Installation and Administration Guide for Cisco MediaSense

Release 8.5(1)

December 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0833

Table of Contents

List of Figures

Preface

Purpose

Cisco Unified Media Capture Platform (Unified MCP) is Cisco's media capture platform which uses Web 2.0 Application Programming Interfaces (APIs) to expose its functionality to third-party customers so they can create custom applications.

Audience

The *Installation and Administration Guide for Cisco Unified Media Capture Platform* is written for system administrators who have the domain-specific knowledge required to install, set up, configure, maintain, and troubleshoot the Unified MCP system. Experience or training with Java is not required but is useful for making best use of the capabilities of the Cisco Unified Communications family of products.

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example: • Choose **Edit** > **Find**. • Click **Finish**.
italic font	Italic font is used to indicate the following:

Convention	Description
	• To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • For emphasis. Example: *Do not* use the numerical naming convention. • A syntax value that the user must replace. Example: IF (*condition*, *true-value*, *false-value*) • A book title. Example: See the *Cisco CRS Installation Guide*.
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: **`<html><title>Cisco Systems,Inc. </title></html>`**
`< >`	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Documentation Feedback

You can provide comments about this document by sending email to the following address:

mailto:ccbu_docfeedback@cisco.com

We appreciate your comments.

Chapter 1

Introduction to Unified MCP

Unified MCP Architecture

Note: Product documentation may reÃect varying names that appear in the application user interfaces and application programming interfaces of this product. These names may include Cisco Unified Media Capture Platform (Unified MCP), Media Capture Platform (MCP/mcp), or Open Recording Architecture (ORA/ora).

Unified MCP is an IP media recording and playback system that implements the Media Recording Extensible (MRX) Architecture open interfaces. Unified MCP is part of the solution for Unified Communications, Release 8.5, and runs on Cisco Unified Operating System (Unified OS), Release 8.5.

The Unified MCP architecture contains the following components:

- Application Layer:
  - Search and play API capabilities allow you to play back recordings.
  - APIs support real-time recording controls (e.g. mute, mask, and pause) for third-party applications.
  - Application and Media APIs incorporate requirements from various industry partners and will be published for use by third-party applications.
  - The API Service provides web service interfaces to enable applications to search for and retrieve recordings and associated session (page 97) history and metadata. This metadata information is stored in the *Meta* database.
- Media Processing Layer:
  - The Media Service terminates media streams to be stored on a local disk for archiving and playback.

  - The Media Service running on all the servers in a deployment allows for load balancing.

- Network Layer:
  - Gateway/SBC media forking and media forking at endpoints.
  - Call Control interface supported by Unified CM.

Who Can Use Unified MCP?

Unified MCP can be used by compliance recording companies whose regulatory environment requires all sessions (page 97) to be recorded and maintained. These recordings can later be used by a compliance auditor or a contact center supervisor to resolve customer issues or for training purposes. These recordings can also be used by speech analytics servers or transcription engines. Unified MCP is not dependent on the use of any specific contact center product.. However, it is capable of working with all contact center products. Its' only dependency is Unified Communication Manager (Unified CM), which is used to set up the recording profile and call control service connection (SIP trunk) information.

Understanding Unified MCP Terminology

This section identifies the commonly used Unified MCP terms and provides a conceptual context for your reference and understanding.

Mapping a Session to a Recording

In the context of Unified MCP, a *session* is a recorded monologue, dialog, or conference which can involve one or more participants (page 96). A Unified MCP session is the same as a *recording session* in Unified CM. See the *Cisco Unified Communications Manager Features and Services Guide* available at **http://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/prod_maintenance_guides_list.html** for more information on recording sessions.

The participants (page 96) in a session use a device (page 94) to participate in a Unified MCP session.

A *device* is a physical entity that can be an end point or a personal computer and refers to any item that can be recorded. A device is identified by a deviceRef which is a phone number or extension for each device. The deviceId is the unique identifier for each device and it corresponds directly to the name of the device (like the MAC address or Universal Device Identifier--UDI).

A session can be *live* (active) or *recorded* (completed). A live session can be monitored and recorded at the same time. A recorded session can be played back at any time.

Playing Back Recordings

You can search for a session (page 97) and play the audio and/or video data for each session using the Unified MCP APIs. See the *Cisco Unified MCP Developer Guide* for more information.

You can play back Unified MCP recordings using the Real Time Streaming Protocol (RTSP) or by downloading the recording as an .mp4 file.

- **Playback**: You can playback Unified MCP recordings using any player which supports RTSP or .MP4 formats (for example, VLC--VideoLAN Client, or Quicktime). If you listen to a forked media recording using VLC, you can only listen to one track (page 97) at a time, and not both at the same time. With other players like Quicktime, you can listen to both tracks at the same time.

- **Download**: If you prefer to listen to both audio channels and view the video at the same time, export any Unified MCP recording to MP4 format (using the **`convertSession`** API). You can then download that file using standard HTTP access methods. Using the downloaded MP4 file, you can listen to both audio channels and view the video at the same time. Converting to MP4 also makes the file portable and allows you to copy it to a location of your choice.

- Client applications can communicate directly with the Unified MCP Media Service by using the **`downloadUrl`** parameter in the Session Query APIs. Each API will have a **`downloadUrl`** only for AUDIO tracks. You cannot download Unified MCP video tracks in the RAW format. The downloaded recording is only available in the RAW format. This URL is conditionally present in the session query response only if the **`sessionState`** is CLOSED_NORMAL or in the **`sessionEvent`** only if the eventAction is ENDED. For other sessions in other states, (ACTIVE, DELETED, or CLOSED_ERROR), **`downloadUrl`** is not available. See **http://en.wikipedia.org/wiki/Raw_audio_format** for more details on RAW formats.

While **`rtspUrl`** allows streaming, **`downloadUrl`** provides downloading capability. Consequently, the RTSP URL is provided for active sessions (page 97), while the downloaded URL is only available for closed sessions.

Media Forking

All Cisco IP phones, supported by Unified MCP, have a built-in bridge (BIB) which allow incoming and outgoing media streams to be forked. Unified MCP makes use of this capability to record inbound and outbound forked media. See the Unified CM documentation for more details on media forking. See **http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html**.

Blog Recording

Unified MCP enables you to create blog recordings (audio and video) using supported Cisco IP phones. Once recorded, third-party applications can publish these blog recordings.

A blog recording is initiated in one of the following ways:

- By a user who dials into an Unified MCP server.
- By the Unified MCP server calling a user's phone in response to an API request.

Unified MCP Requirements

This section identifies the general and specific requirements for Unified MCP.

- Hardware Requirements (page 6)
- Software Requirements (page 7)
- License Requirements (page 7)
- Other Requirements (page 7)
- Pre-Installation Requirements (page 7)

Media Storage Requirements

You must be aware of and address all media storage requirements before setting up the virtual machine (VM). For efficient storage management and optimal utilization you must provision adequate storage space for all media-related data (recording and meta data) *before* you deploy any Unified MCP servers. See the *Unified MCP Solution Reference Network Design* document for more information.

Hardware Requirements

Unified MCP, Release 8.5(1) is packaged with the Linux-based Unified Communications Operating System (OS), an appliance model developed by Cisco. Unified MCP uses Unified OS to integrate, communicate, and coordinate with Unified CM.

An approved server on which you install Unified MCP must meet the following hardware requirements:

- Approved Unified Computing System (UCS) servers. For a list of approved UCS servers, see the server requirements and version compatibility with Unified CM sections in the *Hardware & System Software Specification (Bill of Materials) for Cisco Unified Contact Center Enterprise Guide* available at **http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_user_guide_list.html**.
- Unified MCP does not co-reside with any product, including Unified CM. Unified MCP requires a dedicated server.

- Virtual Machine (VM) requirements specific to Unified MCP are available at **Virtualization for Cisco MediaSense:** (http://docwiki.cisco.com/wiki/Virtualization_for_Cisco_MediaSense)).

  For details on VM templates, ESXi, sizing information , and other VM-specific process details see **Unified Communications Virtualization:** (http://cisco.com/go/uc-virtualized).

- See the *Release Notes for Cisco MediaSense, Release 8.5(1)* on Cisco.com (CDC) for more information on hardware limitations.

Software Requirements

Unified MCP must meet the following software requirements:

- The required Unified CM cluster must already be configured and deployed before you set up Unified MCP.
- The Unified MCP Administration web interface uses approved web browsers. For a list of approved web browsers, see the *Cisco Unified Contact Center Hardware and Software Compatibility Guide* available at the following website: **http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_device_support_tables_list.html**.

License Requirements

The primary licensing and feature activation method for Unified MCP is trust-based licensing.

Unified MCP does not require any licenses from Cisco Systems for this release.

Other Requirements

All other requirements to use Unified MCP are identified in this section.

- Uninterrupted power supply to the Unified MCP server at all times (to prevent unpredictable behavior due to power failure).
- While most of these requirements are intended before you install Unified MCP, you will also need to follow the specified Post-Installation Requirements (page 18) to ensure a smooth configuration and maintainance process.

Pre-Installation Requirements

For a list of approved hardware and software versions, refer to the *Cisco Unified Contact Center Hardware and Software Compatibility Guide* available at the following website: **http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_device_support_tables_list.html**.

Before proceeding with the Unified MCP installation, ensure to address the following requirements:

- Planning for the Unified MCP Installation (page 8)
- Important Installation Considerations (page 8)
- Completing the Installation and Configuration Worksheet (page 9)

Planning for the Unified MCP Installation

A Unified MCP cluster consists of one to three Unified MCP servers:

- Be sure to perform a thorough analysis of all storage requirements prior to installationAfter installation, it is not possible to change any storage-related settings (see Media Storage Requirements (page 6)).
- The first server installed in any cluster is referred to as the*primary* server. All feature services (see Understanding Unified MCP Services (page 19) for more details) are automatically enabled in this server during the installation process.
- All servers in a Unified MCP cluster must always must have a functioning Call Control Service (page 21) and Media Service (page 21).
- A Unified MCP cluster with multiple servers must also have one API Service (page 20), one Configuration Service (page 20), and one Database Service (page 20) in two servers in the cluster. Once these three services are assigned to the primary server (during the installation process), you can assign these services to one other server in the same cluster after the installation process. The server which has all feature services enabled becomes the*secondary* server.
- The remaining servers in the cluster are called *expansion* servers. Expansion servers do not have the API Service, the Configuration Service, or the Database service. They will only have the Call Control Service, the Media Service, and the SM Agent (page 21).

Important Installation Considerations

Unified MCP supports the following deployments in this release:

- Single-server deployment: One active server (page 93)
- Dual-server deployment: Two active servers (page 93) providing high availability (page 95).
- Triple-server deployment: Two active servers (page 93) providing high availability (page 95) and one expansion server (page 95) to provide additional recording capacity.

In all the deployment scenarios, the installation for the primary server varies from the installation for other servers in the same deployment. If you are configuring the primary server in any Unified MCP deployment, be aware that the platform administrator will configure the Unified MCP application administrator username and password (in addition to the platform and security password). See theInstalling the Unified MCP Software (page 13) section for further details.

Note: The application administrator's username and password must be the same in all servers in a Unified MCP deployment. You can reset the application administrator username and password using the **`utils reset_application_ui_administrator_name`** and the **`utils reset_application_ui_administrator_password`** CLI commands.

Completing the Installation and Configuration Worksheet

Use this worksheet to document network and password information that both the installation and set up wizard prompt you to enter. Store this worksheet information for future reference.

Use the following table to document information about your server that the basic installation wizard prompts you to enter. Gather this information for each Unified MCP server that you install. You may not need to obtain all the information; gather only the information that is pertinent to your system and network configuration. You should make copies of this table and document your entries for each server in a separate table so it is easy to configure your system.

Caution: If you record the relevant information in this table, be sure to store the recorded information in a secure location.

