .	7. Click Save .
8. To add a directory number, click OK .	8. To add a directory number, click one of the line links.
9. Complete the following fields: - Directory Number—Enter a number that matches the directory number for the physical phone. - Configure the rest of the parameters in the window to have the same values as the physical phone.	
Note A red text label to the right of the Directory Number field indicates that this is a shared line.	
10. Click Add .	10. Click Save .
Note To add additional numbers, click Copy , and then repeat the previous steps of this process.	Note To add additional numbers, click Copy , and then repeat the previous steps of this process.

Creating a CTI Route Point

You must create a CTI route point to provide the correct Caller ID to the receiving phone. Without a CTI route point, the display for an incoming call would show only the Caller ID of the CTI port originating the call, rather than the actual originating phone number. The CTI route point is also used by the outgoing CTI ports to place calls to the remote destinations.

To create a CTI route point, follow the steps in [Table 10](#):

Table 10 **CTI Route Point Settings**

Cisco Communications Manager 4.x	Cisco Unified Communications Manager 5.x
1. Log in to Cisco Communications Manager 4.x.	1. Log in to Cisco Unified Communications Manager.
2. Choose Device > CTI Route Point .	2. Choose Device > CTI Route Point .
3. Click Add a New CTI Route Point .	3. Click Add New .

Table 10 **CTI Route Point Settings (continued)**

Cisco Communications Manager 4.x	Cisco Unified Communications Manager 5.x
4. Complete the following fields: • Device Name—Enter an alphanumeric name to identify the CTI route point. • Description—Enter a description for the port. If this field is left blank, the system uses a default description that matches the device name. • Device Pool—Choose a device pool. Make sure the Media Resource group for the Device Pool does not include Music-On-Hold (MOH) servers. • Calling Search Space—Choose a search space. Ensure the chosen calling search space is identical to that of the majority of your desk phones. The search space should be able to reach a voice gateway that is capable of making calls to the PSTN. It can also contain a desk phone, which then becomes a valid destination phone for Mobile Connect. If your Cisco Unified Communications Manager network includes different types of gateways for different types of calls (such as local calls, long distance calls, and intercluster trunk calls), ensure the calling search space can reach route patterns that would point to each of the appropriate gateway types. You can also use the calling search space as a means of restricting the destinations that users can configure. Note Any phone or gateway that resides in the <None> space will be called directly from the outgoing CTI ports. The CTI route point cannot intercept the call and display the correct Caller ID. This will result in the Caller ID being incorrect; however the overall function of Mobile Connect will not be impaired. Cisco recommends that no devices be in the <None> partition.	
5. Click Insert.	5. Click Save.
6. To add a directory number, click OK.	6. To add a directory number, click a line link.

Table 10 CTI Route Point Settings (continued)

Cisco Communications Manager 4.x	Cisco Unified Communications Manager 5.x
7. Complete the following fields:	
• Directory Number – Cisco Unified Communications Manager 4.0 and 4.1—Enter ! (single exclamation point without quotes). – Cisco Unified Communications Manager 4.2 and 5.x—Enter !# (single exclamation point followed by number sign) • Partition—Choose the partition that you created in “Creating a Partition for the Route Point” section on page 22.	
Leave the remaining fields on this window at their default values.	
8. Click Add .	8. Click Save .

Adding Cisco Unified MobilityManager CTI Users

To support Cisco Unified MobilityManager, you must create two users. One user controls the outgoing CTI ports. The second user controls the CTI ports that have a shared line with the physical desk phones and also controls the CTI route point.

Before You Begin

Cisco Unified Communications Manager 5.x and later enable you to configure application and end users. You can use either user type with the following caveats:

- The two user types (end user and application) require you to enter slightly different information. Be sure to refer to the instructions appropriate for your configuration.
- If you are using Active Directory, be aware that you should configure end users using Active Directory and application users using Cisco Unified Communications Manager. To configure the CTI user following these guidelines, choose one of these options:
 - If you already have the CTI user in Active Directory, you need to configure the CTI user as an end user in Cisco Unified Communications Manager. After synchronizing with Active Directory, the users display as

end users in Cisco Unified Communications Manager. To verify whether synchronization with an LDAP server is enabled, from Cisco Unified Communications Manager, choose **System > LDAP > LDAP System**.

- If you prefer to configure the CTI user as an application user, first verify that the CTI user is not configured in Active Directory. Then, add the CTI user as an application user using Cisco Unified Communications Manager.