Table 1: Unified MCP Installation and Configuration Worksheet

Installation Data	Your Entry	Notes
Platform administrator information	Username: Password:	Information used to log into the Unified Communications Operating System Administration.
Unified MCPapplication administrator information	Username: Password:	Information used to log into the Unified MCP Administration. You can change the entry after installation by using the following CLI commands: **`utils reset_application_ui_administrator_name`** **`utils reset_application_ui_administrator_password`**
Unified MCPcluster deployment information	Primary server IP address: Secondary server IP address: Expansion server IP address:	All servers in the Unified MCP cluster must have the same username and password.

Installation Data	Your Entry	Notes
The MTU size in bytes for your network. This setting must be the same on all nodes in a cluster.	MTU size:	If you are unsure of the MTU setting for your network, use the default value. Default: 1500 bytes
NIC speed is either 10 megabits per second or 100 megabits per second. This parameter only displays when you choose not to use Automatic Negotiation.	NIC Speed:	Check with your network administrator for further guidance on this setting.
Static Network Configuration	IP Address: IP Mask: Gateway:	Provide this information if you are *not* configuring DHCP.
DNS Client Configuration	Primary DNS: Secondary DNS (optional): Domain:	Provide this information if you are configuring DHCP. **Caution: A Unified MCP server's IP address or hostname cannot be changed after installation. Use DNS and hostnames in your deployment to keep your Unified MCP cluster independent of the underlying IP configuration.**
NTP or Hardware Clock configuration for the first node. Set the NTP for other servers in the Unified MCP deployment to the time on the first server.	Hostname or IP address of the first server:	You must specify at least one (three NTP server details are preferred) valid and reachable NTP server.
Enter the same security password for all servers in the Unified MCP deployment.	Security password	The security password must contain at least six alphanumeric characters. It can contain hyphens and underscores, but it must start with an alphanumeric character. You can change the entry after installation by using the following CLI command: **`set password security`**
SMTP Location used for outbound calls.	Hostname or IP address for the SMTP server:	The hostname can contain alphanumeric characters, hyphens, or periods, but it must start with an alphanumeric character.

Chapter 2

Installing Unified MCP

This section describes how to install the Cisco Unified Operating System (Unified OS) and the Unified MCP application. You install the operating system and application by running one installation program.

Before you proceed with installing the Unified MCP application, be sure to review and meet the Pre-Installation Requirements (page 7).

This section included the following subsections:

This chapter contains the following topics:

Installing the Software

The installation process deploys the Unified MCP application and the Unfied Communications Operating System (Unified OS) from the provided media (the DVD disc).

To install the Unified MCP software, you should have already addressed the following pre-requisites:

- Addressed all virtual machine (VM) requirements for this deployment.

This document assumes the following information:

– You are familiar with the VMware toolset.

– You have already mounted and mapped the DVD drive to the VM host DVD device (physical DVD drive with the DVD disk inserted) or you have mounted your DVD drive to the datastore ISO file.

– You have already powered on your VM server in preparation for this installation.

– You have to address all the VM requirements listed in the **http://cisco.com/go/uc-virtualized** (http://cisco.com/go/uc-virtualized) website.

A basic installation allows you to install the Unified MCP, Release 8.5(1) software from the installation disc and configure it with one DVD insertion. The disc contains the Unified Communications Operating System (Unified OS) and the Unified MCP installer application. When you run a Unified MCP installation program, you install the Unified OS and Unified MCP application at the same time.

Note: The primary server (page 96) must be up and functioning (at least the network services) for any subsequent server to be installed from the DVD.

This section includes the following subsections:

Navigating within the Installer Wizard

For instructions on navigating within the installation wizard, see the following table:

Table 2: Unified MCP Installation Wizard Navigation

To perform this function	Follow this action
Move to the next field	Tab
Move to the previous field	Alt-Tab
Choose an option	Space bar or Enter
Scroll up or down in a list	Up or Down arrow
Go to the previous window	Space bar or Enter to choose Back (when available)
Get help information on a window	Space bar or Enter

Note: During installation it is possible for your monitor screen to go blank if you left it unattended for a period of time. In such a situation, do not use the Space barPressing the Space bar selects the default option available on the current window and moves to the next window. Instead, press Escape on your keyboard to display the current screen with the available options and proceed with the installation.

Installing the Unified MCP Software

To install the Unified MCP application and the Unified OS, follow this procedure.

Note: At any time during the installation process, you can click **Help** to get further information about that particular screen.

Caution: The installation process is different for the primary server and for all other servers in a deployment. Once you have identified and assigned your primary and secondary servers, you will not be able to change the assignment. Be sure to carefully identify these two servers before you install or configure them.

Verify that you have already addressed all VM requirements listed in the **http://cisco.com/go/uc-virtualized** (http://cisco.com/go/uc-virtualized) website.

Step 1 Insert the Unified MCP installation disc into the DVD tray and restart the server, so it boots from the DVD. After the server completes the boot sequence, the DVD Found window displays.

Step 2 To perform the media check, select **Yes**. To skip the media check, select **No.**

The media check verifies the integrity of the installation disc. If your disc passed the media check previously, you may choose to skip this step.

a. If you choose to perform the media check, the Media Check Result window displays with the progress bar for the media check.

Note: Depending on your server setup, the media check can take approximately five minutes to complete.

b.

If: If the Media Check Result displays PASS,

Then: click **OK** to continue the installation.

If: If the media check fails,

Then: eject the DVD to terminate the installation.

At this point you have several choices depending on your service-level agreement:

- Download another copy from Cisco.com (CDC)
- Obtain another installation disc directly from Cisco
- Contact your service provider for assistance

Step 3 The system installer performs the following hardware checks to ensure that your system is correctly configured. If the installer makes any changes to your hardware configuration settings, you will get prompted to restart your system.

a. First, the installation process checks for the correct drivers, and you may see the following warning: .

No hard drives have been found. You probably need to manually choose device drivers for install to succeed. Would you like to select drivers now?

To continue the installation, choose **Yes.**

b. The installation next checks to see whether you have a supported hardware platform. If your server does not meet the exact hardware requirements, the installation process fails with a critical error. If you think this is not correct, capture the error and report it to your service provider.

c. The installation process next verifies RAID configuration and BIOS settings.

If the installation program must install a BIOS or RAID update, a notification appears telling you that the system must reboot. Press any key to continue with the installation.

When the hardware check completes, the Product Deployment Selection screen is displayed.

Step 4 The Product Deployment Selection screen states that Unified MCP will be installed. Click **OK** to proceed with the Unified MCP installation.

The installation process begins.

Step 5 Select **Yes** if you agree with the information displayed in the Proceed with Install screen. If you select No at this point, the installation is cancelled.

The Proceed with Install screen displays any pre-existing version of Unified MCP on the hard drive (if any) and the version available on the disc. For the initial installation of Unified MCP, the version on the hard drive is displayed as **NONE.**

Step 6 Select **Proceed** in the Platform Installation Wizard screen to set up the initial configuration for the Unified MCP platform.

If you choose to Skip the initial configuration, then you have the option to complete the initial configuration when the OS installation ends.

Step 7 Select **No** in the Apply Patch screen if you do not need to apply the patch.

The software installation begins immediately after you click **No** (if your are not installation a patch).

Caution: If a critical error occurs during installation, you are prompted to collect log files. To do this, insert a USB memory key in any available USB port and follow the instructions on the screen.

During the installation process (from Step 8 to Step 19), the monitor shows a series of processes. You see:

- Formatting Progress Bars
- Copying File Progress Bar
- Platform Installation Progress Bars
- Post Install Progress Bar
- Application Installation Progress Bars
- A System Reboot Messages appear during the reboot, some of which prompt you to press a key. Do not respond to these prompts to press a key.

Note: During the reboot, the VM prompts you to eject the DVD. This is normal. You can retrieve your disc at this point and close the tray.

Step 8 Click **Continue** in the Basic Install screen. (This screen only appears for a fresh installation.)

If you do not click **Continue** at this point, this screen remains in this state if you do not click Continue.

The Basic Install screen launches the set up configuration wizard—a series of screens with options pertinent to your Unified MCP deployment.

Note: You can change many of the basic network installation configuration settings after the installation using the `set` Unified Communications CLI commands (for example, `set network` and verify the changes using the `view network` command).

Step 9 Use the down arrow to select the local timezone (closest match to your server location) in the Time Zone Configuration screen, and click **OK**.

Caution: The timezone field is based on city/country and is mandatory. Setting it incorrectly can affect system operation.

Step 10 In the Auto Negotiation Configuration screen, select whether or not you want to use automatic negotiation for the settings of the Ethernet Network Interface Card (NIC).

a. **If:** The ethernet NIC is attached to your hub or the Ethernet switch supports automatic negotiation,

Then: select **Yes** and proceed to the MTU Configuration screen.

If: You want to disable automatic negotiation and specify the NIC speed and duplex settings,

Then: Select **No** and proceed to the NIC Speed and Duplex Configuration screen to manually configure these settings.

Step 11 In the NIC Speed and Duplex Configuration screen, configure the following settings:

a. Specify the speed of the NIC in Megabits per second. Speed options are 10 or 100.

Note: Only full duplex setting of the NIC server is supported for the 10/100 megabit speed. With Gigabit, auto-configuration is also supported. Check with your network administrator to configure the required settings for your deployment.

b. Select **OK**.

Step 12 In the MTU Configuration screen, select **No** to keep the default setting (1500).

If you choose to change this configuration, check with your network administrator to configure the required settings for your deployment.

The MTU represents the largest packet, in bytes, that this host will transmit on the network. If you are unsure of the MTU setting for your network, use the default value.

Caution: If you configure the MTU size incorrectly, your network performance can be affected.

Step 13 In the DHCP Configuration screen, select your preferred Dynamic Host Configuration Protocol (DHCP) mode for this server.

Check with your network administrator to configure the required settings for your deployment.

If you select **Yes** in this step, you can skip Step 14 and go directly to Step 15.

Step 14 If you select **No** in the previous step, you see the Static Network Configuration window, enter the required values in the following fields: IP Address, IP Mask, and Gateway (GW) Address. Click **OK**.

A configuration and network setup script runs.

Step 15 In the DNS Client Configuration screen, select **No** to disable DNS.

Caution: A Unified MCP server's IP address or hostname cannot be changed after installation. Use DNS and hostnames in your deployment to keep your Unified MCP cluster independent of the underlying IP configuration.

If you enable DNS in this screen, you will need to provide the DNS server details in the following DNS Client Configuration screen (Primary DNS, Secondary DNS [Optional] , and Domain).

Caution: To display both IP addresses, you must configure the Domain Name Server (DNS) suffix information (for the required nodes in the cluster) in the server in which Unified MCP is installed. If you plan to install the Unified MCP software without DNS information, then make sure you provide only the IP Address as reference instead of host names in all servers in this Unified MCP cluster. See the Command Line Interface Reference Guide for Cisco Unified Communications Solutions guide at https://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html for more information.

Step 16 In the Administrator Login Configuration screen, enter the Administrator ID of the Unified OS (platform) administrator for this deployment. Also enter and confirm the password for this administrator. Select **OK**.

Step 17 In the First Node Configuration screen, select **Yes** if you are configuring the first server for this Unified MCP deployment. Go to Step 18.

If you are configuring any other server, then select **No.** Go to Step 19.

Step 18 Complete the Network Time Protocol Client Configuration screen. Click **OK**.

This configuration only applies if you are configuring the first server in a Unified MCP deployment. It does not apply if you are configuring any of the other servers in the same deployment.

The first server in a Unified MCP deployment can get its time from any external Network Time Protocol (NTP) server that you define—or—from a time that you set on the Hardware Clock screen. NTP or Hardware Clock configuration is only set for the first node. For other servers in the deployment, you must set their time to the time on the first server.

Note: You must specify at least one (three NTP server details are preferred) valid and reachable NTP server.