Adding a User for the Outgoing CTI Ports

To add the user who controls the outgoing CTI ports, follow the steps in [Table 11](#):

Table 11 **Outgoing CTI Ports User Settings**

Cisco Communications Manager 4.x	Cisco Unified Communications Manager 5.x
1. Log in to Cisco Communications Manager 4.x.	1. Log in to Cisco Unified Communications Manager 5.x.
2. Choose User > Add a New User .	2. Choose one of the following: • User Management > Application User • User Management > End User

Table 11 **Outgoing CTI Ports User Settings (continued)**

Cisco Communications Manager 4.x	Cisco Unified Communications Manager 5.x
3. Complete or enable these fields: • First Name and Last Name. • User ID—enter an alphanumeric identifier. Note The chosen names do not affect Cisco Unified MobilityManager, but using names with a common prefix such as CMM makes it easier to find later. • User Password and Confirm Password—Enter and confirm a password. The password is used for access to the XML configuration file of Mobile Connect. The password must be at least 5 characters. • PIN and Confirm PIN—Although the PIN field is required, Mobile Connect does not use a PIN, so it does not matter what value you enter. The PIN must be at least 5 characters. • Enable CTI Application Use. • Call Park Retrieval Allowed. • Enable Calling Party Number Modification.	3. Complete or enable these fields: • First Name and Last Name (End user only). • User ID—enter an alphanumeric identifier. Note The chosen names do not affect Cisco Unified MobilityManager, but using names with a common prefix such as CMM makes it easier to find later. • Password and Confirm Password—Enter and confirm a password. The password is used for access to the XML configuration file of Mobile Connect. The password must be at least 5 characters. • PIN and Confirm PIN (End user only)— Enter at least 5 characters. The PIN field is required, but Mobile Connect does not use a PIN. So, it does not matter what value you enter. • Enable Allow Control of Device from CTI (End user only). • Groups—Configure as part of “Standard CTI Allow Calling Number Modification” and “Standard CTI Enabled.”
4. Click Insert to add the user to the Cisco Unified Communications Manager database.	4. Click Save to add the user to the Cisco Unified Communications Manager database.
5. Click Device Association to associate the devices to the user and search for and associate all the devices you created in the “Creating a Pool of CTI Ports for Outgoing Calls” section on page 24.	5. Click Device Association to associate the devices to the user and search for and associate all the devices you created in the “Creating a Pool of CTI Ports for Outgoing Calls” section on page 24.
6. Select Check All in Search and No Primary Extension to add the pooled CTI ports to the CTI user.	6. Select Check All in Search and No Primary Extension to add the pooled CTI ports to the CTI user.
7. Choose Update.	7. Click Save.

Adding a User for a Shared Line CTI Port and Route Point

To add the user who controls the shared line CTI port and route point, follow the steps in [Table 12](#):

Table 12 **Shared Line CTI Port and Route Point User Settings**

Cisco Communications Manager 4.x	Cisco Unified Communications Manager 5.x
1. Log in to Cisco Communications Manager 4.x.	1. Log in to Cisco Unified Communications Manager 5.x.
2. Choose User > Add a New User .	2. Choose one of the following: User Management > Application User User Management > End User
3. Complete or enable these fields: - First Name and Last Name. - User ID—enter an alphanumeric identifier. Note The chosen names do not affect Cisco Unified MobilityManager, but using names with a common prefix such as CMM makes it easier to find later. - User Password and Confirm Password—Enter and confirm a password. The password is used for access to the XML configuration file of Mobile Connect. The password must be at least 5 characters. - PIN and Confirm PIN—Although the PIN field is required, Mobile Connect does not use a PIN, so it does not matter what value you enter. The PIN must be at least 5 characters. - Enable CTI Application Use. - Call Park Retrieval Allowed. - Enable Calling Party Number Modification.	3. Complete or enable these fields: - First Name and Last Name (End user only). - User ID—enter an alphanumeric identifier. Note The chosen names do not affect Cisco Unified MobilityManager, but using names with a common prefix such as CMM makes it easier to find later. - Password and Confirm Password—Enter and confirm a password. The password is used for access to the XML configuration file of Mobile Connect. The password must be at least 5 characters. - PIN and Confirm PIN (End user only)— Enter at least 5 characters. The PIN field is required, but Mobile Connect does not use a PIN. So, it does not matter what value you enter. - Enable Allow Control of Device from CTI (End user only). - Groups—Configure as part of “Standard CTI Allow Calling Number Modification” and “Standard CTI Enabled.”