Step 19 In the Security Configuration screen, enter the same security password on all servers in the cluster (page 94). This password is used by the servers in the cluster to communicate with each another. You must enter the same security password for all servers. Select **OK**.

This security configuration only applies if you are configuring the first server in a Unified MCP deployment. It does not apply if you are configuring any of the other servers in the same deployment.

The security password defined in the installation wizard is used by the system for the database security password to authorize communications between devices (page 94). This password must be identical on all servers in the cluster. You can change the security password using the CLI command **`set password security`**.

Note: The Security password must start with an alphanumeric character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores. The system uses this password to authorize communications between Unified MCP servers, and you must ensure this password is identical for all servers in a Unified MCP cluster.

a. **If:** If you are adding subsequent servers,

Then: You will need to provide the IP address and the host name of the first server along with this security password. Once you provide this information, you go skip the remaining steps and go directly to Step 22.

If: If you are not adding any other servers,

Then: Keep a record of this password; you will need to provide this password if you add a subsequent server. Once you note down the password, go to Step 20.

Step 20 In the SMTP Host Configuration screen, select **No** to disable SMTP host configuration.

Note: Simple Mail Transfer Protocol (SMTP) is only used for email notifications and this feature is not required by Unified MCP.

If you want to configure a SMTP server for your system, select **Yes**, enter the SMTP host name or IP address in the SMTP Host Configuration window, and click **OK**.

The Application User Configuration screen displays.

Step 21 In the Application User Configuration screen, enter the user information for the application user. Enter and confirm the application user password. Click **OK**.

The Unified MCP application administrator is different from the Unified MCP application administrator. This configuration difference is only visible if you are configuring the first server in a Unified MCP deployment. It is not visible if you are configuring any of the other servers in the same deployment.

See Configuring Unified CM User Information in Unfied MCP (page 44) for more information on configuring Unified CM users.

Step 22 In the Platform Configuration Confirmation screen, select **OK** to proceed with the installation.

The installation process continues (may take several hours depending on your configuration setup, your hardware setup, disk size, and other factors). A VM dialog prompts you to disconnect the DVD. Click **Yes** to disconnect and restart the system. On completing the installation procedure, the system restarts automatically. You must explicitly login to the Unified MCP Administration for the required server.

Note: To complete the server setup in any Unified MCP deployment, the Administrator must access and configure the Unified MCP Post-Installation Setup wizard, also referred to as the setup wizard..

Post-Installation Requirements

After installing Unified MCP on your server, you must set some configuration parameters and perform other post-installation tasks before you start using the system. See the following table for a list of post-installation tasks.

Task #	Task Description	Notes
1	Perform the installation setup for the primary server in your Unified MCP deployment.	See Completing the Installation for the Primary Server (page 28) to perform this task.
2	Add subsequent servers.	See Adding Subsequent Server Information to the Primary Server (page 32)
3	Perform the installation setup for subsequent servers in your Unified MCP deployment.	See Completing the Installation for Subsequent Servers (page 33)to perform this task.

Understanding Unified MCP Services

Once you have installed the Unified MCP application and rebooted your server, you need to be aware of the following services:

Network services: When you reboot your server after the installation process, the network services are enabled by default on all servers in a cluster. Network services allow you to configure and monitor overall system functions.

- Unified MCP Administration (page 37): This service allows you to configure the Unified MCP application using the graphical user interface.
- Unified MCP Serviceability Administration (page 55): This service allows you to configure the Unified MCP Serviceability application using the graphical user interface.
- Unified MCP System Service: This network service controls service operations within Unified MCP clusters. Unlike other Unified MCP network services, it does not have a separate UI . Like other network services, the System Service is operational at start up. This service manages the clustering and setup functionality for the secondary server and expansion server(s).
- Unified MCP Perfmon Agent: This network service controls the performance monitoring infrastructure. It does not have a separate UI and operates seamlessly within the Unified MCP Serviceability Administration. Like other network services, the Perfmon Agent is operational at start up. The Java Management Extensions (JMX) technology which allows you to manage and monitor applications and other system objects are represented by objects called Managed Beans (MBeans). The Perfmon Agent retrieves the counter values from the JMX MBeans and writes it to the Unified CM database.

Feature services: Each Unified MCP deployment contains the following feature services.

- Configuration Service (page 20)
- API Service (page 20)
- Media Service (page 21)
- Call Control Service (page 21)
- Database Service (page 20)
- SM Agent (page 21)

Note: Each feature service is always preceded by the product name, Unified MCP. To avoid redundancy in this document, all service names are referred to without the preceding product name. In both administration interfaces, each feature service name is preceded by the Unified MCP in all references.

Unified MCP Feature Services have the following dependencies:

- The primary (first) server and secondary server (a subsequent server with all services enabled) in a Unified MCP cluster contain all feature services listed in this section. The remaining servers in a cluster, referred to as *expansion servers*, only contain the (Media Service (page 21), Call Control Service (page 21), and SM Agent (page 21)).
  - Once you have installed the Unified MCP application and rebooted your server, all feature services are *enabled by default on the primary server* (primary server) in a cluster.
  - Once you access the Unified MCP Administration (page 37), and enable all feature services in that server, this server automatically becomes the secondary server. Once all feature services are enabled in the secondary server, you can only enable the Media Service (page 21), Call Control Service (page 21), and SM Agent (page 21) in the remaining servers in the cluster.
- While the service activation order is controlled by the system, the following information is pertinent when you manually enable services from the Unified MCP Serviceability Administration (see Using Unified MCP Serviceability Administration Tools (page 60)).
  - The Database Service (page 20) must be enabled first, followed by the Configuration Service (page 20), and then the API Service (page 20).
  - The Call Control Service (page 21) can only be enabled if the Media Service (page 21) is already enabled.
  - The SM Agent (page 21) can only be enabled if the Media Service (page 21) is already enabled.

Configuration Service

In the Unified MCP platform, the Configuration Service saves and updates all configuration changes made to the Unified MCP database,

Each Unified MCP cluster (page 94) can only have two instances of the Configuration Service in each multi-node deployment, with only one instance in the primary server and the other instance in the secondary server.

If a Unified MCP cluster has more than two servers, the additional servers will not have a Configuration Service, Database Service , or API Service.

API Service

The API Service can only be enabled if the Database Service (page 20) is already enabled.

Each Unified MCP cluster (page 94) can only have two instances of the Application Programming Interface (API) Service in each multi-node deployment, with only one instance in the primary server and the other instance in the secondary server.

If a Unified MCP cluster has more than two servers, the additional servers will not have a Configuration Service, Database Service, or API Service.

Database Service

The API Service (page 20) and the Configuration Service (page 20) can only be enabled if the Database Service is already enabled.

Each Unified MCP cluster (page 94) can only have two instances of the Database Service in each multi-node deployment, with only one instance in the primary server and the other instance in the secondary server.

The Database Service contains and controls the two Unified MCP databases.

Once you have installed the Unified MCP application and rebooted your server the following databases capture all Unified MCP-related information:

- Meta database: Stores call history and metadata information associated with each recording. This metadata supports the ability to search, play, export, and otherwise manage recordings with various characteristics. The Meta database directly corresponds to the API service.
- Configuration database: The configuration database, often referred to as the Config database stores the configuration information for the entire Unified MCP system. The Config database directly corresponds to the Configuration Service.

The two main servers containing the two databases are not tied down to the local databases in each server. They are both capable of interacting with the database in the other server. Both servers only write data to their local database. They do not write data to the remote database. Data between the two servers are synchronized using Informix Enterprise Replication (ER) technology.

Media Service

The Media Service must be enabled before the Call Control Service (page 21). This service is available in all servers in the cluster.

Call Control Service

The Call Control Service can only be enabled if the Media Service (page 21) is already enabled. This service is available in all servers in the cluster.

SM Agent

This service monitors the overall storage in each server in the Unified MCP cluster and generates threshold events based on disk usage. This service is available in all servers in the cluster.

Understanding Unified MCP Clusters

Cluster architecture accommodates high availability (page 95) and failover--if the primary server fails, there is automatic failover to the secondary server. The primary and secondary servers in a Unified MCP deployment are synchronized when administrative changes are made on either server. The system uses database replication to copy the data automatically from the primary server to the secondary server and vice versa. In a Unified MCP deployment, a cluster contains a set of servers, with each server containing a set of services.

A Unified MCP deployment can consist of one to three Unified MCP servers. Each server in a Unified MCP cluster must always have a running Call Control Service (page21), Media Service (page 21), and SM Agent (page 21).

Caution: Unified MCP does not co-reside with any product, including Unified CM. Unified MCP requires a dedicated server. No other Cisco product can be installed on the same VM running Unified MCP.

Adhere to the following guidelines when configuring Unified MCP clusters (page 94) (these guidelines are enforced by the installation and initial configuration procedures):

- All servers in the cluster must run the same version of Unified MCP and must be reachable through your network.
- A Unified MCP deployment cannot have more than three servers running Call Control Service (page 21) and Media Service (page 21) in the cluster.
- A Unified MCP deployment cannot have more than two servers running the API Service (page 20), Configuration Service (page 20), and Database Service (page 20) in the cluster. Both servers must have one instance of the API Service and one instance of Configuration Service; so each API Service has a corresponding Configuration Service in each server.

Be aware of the following characteristics when configuring clusters:

- If a service goes ofÃine for any reason, then all active recordings on that service are affected.
- High availability (page 95) is provided for recording, but not for playback.
- WAN deployments are not supported for any Unified MCP scenario. All nodes must be deployed over LAN.

  Note: High availability (page 95) servers should be in the same campus network. *Campus* refers to the close proximity of the servers to ensure that the servers are within the LAN. The Unified MCP servers must be located in the same campus network as the Unified CM servers (see **Designing Campus Networks** (http://www.ciscopress.com/articles/article.asp?p=25259) for more information on campus networks). The maximum round-trip delay between any pair of servers in a campus network must be less than 2ms.

- Recording of mid-session (page 97) failure is not supported. If the recording has been successfully started, and the Media Service (page 21) stops functioning while the session is in progress, then the entire recording for this session will not be available.

Each deployment with one or more servers is considered a cluster (page 94).Unified MCP can have any one of the following deployment scenarios:

- Single-server Deployment (page 23): This scenario does not allow high availability (page 95) capabilities,
- Multiple-server deployments: Deployments with two or more servers provide redundancy and allow you to increase storage and simultaneous recording capacity.
  - Dual-server Deployment (page 24): This scenario allows high availability as it contains one primary server and one secondary server.
  - Three-server Deployment (page 25): This scenario allows high availability as it contains one primary server, one secondary server, and one expansion servers which provide additional storage and recording capacity.

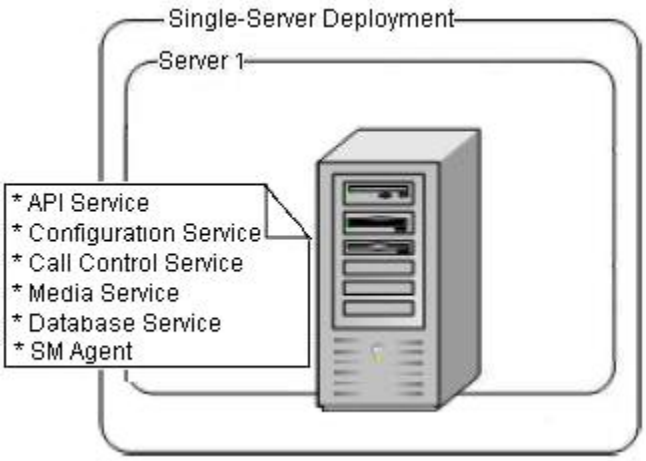
Single-Server Deployment

A single-server deployment indicates that this scenario has a single Unified MCP server on the Unified Communications OS platform.