Table 12 *Shared Line CTI Port and Route Point User Settings (continued)*

Cisco Communications Manager 4.x	Cisco Unified Communications Manager 5.x
4. Click Insert to add the user to the Cisco Unified Communications Manager database.	4. Click Save to add the user to the Cisco Unified Communications Manager database.
5. Click Device Association and enter the name of the route point and click Select Devices .	5. Click Device Association and enter the name of the route point and click Find .
6. Select Check All in Search and No Primary Extension .	6. Select Check All in Search and No Primary Extension .
7. Click Update .	7. Click Save .
8. Click Device Association .	8. Click Device Association .
9. Enter the prefix that you used when defining the shared line CTI ports (such as CMM_), choose Begins With , and click Select Devices . See the “ Creating a CTI Port for the Shared Line ” section on page 26.	9. Enter the prefix that you used when defining the shared line CTI ports (such as CMM_), choose Begins With , and click Find . See the “ Creating a CTI Port for the Shared Line ” section on page 26.
10. Select Check All in Search and No Primary Extension .	10. Select Check All in Search and No Primary Extension .
11. Click Update Selected .	11. Click Update Selected .

Using Active Directory with Cisco Unified Mobility Manager

To use Active Directory with Cisco Unified MobilityManager 5.x, follow these steps using Cisco Unified Communications Manager:

Procedure

-
- Step 1** Log in to Cisco Unified Communications Manager 5.x.
- Step 2** Configure the LDAP System settings.
- a. In Cisco Unified Communications Manager, choose **System > LDAP > LDAP System**.
 - b. Complete these fields:
 - Enable Synchronizing from LDAP Server—Select this option.

- LDAP Server Type—Choose Microsoft Active Directory.
- LDAP attribute for User ID—Choose sAMAccountName.

c. Click **Save**.

Step 3 Configure the LDAP Directory settings:

- a. In Cisco Unified Communications Manager, choose **System > LDAP > LDAP Directory**
- b. Complete these fields:
 - LDAP Manager Distinguished Name.
 - Perform Sync Just Once.
 - Host Name or IP Address for Server—Enter the host name or IP address of the server where the data for this LDAP directory resides.
 - Add Another Redundant LDAP Server—Click this option to add an additional server.
- c. Click **Save**.

Step 4 Configure the LDAP Authentication settings.

- a. In Cisco Unified Communications Manager, choose **System > LDAP > LDAP System**.
- b. Complete these fields:
 - Use LDAP Authentication for End Users—Select this option.
 - LDAP Manager Distinguished Name.
 - LDAP User Search Base.
 - Host Name or IP Address for Server—Enter the host name or IP address where you installed the corporate directory.

Setting Parameters for the Mobile Connect IP Phone Service in Cisco Unified Communications Manager

The Mobile Connect IP Phone Service, which is assigned to individual phones, enables users to determine the status of Mobile Connect functionality on their phones or to pick up calls at defined remote destinations.

To set parameters for the Mobile Connect IP phone service in Cisco Unified Communications Manager, follow the steps in [Table 13](#):

Table 13 **Mobile Connect IP Phone Service Settings**

Cisco Communications Manager 4.x	Cisco Unified Communications Manager 5.x
1. Log in to Cisco Communications Manager 4.x.	1. Log in to Cisco Unified Communications Manager.
2. Choose Feature > Cisco IP Phone Services .	2. Choose Device > Device Settings > Phone Services .
3. Click Add a New IP Phone Service .	3. Click Add New .
4. Complete the following fields:	
- Service Name—Enter Mobile Connect or another name for the service. - Description—Enter a description that identifies the service as Mobile Connect. - Service URL—Enter <code>http://<i>cmmpaddress</i>:8081/ip_phone/main.xml</code>, where <i>cmmpaddress</i> specifies the IP address of the server on which you have installed Cisco Unified MobilityManager. You must specify this case-sensitive field as lower case. - Character Set (Cisco Communications Manager 4.x only)—Confirm that this setting specifies Western European (Latin 1). - Service Name (ASCII Format) (Cisco Unified Communications Manager 5.x only)—Enter the name of the service to display if the phone cannot display Unicode.	
5. Click Insert .	5. Click Save .
6. To add a new parameter, click New .	6. To add a new parameter, click New .