Single-server deployments contain the following Unified MCP services:

- Configuration Service (page 20)
- API Service (page 20)
- Media Service (page 21)
- Call Control Service (page 21)
- Database Service (page 20)
- SM Agent (page 21)

Figure 1: Single-Server Deployment



Single-server deployments have the following features:

- Supports a maximum of 300 simultaneous recordings/playback/monitoring sessions (page 97).
- Supports a Busy Hour Call Completion (BHCC) Of 9,000 session (page 97) per hour, with each call having a two-minute average duration..
- Does not provide any high availability (page 95) options.
- Allows you to add on more servers to address redundancy issues and to increase storage and simultaneous recording capacity.

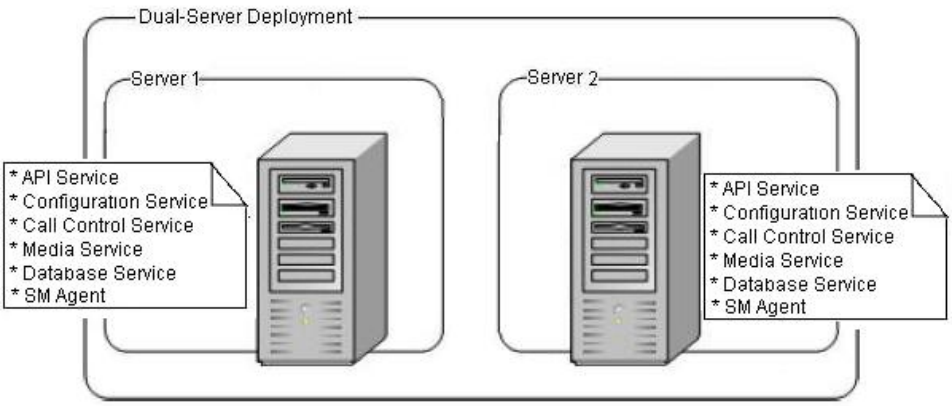
Dual-Server Deployment

A dual-server deployment indicates that this scenario has two Unified MCP servers on the Unified Communications OS platform.

Dual-server deployments contain the following Unified MCP services in *each* server:

- Configuration Service (page 20)
- API Service (page 20)
- Media Service (page 21)
- Call Control Service (page 21)
- Database Service (page 20)
- SM Agent (page 21)

Figure 2: Dual-Server Deployment



Dual-server deployments have the following features:

- All services are always active on both servers, hence the recording load is automatically balanced across both nodes.

  Note: Unified MCPdoes not provide automatic load balancing in theAPI and Configuration services. While those services are enabled on both servers, you must point your browser or server-based API to one of these services.

- See the *Unified MCP Solution Reference Network Design* guide for details on the maximum number of simultaneous recordings/playback/monitoring sessions (page 97).

- The simultaneous calls for both single-server and dual-server deployments is the same. By adding the second server, Unified MCP provides high availability (page 95). If one server goes down, the other server can handle the entire load in generic cases. However, this response also depends on the number of simultaneous calls in the Unfied MCP system. If each server is already handling the maximum number of calls, then that server will not be able to cover the failed server.

- Add on more servers to address redundancy issues and increase storage and simultaneous recording capacity.

Three-Server Deployment

Three-server deployments contain the following Unified MCP services in *two* of the three servers:

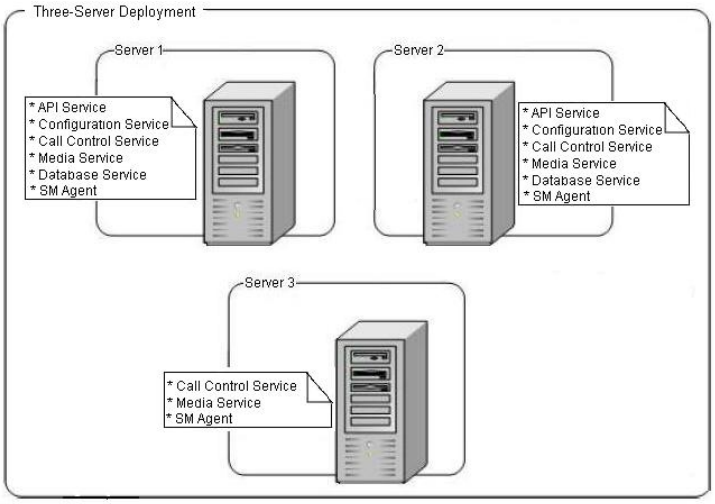
- Configuration Service (page 20)
- API Service (page 20)
- Media Service (page 21)
- Call Control Service (page 21)
- Database Service (page 20)

- SM Agent (page 21)

The remaining server, referred to as *expansion server*, contain the following Unified MCP services:

- Call Control Service (page 93)
- Media Service (page 95)
- SM Agent (page 21)

Figure 3: Three-Server Deployment



Three-server deployments have the following features:

- All the services are always active on their respective servers, hence the recording load is automatically across the three servers.

  Note: Unified MCPdoes not provide automatic load balancing in theAPI and Configuration services. While those services are enabled on both servers, you must point your browser or server-based API to one of these services.

- See the *Unified MCP Solution Reference Network Design* guide for details on the maximum number of simultaneous recordings/playback/monitoring sessions (page 97).

- If one server goes down, the other server can handle the entire load in generic cases. However, this response also depends on the number of simultaneous calls in the Unified MCP system. If each server is already handling the maximum number of calls, then that server will not be able to cover the failed server.

- This model adds redundancy as well as increases the storage and simultaneous recording/playback capacity.

High Availability in Unified MCP Deployments

Some deployment scenarios require all available media to be recorded. The high availability feature is imperative for Call Control services (page 93) deployed in these scenarios. A Call Control Service (page 93) failure may end up with no recordings unless your deployment supports high availability. If the Unified CM application is unable to contact one of the Unified MCP servers, you must ensure that an alternate server is available for Unified CM to make the required connection.

Considerations for Data Replication

Database high availability support in Unified MCP deployments is provided using Informix Enterprise Replication (ER) for both the Meta database and Config database. While an Unified MCP cluster can have up to three servers, data replication is only enabled between the primary server and secondary server.

At installation time, if the server being installed is identified as a secondary server, then the following considerations apply to this server:

- This server will automatically apply the ontape backup from the primary server without any constraints on the data size in the primary node.
- Data replication is performed between the primary and secondary servers. So, data written to the primary server is also replicated to the secondary server, and vice versa.

Caution: If the server being installed is a primary server, the above considerations do not apply.

The replication behavior between the primary and secondary Unified MCP servers differs based on the time of replication:

- **Activation time**:During the service activation process, Informix ER automatically begins replication between the primary and secondary servers. The differential data between both servers are replicated from the primary server to the secondary server.
- **Run time**: During run time, data replication is bidirectional. For any reason, if the one of the Unified MCP servers is shutdown or in a failed state, data continues to be written to the surviving server. When the shutdown/failed server is revived, Informix ER automatically restarts between the two servers and synchronizes the data. Depending on the data size, this synchronizing time may vary. *Retention period* refers to the numbers of days for which data can be stored on the surviving server, without breaking the replication. See the *Unified MCP Solution Reference Network Design* guide for details on the database retention period recommendations.

Considerations for Unified MCP High Availability Deployments

Follow these guidelines to ensure highly-available deployment and to provide data replication:

- Verify that the API Service is enabled and running: The API Service monitors its internal performance in order to provide overload protection. If an overload condition is detected, the API Service may begin to automatically reject third-party requests. Client applications should have the ability to retry requests on the alternate API Service if they receive rejections.

- A deployment can contain up to three possible Call Control Services in the cluster. The Unified CM uses a round-robin method to reach an available Call Control Service to place an outbound call. Otherwise, it tries to place a call to the next Call Control Service and times out after the last Call Control Service.

Primary Server Post-Installation Process

To complete the installation for the primary server, you should have already installed Unified MCP on this server and completed the following tasks during the installation process:

1. Entered the Network Configuration information for the machine (Unified OS requirement).

2. Identified this server as the "first node" (Unified OS requirement).

3. Configured the User ID and password for the Cisco Unified Communications platform administrator and the Unified MCP application administrator.

4. Once you have completed the installation process and the system restarts, you see the Unified MCP First Server Setup Wizard.

Completing the Installation for the Primary Server

The Unified MCP deployment model is transparent to the Unified MCP installer as the clustering for Unified MCP is performed through the Unified MCP Administration interface using the Unified MCP Post-Installation Setup wizard.

The post-installation setup procedure that you perform depends on the following answers:

- Access to Unified CM is required to continue with the Unified MCP installation.

  Do you have the Unified CM IP address, AXL Admin username, and AXL Admin Password to continue with the post-installation tasks.

- Did you review the considerations listed for the required deployment?

  Separate sections are available for the following deployments

  - Single-server Deployment (page 23)

  - Dual-server Deployment (page 24)

  - Three-server Deployment (page 25)

- Determine the Recording Retention Modes: Will your deployment use the New Recording Priority mode (default) or the Old Recording Retention mode (see Configuring the Recording Retention Modes (page 49)). This option is only configured in the primary server.

Caution: Once you select the primary server to complete the initial setup procedure, you *will not be able to change* your primary server assignment nor your Recording Retention Modes selection for this deployment--other than to restart all servers in the cluster.

If you later need to update all other information that you specify during the setup procedure, you can use the Unified MCP Administration interface to make changes. For more information, see the Using the Unified MCP Administration (page 37)

To complete the setup for the primary server in any Unified MCP deployment, follow this procedure.

Step 1 On completing the installation procedure (see Installing the Unified MCP Software (page 13)), the system restarts automatically. You must explicitly login to the Unified MCP Administration for the primary server.

Once you login, the Welcome screen of the Unified MCP First Server Setup Wizard displays.

Step 2 Read the message in this screen and when you are ready to proceed, click **Next.**

The Service Activation screen displays.

Step 3 The system internally verifies the IP address of this server and automatically begins enabling the Unified MCP feature services in this server. Wait until all the features services are enabled in the Service Activation window. Once all the services are successfully enabled, click **Next.**

If a feature services cannot be enabled, an error message is displayed in the Status section.

Table 3: Feature Service Status Description

Status	Description	Take the Following Action
Enabling	This service is in the process of being enabled.	Do nothing. Wait for the state to moved to the *Enabled* state.
Enabled	This service is now fully turned on and ready to function as designed.	Wait until all the feature services for this server reach the Enabled state. The primary server requires all feature services to be enabled (see Enabling or Disabling Feature Services (page 62)).
Error	The system cannot enable this service due to an error.	**Warning: If the Database Service (page 20) or the Configuration Service (page 20) is not enabled, the**

Status	Description	Take the Following Action
		system will not allow you to proceed with the setup procedure. You response depends on the service that failed to be enabled. • If it is Database Service or the Configuration Service, you mustfirst correct the error and re-login to restart the initial setup. • If it is any other service, you can continue with the setup and fix the errors after the setup is completed. Be aware that your system will not be in full service until you fix these issues.

Once you click Next, the AXL Service Provider screen displays.

Step 4 In the AXL Service Provider Configuration screen, enter theAXL Service Provider (IP address), AXL Administrator username, and Password in the respective fields for the Unified CM that should communicate with Unified MCP.

The Administrative XML Layer (AXL) authentication allows you to enter the Unified CM cluster and retrieve the list of Unified CM servers within that cluster. During the AXL authentication, if the Unified CM Publisher is ofÃine or not available, you can provide the next available Unified CM Subscriber for the AXL authentication.

The AXL Administrator username may not be same as the Unified CM Administrator username for that cluster. Be sure to add the username for theAXL Administrator to the Standard Unified CM Administrators group and "Standard AXL API Access" roles in Unified CM.

Note: You will not be able to change the password for the AXL user in the Unified MCP application. The Unified MCP application only authenticates the password configured in Unified CM. You can, however, modify the AXL server IP address (see Modifying AXL Information (page 44)).

If the selected AXL services cannot be enabled, an error message instructs you to reselectAXL service providers.

Once the system accepts theAXL server and user information, the Call Control Service Provider screen displays.