Table 13 **Mobile Connect IP Phone Service Settings (continued)**

Cisco Communications Manager 4.x	Cisco Unified Communications Manager 5.x
7. Complete the following fields:	
- Parameter Name—Enter dn. You must specify the dn parameter as lower case. - Parameter Display Name—Enter Shared line directory number. If an incorrect directory number is configured, the pickup feature does not work. - Parameter Description—Enter an description, such as “Shared Line Directory Number,” that indicates that this is for a shared line. - Parameter is Required—Check this option. - Parameter is a Password—Leave unchecked.	
8. Click Insert and Close .	8. Click Save and Close .
9. Choose Device > Phone .	9. Choose Device > Phone .
10. Use Find to locate the phone to be used for the Mobile Connect service and click to open its Phone Configuration window.	10. Use Find to locate the phone to be used for the Mobile Connect service and click to open its Phone Configuration window.
11. Click Subscribe/Unsubscribe Services in the upper right portion of the window.	11. On the upper, right side of the window, choose Subscribe/Unsubscribe Services from the Related Links drop-down list box and click Go .
12. From the Select a Service drop-down list box, choose the service that you want to add.	12. From the Select a Service drop-down list box, choose the service that you want to add.
13. Enter the shared-line extension in the Shared Line Directory Number field, and click Subscribe .	13. Enter the shared line extension in the Shared Line Directory Number field, and click Subscribe .
Note The number entered in the Shared Line Directory Number field is not validated. If the desk phone number or extension is not entered correctly, the user cannot take advantage of Mobile Connect services.	Note The number entered in the Shared Line Directory Number field is not validated. If the desk phone number or extension is not entered correctly, the user cannot take advantage of Mobile Connect services.
14. Click Update and close the Service Subscription window.	14. Click Save and close the Service Subscription window.

Configuring H.323 Gateways for Mobile Voice Access

To configure H.323 gateways for Mobile Voice Access, you have two options available, depending on whether you are using PRI or not:

- [Configuring a H.323 Gateway for System Remote Access Using PRI, page 38](#)
- [Configuring a H.323 Gateway for System Remote Access Using Hairpinning, page 41](#)

Configuring a H.323 Gateway for System Remote Access Using PRI

If you already have an H.323 gateway configured in Cisco Unified Communications Manager, you can use it to support system remote access. If you do not have an H.323 gateway, then you must add and configure one. For more information, see the section on adding a Cisco IOS H.323 Gateway in the *Cisco Unified Communications Manager Administration Guide*.

**Note**

When a Mobile Connect call is placed from an internal extension, only the internal extension is presented as the caller ID. If an H.323 gateway is used, you can use translation patterns to address this issue.

To configure the gateway, follow these steps.

Procedure

Step 1 Configure the T1/E1 controller for PRI from PSTN.

Sample configuration:

- controller T1 1/0
- framing esf
- linecode b8zs
- pri-group timeslots 1-24

Step 2 Configure the serial interface for the PRI (T1/E1).

Sample configuration:

- interface Serial 1/0:23

- ip address none
- logging event link-status none
- isdn switch-type primary 4ess
- isdn incoming-voice voice
- isdn bchan-number-order ascending
- no cdp enable

Step 3 Load the VXML application from the Cisco Unified MobilityManager server.
Sample configuration for IOS Version 12.3 (13) and later:

- application service CMM
- <http://<Mobility Server IP Addr>:8080/cmmivr/pages/IVRMainpage.vxml>

Sample configuration before IOS Version 12.3(12):

- call application voice CMM
- <http://<Mobility Server IP Addr>:8080/cmmivr/pages/IVRMainpage.vxml>



Note Although, VXML was added in Version 12.2(11), Versions 12.3(8), 12.3(9), 12.3(14)T1, and 12.2(15) have VXML issues and should not be used.

Step 4 Configure the dial-peer to associate Mobile Connect application with system remote access.

Sample configuration for IOS 12.3(13) and later:

- dial-peer voice 58888 pots
- service cmm
- incoming called-number 58888
- no digit-strip

Sample configuration for IOS 12.3(12) and earlier:

- dial-peer voice 100 pots
- application CMM (*Mobile Connect VXML application*)
- incoming called-number 1234567 (*where 1234567 is the Mobile Voice Access number*)

- no digit-strip

Step 5 Add a dial-peer for transferring calls to the outgoing CTI port.

Sample configuration for primary Cisco Unified Communications Manager:

- dial-peer voice 101 voip
- preference 1
- destination-pattern <wild-card>



Note

The destination-pattern value should match the directory numbers for your outgoing ports. For example, if your outgoing ports are 16000 through 16999, configure destination-pattern 16...