Step 5 (Optional step.) In the Call Control Service Provider Configuration screen, you will need to provide the Unified CM IP address for the Call Control service (referred to as SIP trunk in

Unified CM UI and documentation). Provide this information only if you know the applications using Unified MCP (for example, if the client applications need to make outbound recording calls).

Note: You can request this information by sending an AXL request to the Unified CM server which was configured as AXL Service Provider.

If you choose to skip this step, you can add the information later (see Configuring the Call Control Service Connection (page 45)).

Even if it is already enabled, the Call Control Service will not be *In service* (either directly through Unified CM or from Unified MCP using AXL) until the Unified CM information is configured.

If you enter the information in this screen, you will need to configure the Unified CM IP Address for Call Control Service (SIP trunk), Route Group, Route List, Recording Profile, and the Route Pattern to ensure that the Unified MCP Call Control Service will be *In service*.

When you click Next, the Recording Retention Modes screen displays.

Step 6 In the Operation Mode screen, select the required recording mode (see Configuring the Recording Retention Modes (page 49)): New Recording Priority mode (default) or Old Recording Retention mode click **Next.**

The recording mode is only configured in the primary server.

If you select the New Recording Priority mode, you can choose the retention period of the recordings. The retention period range for this mode is from 1 to 180 days. The default is 60 days. See Configuring the New Recording Priority Mode (page 49).

Note: See the Considerations for Data Replication (page 27) section for more details on run time replication behavior and data synchronization.

Caution: Once you complete this setup procedure for the primary server, you *will not be able to change* your Recording Retention Modes selection.

Step 7 Click **Finish** to complete the initial setup for the primary server.

The Unified MCP Setup Result Information window displays the result of the initial setup.

When you finish the post-installation process for any Unified MCP server, you are provided with an IP address link in the final page of the post-installation wizard. This link connects you to the Unified CM server in your deployment (based on the information provided during the installation and post-installation process). In the Unified CM Administration, you will need to configure the SIP Trunk, Route Group, Route List, and Recording Profile (see Configuring the Call Control Service Connection (page 41)). If you do not need to access this URL, you are automatically presented with the Unified MCP authentication window when the Unified MCP application restarts.

You have now completed the initial setup of the primary server for Unified MCP. You need to sign into the Unified MCP Administration web interface before you configure and manage the Unified MCP system.

Adding Subsequent Server Information in the Primary Server

Before you install Unified MCP on the second server, you must first add the new server details to the primary server using the Unified MCP Administration interface.

After you add the new server details in the cluster's primary server, you must install the server to complete the clustering process.

Add New Server Details

To add the new server details to an existing Unified MCP cluster, follow this procedure.

Step 1 From the Unified MCP Administration of the primary Unified MCP server, select **System** > **Unified MCP Server Configuration**.

The Unified MCP Server Configuration web page displays.

Step 2 In the Unified MCP Server Configuration web page, you can view or add servers in that Unified MCP cluster.

The Server Configuration window displays. It lists all configured servers in this cluster. The primary server cannot be changed or configured.

See the Understanding Unified MCP Clusters (page22) section for more information on clusters. You cannot assign the server type in this web page. You can only assign the server type during the post-installation procedure (see Completing the Installation for Subsequent Servers (page 33)). Between the time a new server is added to Unified MCP Server list and until the post-installation is configured successfully, the type for the new server will remain *unknown*.

Step 3 In the Unified MCP Server Configuration web page, click **Add Unified MCP Server**.

The Add Unified MCP Server web page displays.

Step 4 Enter the IP Address for the new server. All other fields in this page are optional.

Caution: To display the IP addresses, you must configure the Domain Name Server (DNS) suffix information (for the required nodes in the cluster) in the server in which Unified MCP is installed. If you plan to install the Unified MCP without the DNS information, then make sure you provide only the IP Address as reference instead of host names in all servers in this Unified MCP cluster.

Note: See the Command Line Interface Reference Guide for **Cisco Unified Communications Solutions guide at** (https://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html) for more information.

Step 5 Click **Save** to add and save the details of the new server.

The Unified MCP database is updated and saved.

Click **Reset**, for all settings to revert to the previously-configured list of servers without making any changes.

Click **Back to Unified MCP Servers List** to return to the Unified MCP Servers List page at any time.

Subsequent Server Post-Installation Process

To complete the installation for the subsequent servers, you should have already installed Unified MCP on each server and completed the following tasks:

1. You have already completed the installation for the primary server (see Completing the Installation for the Primary Server (page 28)).
2. The primary server must be up and functioning (at least the network services) before any subsequent server to be installed.
3. The subsequent server information should already be added to the primary server (see Adding Subsequent Servers (page 32)).
4. Configured the User ID and password for the Cisco Unified Communications platform administrator.
5. Entered the Network Configuration information for the machine (Unfied OS requirement).
6. Identified that this server is **not** the "first node" (Unified OS requirement).
7. Provide the primary server information of the Unified MCP cluster to which this server must join.
8. Once you have completed the installation process and the system restarts, you see the Unified MCP Administration's login prompt.

Completing the Installation for Subsequent Servers

The Unified MCP deployment model is transparent to the Unfied MCP installer as the clustering for Unified MCP is performed through the Unified MCP Administration interface using the Unified MCP Post-Installation Setup wizard.

The post-installation setup procedure that you perform depends on the following answers:

- Access to Unified CM is required to continue with the Unified MCP installation.

  Do you have the Unified CM IP address, AXL Admin username, and AXL Admin Password to continue with the post-installation tasks.

- Did you review the considerations listed for the required deployment?

Separate sections are available for the following deployments:

- Dual-server Deployment (page 24)

- Three-server Deployment (page 25)

Caution: Once you complete the initial setup procedure for the secondary server, you cannot change your secondary server assignment for this deployment.

If you later need to update information that you specify during the setup procedure, you can use Unified MCP Administration interface to make changes. For more information, see the Using the Unified MCP Administration (page 37)

To complete the setup for a subsequent server in any Unified MCP cluster, follow this procedure.

Step 1 On completing the installation procedure (see Installing the Unified MCP Software (page 13)), the system restarts automatically. You must explicitly login to the Unified MCP Administration for subsequent servers.

Once you login, the Welcome screen of the Unified MCP First Server Setup Wizard displays.

Step 2 Read the message in this screen and when you are ready to proceed, click **Next.**

The Service Activation screen displays.

Step 3 Read the message in this screen and when you are ready to proceed, click **Next.**

You determine the type of server in this Welcome screen. Based on your choice, the list of services to be turned on is pre-determined and then displayed in the service activation page.

During this step, you must determine if this subsequent server will become the secondary server or if it will become the expansion server.

- Secondary server: If you enable all the services in the Service Activation window, this server will automatically become the secondary server. Once you have enabled all the services and the initial setup in complete, you will not be able to change the secondary server assignment.

- Expansion servers(s): If the API Service and the Configuration Service has already been turned on in the secondary server, these services will no longer be available for activation. Only the Media Service (page 21), Call Control Service (page 21), and SM Agent (page 21) will be available for activation. A server with only these four services enabled automatically becomes an expansion server.

The following table identifies which feature services will be enabled in each server:

Feature	Enabled in Primary Server?	Enabled in Secondary Server?	Enabled in Each Expansion Server?
Database Service	Yes	Yes	No

Feature	Enabled in Primary Server?	Enabled in Secondary Server?	Enabled in Each Expansion Server?
Configuration Service	Yes	Yes	No
API Service	Yes	Yes	No
Media Service	Yes	Yes	Yes
Call Control Service	Yes	Yes	Yes
SM Agent	Yes	Yes	Yes

When you click **Next**, the Service Activation screen displays.

Step 4 After the services are enabled, click **Finish** to complete the initial setup for the subsequent server.

If a feature service cannot be enabled, an error message is displayed in the Status section.

The Unified MCP Setup Result Information window displays the result of the initial setup.The Unified MCP application restarts.

You have now completed the initial setup of the subsequent server for Unified MCP and this server is also ready to record.

Unified MCP System Verification

Once you have installed Unified MCP, use the following indicators to verify the health of your Unified MCP deployment:

- Access and sign in to the Unified MCP Administration in each server. See Accessing the Unified MCP Administration (page 38).
- Access and sign in to the Unified MCP Serviceability Administration in each server. See Accessing Unified MCP Serviceability Administration (page 55)
- All applicable feature services are enabled in each server as provided in the Setup Summary page of your Unified MCP Post-Installation Setup wizard(see the *Feature Service Status Description* table in the Completing the Installation for the Primary Server (page 28)section for status descriptions).

Chapter 3

Using the Unified MCP Administration

The Unified MCP Administration interface allows you to configure the Unified MCP system. You can then use a web browser located on any computer on the Unified Communications network to configure and administer your applications with the Unified MCP Administration web interface.

This chapter contains the following topics:

Using Single-Sign In

The Navigation drop-down list box in the top right corner of each Administration page provides a list of applications which you can access with a single-sign in. Once you sign in to the Unified MCP Administration, you can access the following applications:

- Unified MCP Administration
- Unified MCP Serviceability Administration
- Cisco Unified Serviceability

Caution: Cisco Unified OS Administration and Disaster Recovery System requires a separate (Unified CM) authentication procedure.

To access these applications from the Unified MCP Administration, you must first select the required application from the Navigation drop-down and click **Go.**

Accessing the Unified MCP Administration

When you finish the post-installation process for any Unified MCP server, you are provided with an IP address link in the final page of the post-installation wizard. This link connects you to the Unified CM server in your deployment (based on the information provided during the installation and post-installation process). In the Unified CM Administration, you will need to configure the SIP Trunk, Route Group, Route List, and Recording Profile (see Configuring the Call Control Service Connection (page 45)). If you do not need to access this URL, you are automatically presented with the Unified MCP authentication window. You need to sign into the Unified MCP Administration web interface before you configure and manage the Unified MCP system.

Note: You can access the Unified MCP Administration at any time by entering the following URL in a web browser, where *servername* is the IP address of the server on which you installed Unified MCP: **http:**//*servername*/**oraadmin**

Use the following procedure to sign in and access the Unified MCP Administration.

Step 1 From a web browser on any computer in your Unified Communications network access the Unified MCP Administration Authentication page:

Note: Ensure that Cisco Tomcat services are up and running before you login to the Unified MCP Administration using the above-mentioned URL. Verify that your popup blocker is disabled.

Step 2 A Security Alert message may appear, prompting you to accept the self-signed security certificate, if you have not already accepted it. This security certificate is required for a secure connection to the server. Click the required button.

This security message may not appear if you have already installed a security certificate. The security certificate is required for a secure connection to the server.

The Authentication page is displayed.

Step 3 In the Unified MCP administration interface's authentication window, enter the Application Administrator User ID and password for the primary server. This information was configured during the installation procedure and you may have noted the details in the worksheet (see Completing the Installation and Configuration Worksheet (page 9)). Click **Log in**.

Note: The application administrator's user ID and password must be the same in all servers in a Unified MCP deployment. The Unified MCP application administrator's user password is case-sensitive. Be sure to enter the password (exactly as created during the installation process) in the Unified MCP Administration Authentication page.

Caution: For security purposes, the Unified MCP Administration logs you out after 30 minutes of inactivity, and you must sign in again. When you sign in again, you are placed back in the last-accessed screen.

The welcome page appears after you have successfully logged in. The welcome page displays the version number of the product as well as trademark, copyright, and encryption information.

Unified MCP Administration Navigation and Menus

The minimum supported screen resolution specifies 1024x768. Devices with lower screen resolutions may not display the applications correctly.

This section includes the following subsections:

Navigation

After you log on, the main Unified MCP Administration web page displays. The web page includes the drop-down list box in the upper, right corner called Navigation. To access the applications in the drop-down list box, choose the required application and click **Go**.

The choices in the drop-down list box include the following Unified MCP-related applications:

- **Unified MCP Administration**: Use the Unified MCP Administration to configure Unified CM, Unified MCP users, prune policy, and other procedures described in this section .
- **Unified MCP Serviceability Administration**: Takes you to the main Unified MCP Serviceability web page that is used to configure trace files, and to enable and disable Unified MCP services. See Using the Unified MCP Serviceability Administration (page 55)
- You must be an end user on the configured Unified CM with Administrator capability in Unified MCP to log in to any of the Unified MCP-related applications.
  - **Disaster Recovery System**: Takes you to the Disaster Recovery System, a program that provides data backup and restore capabilities for all servers in a Unified MCP cluster. Access the Unified DRS Administration for more information. Unified MCP-specific DRS information is provided in the Using the Disaster Recovery System Administration (page 67) section.
  - **Cisco Unified OS Administration**: Takes you to main Cisco Unified OS Administration web page, so you can configure and administer the Cisco Unified Communications platform for Unified MCP. Access the Unified OS Administration directly for more information.
  - **Cisco Unified Serviceability**: Takes you to the main Cisco Unified Serviceability web page that is used to configure trace files and alarms and to enable and disable Cisco Unified Communications services.

The Unified MCP Administration menu bar appears at the top of every web page in the Unified MCP Administration web interface. You begin every Unified MCP configuration and administration task by choosing a menu and submenu option from the menu bar.

Unified MCP Administration Main Menu

The Unified MCP Administration menu bar contains the following menu options:

- **Administration**—Contains options for configuring new servers in the cluster, Unified CM information, and changing system parameters. For a description of all Administration menu options, see Accessing the Unified MCP Administration (page 38).
- **System**—Allows you to add a new server or view the disk usage information for each server in the Unified MCP deployment.
- **Help**—Provides access to online help for Unified MCP.

  Once you are in the required administration interface, select one of the following options:

  – To display documentation for a single window, click **Help** > **This Page**.

  – To verify the version of the administration running on the server, click **Help** > **About** or click the **About** link in the upper-right corner of the window.

Tool Tips for Fields and Parameters

All Unified MCP Administration pages provide descriptive tool tips for each parameter and field. When you place your mouse over the required parameter and field, the tool tip information is briefly displayed for each parameter and field. As the required information for each parameter and field are already provided within these tool tips, this document does not repeat that information.

Configuring Unified MCP with Unified CM

If you use the Unified CM cluster (assumption here is that Unified CM administrator and Unified MCP administrator can be the same person—though they can be two separate people).

This section contains the following subsections:

Provisioning Unified CM for Unified MCP

When you finish the post-installation process for any Unified MCP server, you are provided with two URLs in the final page of the wizard: The first link connects you to the Unified CM server in your deployment to enable Unified MCP to communicate with Unified CM.

Perform the following tasks after you finish your cluster set up and before you start using the Unified MCP servers:

- Configuring the Call Control Service Connection (page 41)
- Configuring the Profile for a Recording Device (page 43)
- Disabling Codec G.722 for the Recording Device (page 43)

Configuring the Call Control Service Connection

The Call Control Service in Unified MCP is referred to as a SIP Trunk in Unified CM UI and documentation. In the Unified CM Administration, you must configure the SIP Trunk, Route Group, Route List, and Recording Profile to enable the Call Control Service in the Unified MCP Administration to communicate with the Unified CM Administration.

Note: Be sure to configure Unified CM to use TCP transport for a SIP Trunk connection to Unified MCP.

Once you have configured the SIP Trunk information in Unified CM, you will need to provide this IP address in the Call Control Service Provider Configuration screen in the Unified MCP Administration.

Even if already enabled, the Call Control Service will not be *In service* until you have configured the Call Control Service Provider.

To configure the SIP Trunk information in Unified CM, follow this procedure.

Step 1 Invoke and connect to the Unified CM Administration web interface, using a valid Unified CM username and password.

Step 2 Select **Device** > **Device Settings** > **SIP Profile** in the Unified CM Administration.

Follow the procedure specified in your Unified CM Administration documentation to enable OPTIONS Ping and save this configuration.

a. Add a new SIP profile.

b. Select the **Enable OPTIONS Ping** checkbox to monitor the destination status for SIP Trunks using the *None* (default) Service Type.

Step 3 Select **Device** > **Trunk** in the Unified CM Administration.

Follow the procedure specified in your Unified CM Administration documentation to add a new SIP Trunk. Configure the Device name, select the Device Pool, assign SIP information, enter the destination (in this case, Unified MCP) IP address and port (5060), select the SIP trunk security profiles and SIP profile and save this configuration.

Step 4 Set the distribution algorithm for the required SIP trunks created in Step 1 to be *circular* by selecting **Call Routing** > **Route/Hunt** > **Route Group** in the Unified CM Administration.

Follow the procedure specified in your Unified CM Administration documentation to select the circular distribution algorithm.

Step 5 Associate Route Group with a Route List by selecting **Call Routing** > **Route/Hunt** > **Route List** in the Unified CM Administration.

Follow the procedure specified in your Unified CM Administration documentation to associate the Route List.

Step 6 Associate this new SIP trunk with a Route Pattern by selecting **Call Routing** > **Route/Hunt** > **Route Pattern** in the Unified CM Administration.

Follow the procedure specified in your Unified CM Administration documentation to add a new route pattern

Step 7 In the **Gateway** > **Route List** web page in the Unfied CM Administration, select the SIP trunk you configured in the steps above and click **Save.**

Step 8 Select **Device** > **Phone** in the Unified CM Administration.

Follow the procedure specified in your Unified CM Administration documentation to perform the following tasks:

a. Find the audio forking phone.

b. Find the Built In Bridge configuration for this device and change the setting to **ON.**

c. Enable Recording for a LineAppearance by selecting **Automatic Call Recording Enabled** in the Recording Option drop-down list.

d. Select the Recording Profile created earlier in this procedure.

Step 9 To prevent Unified CM from sending Session Description Protocol (SDP) invitations, be sure to uncheck the Media Termination Point Required field (or verify if it is already unchecked).

Step 10 Select **System** > **Service Parameters** > **<server>** > **Cisco Call Manager** in the Unified CM Administration. In the Cluster-wide Parameters (System - Location and Region) section, locate the **G.722 Codec Enabled** and **iLBC Codec enabled** parameters and set their value to **Enable for devices except recording enabled devices**.

You have now configured the SIP Trunk information in Unified CM.

Configuring the Profile for a Recording Device

After configuring the SIP Trunk information, you must point the recording device profile to an audio forking device.

To configure the profile for a Recording Device in Unified CM, follow this procedure.

Step 1 Select **Device** > **Device Settings** > **Recording Profile** in the Unified CM Administration.

Follow the procedure specified in your Unified CM Administration documentation to add a new Recording Profile. Configure the Recording Profile name, and the Recording Destination Address (enter the Route Pattern number you configured earlier--see Step 3 in Configuring the Call Control Service Connection (page 41)), and click Save

Step 2 Select **Device** > **Phone** in the Unified CM Administration.

The Find and List Phones window displays. Enter the search criteria to locate the built-in-bridge (BIB) for the phone which support audio forking. Click the device name of the phone and change the setting to **ON.**. In the left navigation section click the link for the phone line of this audio forking phone. In the Recording Option field, enable **Automatic Call Recording**. In the Recording Profile field, select the profile name you configured in Step 1 of this procedure and save your configuration.

Disabling Codec G.722 for the Recording Device

Unified MCP records sessions (page 97) using the following Codecs:

- Audio recordings: g.711 (aLaw or µ-Law) or g.729 (a/b) Codecs
- - Video recordings: h.264 Codecs

Unified MCP does not support Codec G.722. Consequently, this feature must be disabled in Unified CM before you proceed with the Unified MCP configuration.

To disable Codec G.722 in Unified CM, follow this procedure.

Step 1 Select **System** > **Service parameters** > **Select Server** in the Unified CM Administration.

Step 2 Go to the Cluster-wide Parameters (Location and Region) section and locate the **G.722 Codec Enabled** parameter.

Step 3 Set the value for this parameter as *Enable for device except recording enabled device* and save your configuration.

Configuring Unified CM User Information in Unified MCP

When you access the Unified MCP Administration for the first time in a cluster, the system automatically initiates the cluster setup procedure (see Post-Installation Requirements (page 18)) once for each cluster to perform the following tasks:

- Selecting AXL Service Providers (page 44)
- Selecting Call Service Providers (page 45)
- Replacing Unified CM Service Providers (page 45)

Selecting AXL Service Providers

During the Unified MCP post-installation setup process, you may have provided the AXL information for the primary server. Based on the primary server information, the Unified MCP Administration retrieves the list of other Unified CM servers in the cluster and displays them in the list of *available* Unified CM servers. You can select the required server(s) and change the Administrative XML Layer (AXL) user information. If you did not provide this information during the post-installation process or if you need to modify the AXL information, you can do so by following the procedure provided in this section.

Caution: The AXL service must be enabled for the required Unified CM server(s) before the Unified MCP Administration can access that server so you can update the AXL user information.

To modify the AXL information for Unified MCP, complete the following procedure.

Step 1 From the Unified MCP Administration select **Administration** > **Unified CM Configuration**.

The Unified CM Configuration web page opens.

Step 2 In the Unified CM Configuration web page, go to the AXL Service Provider Configuration section to modify the AXL information.

Caution: The Unified CM username and password information are mandatory fields. The password cannot be updated in this page. You will need to change the password in the Unified CM administration.

Step 3 Select and move each server from the Available Unified CM Servers list to the Selected Unified CM Servers list box using the right arrow. Alternately, use the left arrow to move back a selected server.

Step 4 Click the **Save** icon at the top of the Cisco Unified CM Configuration web page to save your changes.

The Unified MCP server validates the connection details and refreshes the Unified CM Configuration web page to display the new settings.

Selecting Call Control Service Providers

During the Unified MCP installation process, you provided the information for the first Unified CM server. Based on the primary server information, Unified MCP retrieves the list of other Unified CM servers in the cluster and displays them in the list of *available* Unified CM servers. You can select the required server so the Unified MCP Call Control Service can determine the Unified CM server to which the outbound call must be sent. Outbound call refers to the call sent to one of the selected Unified CM servers by the Unified MCP Call Control Service. If you select multiple Unified CM servers, you can ensure that the outbound call is placed even if one of the servers is not functional.

To modify the Call Control Service information for Unified MCP, complete the following procedure.

Step 1 From the Unified MCP Administration, select **Administration** > **Unified CM Configuration**.

The Cisco Unified CM Configuration web page opens.

Step 2 In the Unified CM Configuration web page, go to the AXL Service Provider Configuration section to modify the AXL information using the following fields.

Note: If you deselect the Unified CM server from the Selected list box, a browser window pops up informing you about the (list of) deselected server(s).

Caution: If you modify the Unified CM cluster and do not select the required Call Control Service Providers for the new Unified CM server, then the Unified MCP Call Control Service will be out of service (OOS) and the outbound call recording will be disabled.

Step 3 Click the **Save** icon at the top of the Cisco Unified CM Configuration web page to save your changes.

The Unified CM Configuration web page refreshes to display the new settings.

Replacing Unified CM Service Providers

In the Unified CM Configuration web page, you have the ability to select Unified CM servers from the available list. However, you do not have the ability to modify the IP address for a selected service provider.

To modify the IP addresses which show up in the Available list, you must first add a new AXL service provider.

Caution: If you modify the Unified CM cluster configuration, you must also reconfigure the Unified MCP API users. If you do not reconfigure the corresponding users, you will not be able to sign in to use your Unified MCP APIs.

To replace the Unified CM service provider, complete the following procedure.

Step 1 From the Unified MCP Administration select **Administration** > **Unified CM Configuration**.

The Unified CM Configuration web page opens.

Step 2 In the Unified CM Configuration web page, click **Modify** Unified CM Cluster to replace the existing list of service providers..

The Modifying Unified CM Cluster web page opens.