- session target ipv4:10.1.30.3
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

Sample configuration for secondary Cisco Unified Communications Manager (if needed):

- dial-peer voice 102 voip
- preference 2
- destination-pattern <wild-card>



Note

The destination-pattern value should match the directory numbers for your outgoing ports. For example, if your outgoing ports are 16000 through 16999, configure destination-pattern 16...

- session target ipv4:10.1.30.3
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

Configuring a H.323 Gateway for System Remote Access Using Hairpinning

If you do not have an H.323 gateway, and do not want to connect a separate PRI to H.323 gateway and want to use H.323 gateway only to support System Remote Access, then you must add and configure one. For more information, see the section on adding a Cisco IOS H.323 Gateway in the *Cisco Unified Communications Manager Administration Guide*.

**Note**

When adding an H.323 gateway in Cisco Unified Communications Manager for hairpin configuration, you must check the Media Termination Point Required parameter. Without this parameter checked, calls might not complete properly for most gateway images

To configure the gateway, follow these steps.

Procedure

Step 1 Load the VXML application from the Cisco Unified MobilityManager server. Sample configuration for IOS Version 12.3 (13) and later:

- application service CMM
- http://<Mobility Server IP Addr>:8080/cmmivr/pages/IVRMainpage.vxml

Sample configuration before IOS Version 12.3(12):

- call application voice CMM
- http://<Mobility Server IP Addr>:8080/cmmivr/pages/IVRMainpage.vxml

**Note**

Although VXML was added in Version 12.2(11); however, Versions 12.3(8), 12.3(9), 12.3(14)T1, and 12.2(15) have VXML issues and should not be used.

Step 2 Configure the dial-peer to associate Mobile Connect application with system remote access.

Sample configuration for IOS 12.3(13) and later:

- dial-peer voice 1234567 voip
- service CMM

- incoming called-number 1234567
- codec g711u
- session target ipv4:<ip_address of call manager>

Sample configuration for IOS 12.3(12) and earlier:

- dial-peer voice 1234567 voip
- application CMM
- incoming called-number 1234567
- codec g711u
- session target ipv4:<ip_address of call manager>

Step 3 Add a dial-peer for transferring calls to the outgoing CTI port.

Sample configuration for primary Cisco Communications Manager:

- dial-peer voice 101 voip
- preference 1
- destination-pattern <wild-card>



Note

The destination-pattern value should match the directory numbers for your outgoing ports. For example, if your outgoing ports are 16000 through 16999, configure destination-pattern 16...

- session target ipv4:10.1.30.3
- voice-class h323 1
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

Sample configuration for secondary Cisco Communications Manager (if needed):

- dial-peer voice 102 voip
- preference 2
- destination-pattern <wild-card>



Note The destination-pattern value should match the directory numbers for your outgoing ports. For example, if your outgoing ports are 16000 through 16999, configure destination-pattern 16...

- session target ipv4:10.1.30.3
- voice-class h323 1
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

Step 4 Configure hairpin

- voice service voip
- allow-connections h323 to h323

Checking the Desk Phone Configuration

To use Cisco Unified MobilityManager, you do not need to change the configuration for any physical desk phone; however, Cisco recommends that you increase the timeout permitted before the voice-messaging system intercepts an incoming call. The normal default is 16 seconds before a call is redirected to a user's voice mailbox. For Mobile Connect, additional time may be needed for the call to be placed and answered on the remote extension. Refer to the *Cisco Unified MobilityManager Administration Guide* for information on setting timers.

When a call goes out over a voice gateway to the PSTN or cellular endpoint, a delay of approximately 20 seconds suffices for most carriers. Some trial and error experimentation will be required to determine the correct values for your system. Different values may apply for different users depending on the type of end point that is to be reached.

You can configure the Mobile Connect service as a speed dial. To do so, refer to the “Configuring Cisco IP Phones” section in the *Cisco Unified Communications Manager Administration Guide*.

Related Documentation

Refer to the following documents for further information about related Cisco Unified Communications applications and products:

Cisco Unified MobilityManager

Access these Cisco Unified MobilityManager documents at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_mobmg/index.htm

- *Cisco Unified MobilityManager Quick Start Guide*
- *Cisco Unified MobilityManager Installation Guide*
- *Cisco Unified MobilityManager Administration Guide*
- *Cisco Unified MobilityManager User Guide*
- *Release Notes for Cisco Unified MobilityManager*

Cisco Unified Communications Manager

Access the complete set of Cisco Unified Communications Manager documents at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help

solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