Step 3 Enter the IP address, username, and password for the new service provider in the required Unified CM cluster.

If you change your mind about this new server, click **Reset** to go back to the Unified CM Configuration web page without making any changes.

Step 4 Click the **Save** icon at the top of the Add New AXL Service Provider web page to save your changes.

Note: The initial list of selected AXL service providers in the Unified CM Configuration web page will be replaced with the selected Unified CM service provider.

The Unified MCP server validates the connection details, closes the Modifying Unified CM Cluster web page, and refreshes the Unified CM Configuration web page to display the new service provider in the Selected service provider list. The selected service provider is also updated in the Unified MCP database.

Even if you provide only one Unified CM IP address in this page, the other service provider IP addresses in this Unified CM cluster will automatically appear in the list of Available service providers (both AXL and Call Control service providers).

Step 5 The list of Available Call Control Service Providers is also updated automatically for the newly-selected service provider. Select and move the required Unified CM servers from the Available Call Control Service Provider list to the Selected Call Control Service Provider list using the right arrow.

Caution: If you do not select the required Call Control Service Providers for the new Unified CM server, then the Unified MCPCall Control Service will be out of service (OOS) and the outbound call recording will be disabled.

Note: If you modify the Unified CM service provider configuration, you must also reconfigure the Unified MCP API users. If you do not reconfigure the corresponding users, you will not be able to sign in to use your Unified MCP APIs.

Step 6 Click the **Save** icon at the top of the Cisco Unified CM Configuration web page to save your changes.

The Unified MCP server validates the Selected Call Control Service Provider(s) and save this information to the database.

Provisioning Users for Unified MCP Deployments

You can provision Unified CM end users as API users in Unified MCP deployments. This API access can only be provided by the Unified MCP application administrator to the required Unified CM end users.

About Unified MCP API Users

Unified MCP's open Application Programming Interface (API) list is available for third-party consumption to securely perform the following functions:

- Pause and resume a recording while in progress
- Control a recorded session (page 97)
- Search and manage existing recordings
- Monitor a live session (page 97)

Unified MCP APIs provide an alternate to the functionality that is available via the Unified MCP web interfaces. Using these APIs, API users can create customized client applications. Unified MCP system integrators and developers who want to use Unified MCP to integrate with other Unified Communication software or any third-party software applications, need to have access to the Unified MCP API. This API access can only be provided by the Unified MCP Administrator to the required Unified CM Users (service providers) (page 44).

Managing Unified MCP API Users

Unified MCP API users can use variousUnified MCP APIs to perform various functions with the captured recordings.

For more information see the following sections:

- API functionality overview: see Playing Back Recordings (page 5).
- About API users: see About Unified MCP API Users (page 47).
- API usage: see the *Cisco Unified MCP Developer Guide*.

For more details on API usage, you must first provision Unified CM end users as API users in the Unified MCP Administration.

To modify or add to the list of Unified MCP API users, follow this procedure.

Caution: If you modify the Unified CM cluster configuration, you must reconfigure the Unified MCP API users. If you do not reconfigure the corresponding users, you will not be able to sign in to use your Unified MCP APIs.

Step 1 Select **Administration** > **Unified MCP User Configuration** from the Unified MCP Administration.

The Unified MCP User Configuration web page opens to display the Unified MCP User List of the first 75 configured Unified MCP users. You can sort the list by any of the columns, in both ascending and descending order.

Step 2 To modify the list of Unified MCP API users, click **Manage Unified MCP Users**.

The Unified MCP User Configuration web page opens to display the available Unified CM users in the Available Unified CM Users list and the configured API users in the Unified MCP API Users list .

Step 3 To search for a particular user from the Unified CM list, enter the User ID, the first name, or the last name (or, even a partial name) of the user in the Search for Available Unified CM Users field and click the **Search** button.

Your sorted results will display the first 75 users based on your sorting criteria (user ID, descending order, or ascending order). A list of Unified CM users matching your search criteria is displayed in the Available users list box. If this list results in more than 75 users, only the first 75 based on your sorting criteria are listed. You may need to refine your search to get meaningful results.

Step 4 Use the left and right arrows to make the required modifications to the Unified MCP user list and click **Save**.

The Unified MCP User Configuration web page refreshes to display your saved changes.

Click **Reset**, for all settings to revert to the previously-configured list of users.

Click **Back to User List** to return to the Unified MCP User List page.

Managing Storage in Unified MCP Deployments

Unified MCP deployments have a central storage management service (SMAgent) to provision media, monitor storage, and alert administrators on various media- and storage-related thresholds.

This section contains the following subsections:

Understanding Recording Modes

Unified MCP deployments provide multiple pruning options to address varied deployment scenarios. These pruning options (or modes) are collectively referred to as the Recording Retention Modes.

Unified MCP provides two modes to configure the media recording.

- New Recording Priority mode: (Default) This mode is based on disk usage capacity and removes older recording data irrespective of contents. The priority in this mode is provided to newly-recorded media and disk space is overwritten to accommodate new recordings. The retention period range for this mode is from 1 to 180 days. The default is 60 days. See Configuring the New Recording Priority Mode (page 49).

  Note:

  - See the Considerations for Data Replication (page 27) section for more details on run time replication behavior and data synchronization.

  - If you prefer to use this mode and, at the same time, wish to protect a particular session (page 97) from being automatically pruned, be sure to store that session in MP4 format, download the MP4 file, and save it to a suitable location in your network. You can also use the **`downloadUrl`** parameter in the Session Query APIs and download the raw recording to a location of your choice.

- Old Recording Retention mode: This mode focuses on media preservation. If you select this mode, the Unified MCP application does not automatically prune data. You must use your client application (see the *Unified MCP Developer Guide* for further details) to remove unwanted data and free up disk space.

Caution: If you do not clean up unwanted data periodically, the Call Control Service will reject new calls and drop existing recordings at the emergency threshold level (ENTER_EMERGENCY_STORAGE_SPACE). See the Avoiding Data Pruning (page 50) section for further details.

You have the option to select the required mode during the post-installation setup phase. This option is only configured in the primary server (see Completing the Installation for the Primary Server (page 28)) to perform this task. Once you select the required mode, you cannot change it at any time.

Configuring the New Recording Priority Mode

This section only applies if you set up Unified MCP in the New Recording Priority mode during the initial setup. This *Delete recordings older than 60 days* field is not available if you set up Unified MCP in the Old Recording Retention mode (during initial setup--see Completing the Installation for the Primary Server (page 28)). Automatic pruning is not implemented if you have set up the Unified MCP primary server in the Old Recordings Retention mode.

If you have set up the primary Unified MCP server to use the New Recording Priority mode, then a recording can be deleted if any of the following situations occur:

- The age of the recording is equal to or greater than the retention age configured in the *Delete recordings older than 60 days.* field.

  Note: A day is identified as twenty fours from the precise time you change this setting--it is not identified as a calender day. For example, if you change the retention period at 23.15.01 on April 2nd, 2010, the specified recordings will only be deleted at 23.15.01 on April 3rd, 2010. The recordings will not be deleted at 00:00:01 on April 3rd, 2010.

- The disk usage has crossed the 95% mark

For example, if you are within your disk usage percentage and if you automatically wish to delete all recordings older than 90 days, you must enter 90 in the *Delete recordings older than __ days.* field. In this case, all recordings which are older than 90 days are automatically deleted.

Deleted recordings are not immediately removed from the meta database. Instead, they are marked as deleted and removed from the database at off-peak hours. Disk I/O is expensive. A batch delete of multiple database records at off-peak hours reduces the impact on the system during critical hours. The routine is currently scheduled to run at 12 AM (local server time) daily, at which time the deleted recordings are physically removed from the disk. If a session is automatically pruned, it is marked as deleted, but it will not be removed by this scheduled routine. You must use the **`deleteSessions`** API explicitly to remove automatically-pruned recordings from the disk.

Caution:

To configure the number of days to delete old recordings in the New Recording Priority mode, follow this procedure:

Step 1 Select **Administration** > **Prune Policy Configuration** from the Unified MCP Administration.

The Unified MCP Prune Policy Configuration web page opens to display the configured number of days to delete old Unified MCP recordings. The allowed range is from 1 to 180 days (default is 60 days).

Step 2 Change the number of days for recording to be deleted and click **Save** to apply your changes.

The page refreshes to display the newly-configured number of days.

If you prefer to revert to the default of 60 days, click **Reset**.

Avoiding Data Pruning

An API event is issued each time the storage disk space (which stores the recorded media) reaches various thresholds. You can select the Old Recording Retention mode and judiciously follow all threshold alerts by deleting unwanted recordings. By doing so, you can conserve space for the recordings which are required.

The other option to avoid data loss is to select the New Recording Priority mode and to save the required recordings as MP4 files to a safe location in your network.

For either option, see Configuring the Recording Retention Modes (page 49).

The threshold value percentage and each corresponding implications are provided in the following table:

Table 4: Storage Threshold Values

Threshold Storage	Percentage	Description
ENTER_LOW_STORAGE_SPACE	Recorded media crossed the 75% storage utilization mark.	First warning to indicate that the disk storage is running into low space condition.
EXIT_LOW_STORAGE_SPACE	Recorded media usage dropped below 70% utilization mark.	The disk storage is exiting the low storage space condition.
ENTER_CRITICAL_STORAGE_SPACE	Recorded media crossed the 90% local storage utilization mark.	Second warning. When entering this condition, action must be taken to guarantee future recording resources on this node. If operating in the Old Recording Retention mode, new recording sessions are not accepted when you reach this threshold.
EXIT_CRITICAL_STORAGE_SPACE	Recorded media usage dropped below the 85% utilization mark.	The disk storage is exiting the critical storage space condition. At this point the local node is still considered to be low on resources.
ENTER_EMERGENCY_STORAGE_SPACE	Recorded media crossed the 99% storage utilization mark	Last warning. When entering this condition, action must be taken to guarantee future recording resources on this node. If operating in the New Recording Priority mode, the following conditions apply when you reach this threshold: • In-progress recording sessions are terminated. • Existing (older) recording sessions are deleted. • New incoming recording sessions are rejected.
EXIT_EMERGENCY_STORAGE_SPACE	Recorded media usage dropped below the 97% utilization mark.	The disk storage is exiting the emergency storage space condition. At this point, the local node is still considered to be low on resources and

Threshold Storage	Percentage	Description
		new recording sessions are still not accepted.

See the *Unified MCP Developer Guide* for more details on the correspondingAPIs, Events, and error code descriptions.

The following APIs and events correspond to this task:

- Event Subscription APIs
  - subscribeRecordingEvent
  - unsubscribeRecordingEvent
  - verifyRecordingSubscription
- The storageThresholdEvent Recording Event.

Monitoring System Thresholds

The storage thresholds are monitored by the SM Agent (page 21) on a per server basis. The thresholds are dedicated to the space used in each server and do not attempt to distinguish between the media types being stored.

Storage capacity checks are performed every two minutes and the corresponding alerts are issued at the end of each check cycle. This two-minute duration is not configurable as it is required to maintain the health of the system and recordings.

The monitoring scheme tracks the previous threshold alerts and determines the next threshold alert to be issued at the end of two minutes.

When you start the system for thefirst time, this threshold alert's current usage value is 0 (zero).

Viewing Disk Space Usage

To view and monitor the disk space usage in each server in the Unified MCP cluster, follow the procedure identified in this section.

Caution: If the server is not started, or is in an unknown state or is not responding, then the disk usage information is not displayed. You may need to verify the state of your server to verify if it is reachable (using the `ping` command).

The maximum storage figure depends on your storage configuration. See Avoiding Data Pruning (page 50) for more information on threshold value percentages. The information displayed in this page is from the Storage Management APIs. The size and percentage of the disk usage is provided in the API response.

Step 1 From the Unified MCP Administration, select **System** > **Disk Usage**.

The Server Disk Space Usage web page displays

Step 2 In the Server Disk Space Usage web page, select the required server from the Select Server drop-down list and click **Go**.

The Server Disk Space Usage web page refreshes to display the disk space usage for the selected server in gigabytes (GB) or terabytes (TB) depending on the size of the disk drive. This is a read-only page.

If the selected server does not display any information in this web page, you may receive an alert informing you that the disk usage information is not available for this server. If you receive this message, verify the state of the server to ensure that the server is set up and functioning.

Obtaining Storage Usage Information Using HTTP

You can also obtain the current storage usage information using HTTP code. The URL for accessing this information is as follows:

`http://<server-ip-address>/storagemanageragent/usage.xml`

The storage usage information is provided in an XML format.

- Example 1 - Does not use any media disks:

```
<?xml version="1.0" encoding="UTF-8" ?>
- <storageUsageInfo date="Oct 26 2010" time="13:24:22" gmt="1288124662599">
- <partitions>
  <partition name="/common" size="655G" usage="29%" />
  </partitions>
  </storageUsageInfo>
```

- Example 2 - Uses two media partitions:

```
<?xml version="1.0" encoding="UTF-8" ?>
<storageUsageInfo date="Oct 26 2010" time="13:10:53" gmt="1288123853753">
 <partitions>
  <partition name="/media1" size="99G" usage="5%" />
  <partition name="/media2" size="99G" usage="50%" />
  </partitions>
  </storageUsageInfo>
```

Note: The /common partition name is displayed if your deployment does not use any media disks. The number of media partitions directly correspond to the number of configure media disks. If you configure two media disks, you see two media partitions: /media1 and /media2.

Event Management

The Unified MCP API service issues notifications about events taking place in a Unified MCP cluster. For example, events may be created when the storage disk space reaches various

thresholds, when a new recording session is started, an existing recording session is updated/ended, or when a tag is added /deleted from a session.

Enabling Event Forwarding

The Event Subscription APIs allow applications to subscribe, verify subscription, and unsubscribe for all event notifications. For more information, see the *Cisco MediaSense Developer Guide*. If a Unified MCP deployment has two servers (primary and secondary), the third-party client applications must subscribe to each server separately to receive events generated on each server.

However, the Unified MCP Administration provides a cluster-wide property to enable/disable event forwarding between the primary and secondary servers in any Unified MCP cluster. By default, forwarding is disabled in Unified MCP deployments and you need to explicitly enable this feature to receive notification of all events. If you enable this feature, you receive events generated on both servers--you do not need to subscribe explicitly to each of the two servers.

Note: If you enable event forwarding, then you must subscribe to either the primary or the secondary server to start receiving event notifications for both servers.

To enable event forwarding between the primary and secondary servers in the Unified MCP cluster, follow the procedure identified in this section.

Step 1 From the Unified MCP Administration, select **System** > **Event Management**.

The Event Management web page displays.

Step 2 In the Event Management web page, select the Enabled Event Forwarding checkbox to enable event forwarding between both the primary and secondary server in this cluster, and click **Save**.

Once you save this information to the database, you will start receiving notifications for all events on both servers (regardless of the server in which you enable this feature).

Chapter 4

Using the Unified MCP Serviceability Administration

The Unified MCP Serviceability Administration interface allows you to configure, control, and monitor Unified MCP services and trace settings. This section provides description and procedures for these functions.

Depending on the service and component involved, you may perform serviceability-related tasks in both Unified MCP Serviceability and Cisco Unified Serviceability. For example, you may need to start and stop services, and configure traces in both applications to troubleshoot a problem. Unified MCP Serviceability supports the functionality described in this chapter.

This chapter contains the following topics:

Accessing Unified MCP Serviceability Administration

Once you complete the post-installation setup of the Unified MCP Administration interface, you can log in to the Unified MCP Serviceability Administration.

Caution: You must first complete the post-installation setup for this server. See Post-Installation Requirements (page 18). After you successfully complete the post-installation setup, you can sign in and access the Unified MCP Serviceability Administration.

To access Unified MCP Serviceability, follow this procedure.

Step 1 Access the Unified MCP Serviceability Administration

You can access the Unified MCP Serviceability Administration in one of two ways:

- Enter the following URL in a Unified MCP-supported web browser session., where *servername* is the IP address of the server on which you installed Unified MCP:
  http://*servername***/oraservice**

- From the Navigation (page 39) drop-down field in the upper-right corner of the Administration window, select **Unified MCP Serviceability** and click **Go**.

Step 2 A Security Alert message may appear, prompting you to accept the self-signed security certificate, if you have not already accepted it. This security certificate is required for a secure connection to the server. Click the required button.

This security message may not appear if you have already installed a security certificate. The security certificate is required for a secure connection to the server.

The Authentication page is displayed.

Step 3 Enter the single-sign in username and password, and click **Log in**.

Note: If you have already logged into the Unified MCP application, you can access Unified MCP Serviceability Administration without signing in again (see Using Single-Sign In (page 37)).

The welcome page appears after you have successfully logged in. The welcome page displays the version number of the product as well as trademark, copyright, and encryption information.

Note: For security purposes, the Unified MCP Administration logs you out after 30 minutes of inactivity, and you must sign in again. When you sign in again, you are placed back in the last-accessed screen.

Unified MCP Serviceability Administration Main Menu

All Unified MCP Serviceability Administration pages provide descriptive tool tips for each parameter and field. When you place your mouse over the required parameter and field, the tool tip information is brieÃy displayed for each parameter and field. As the required information for each parameter and field are already provided within these tool tips, this document does not repeat that information.

The Unified MCP Serviceability Administration menu bar contains the following menu options:

- **Trace**—Configure log and trace settings for Unified MCP components. Once enabled, you can collect and view trace information using the Real-Time Monitoring Tool (RTMT).

- **Tools**—Contains options that allow you to access system tools such as RTMT Plug-ins, manage network services, and control feature services.

- **Help**—Provides access to online help for Unified MCP.

  Once you are in the required administration interface, select one of the following options:

– To display documentation for a single window, click **Help** > **This Page**.

– To verify the version of the administration running on the server, click **Help** > **About** or click the **About** link in the upper-right corner of the window.

Trace Configuration

This section provides information on using traces in Unified MCP Serviceability

The following topics are included in this section:

About Trace Files

A trace file is a log file that records activity from the Unified MCP components. Trace files allow you obtain specific, detailed information about the system so you can troubleshoot problems. The Unified MCP system can generate trace information for different services. The generated information is stored in a trace file. To help you control the size of a trace file, you can specify the services for which you want to collect information and the level of information that you want to collect.

Trace information is primarily used by developers to debug problems. Each Unified MCP service can consist of several components. Each component can consist of multiple trace flags. You can enable or disable tracing for each component or for the required flags. Unlike logs, trace files are only written at one level. This section describes the trace configuration requirement for the Unified MCP Serviceability Administration.

Caution: If the Unified MCP Administration is unable to contact the Unified MCP Configuration Service, it uses default trace settings. If the Unified MCP Configuration Service is disabled or stopped, the trace configuration information is not displayed in the corresponding UI page(s). Similarly, if trace configuration is not available for any service, the UI page(s) will not display any information for that service.

The following bullets identify the difference between tracing and logging:

- Tracing: trace flags are free from detailed, developer-oriented information that are not printed to the logs by default, but only when increased logging is enabled to debug problems.
- Logging: log messages are predefined, higher-level messages that are always printed to the logs and indicate everything for normal system behavior to severe error conditions

About Unified MCP Log Levels

Trace flag information is stored in the Config database (page 94).

Log Levels identify the Unified MCP message level (Info and Debug) to be generated for each service. The currently-enabled Log Levels for each service component are identified by a green radio button (Log Level column) in the Trace Configuration web page. The currently-enabled Trace Flags are identified by a green check mark (Enabled column) in the Trace Configuration web page. As this information is visible in the Trace Configuration web page, it is not repeated in this document.

Note: There is no log level or trace mask for the Perfmon Agent network service. Hence it will not appear on this screen.

Caution: As the Media Service (page 95) does not support dynamic trace-level change, you cannot create or view a trace file for this service. Trace flags for the Media Service are only used by TAC and are not available to end users.

The Unified MCP log information is provided in the following output files:

- ORASERVICE-oraservice.<yyyy-MM-dd>T<HH-mm-ss.SSS>.startup.log: Contains Debug and Info messages (see the Unified MCP Log Levels table above for more information on Debug and Info message levels).
- Error-oraservice.<yyyy-MM-dd>T<HH-mm-ss.SSS>.startup.log: Contains only system conditions (see the Displaying a Counter Description (page 75) section for more information on system conditions).

Each of these files have a default maximum file size of 50 Megabytes (MB). The log file size and the number of files are not configurable.

Available Unified MCP Trace Flags

Each service component has different logical divisions with corresponding trace flags. Tracing for all services components and trace flags are disabled by default. You can enable the entire component or certain trace flags within each component. You can also set different Log Level values (Info or Debug) for different Unified MCP services in the same cluster. See the About Unified MCP Log Levels (page 57) section for more details on the Log Level values.

The Unified MCP Serviceability Administration lists each trace flag within its Unified MCP service component.

Caution: You cannot create a trace file for the Media Service (page 95) as this service does not support dynamic trace-level changes.

Trace File Location

The trace file contains information about each service. To configure the trace file, follow the procedure mentioned in Configuring Trace File Information (page 59).

After configuring the information that you want to include in the trace files for each service, you can collect and view the trace files by using the Unified Communications Trace and Log Central option in the Unified Communications Real-Time Monitoring Tool (RTMT). Trace and Log Central is the Unified Communications component which manages and provides access to trace files. When the services start up (during the post-installation process), the trace/log files are visible in the RTMT Trace and Log Central section once you launch RTMT. Refer to **Cisco Unified Real-Time Monitoring Tool Administration Guide** (http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html) for detailed information.

Configuring Trace File Information

Caution: Enable trace flags only for troubleshooting purposes and remember to disable trace flag settings once the debugging session is complete.

To configure trace file information and to enable and disable trace Āag settings, follow this procedure.

Step 1 From the Unified MCP Serviceability Administration select **Trace** > **Configuration**.

The Trace Configuration web page opens displaying the configured Unified MCP services (see Available Unified MCP Services (page 58)) along with the applicable trace Āags for each service.

Step 2 For each service, select the required log levels and trace Āags (see About Unified MCPLog Levels (page 57)).

Step 3 Click **Save** to generate the trace files per the configured settings.

Alternately, click **Reset** to revert to the default settings for the selected service or click **Cancel** to revert to your previous settings.

Step 4 Retrieve the saved file from the corresponding location (see Trace File location (page 58)).

See the Viewing and Interpreting Trace Files (page 59) section for details on analyzing Unified MCP trace files.

Viewing and Interpreting Trace Files

The Unified MCP server stores the trace files in a Log folder within the folder in which you installed the Unified MCP component. You can collect and view trace information using the Real-Time Monitoring Tool (RTMT). See Using the Unified Communications RTMT Administration (page 71)for more information.

Using Unified MCP Serviceability Administration Tools

See the Understanding Unified MCP Services (page 19) section for more details on network and feature services.

Control Center in the Unified MCP Serviceability Administration allows you to perform the following tasks:

- Enabling or Disabling Feature Services (page 62)
- Starting and Stopping Unified MCP Network Services (page 63)
- Starting and Stopping Unified MCP Feature Services (page 64)
- Installing and Configuring RTMT (page 72)

Note: You may need to manage services in both Unified MCP Serviceability and Cisco Unified Serviceability to troubleshoot a problem.The Cisco Unified Serviceability services are described in the **Cisco Unified Serviceability Administration Guide** (http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html).

Understanding Service Activation

Once all the feature services are assigned to two servers in the cluster, the system only allows you enable the Call Control Service, the Media Service, and the SM Agent in the remaining servers in the Unified MCP deployment.

Unified MCP Serviceability only allows you to enable and disable feature services (not network services). You may enable or disable multiple services at the same time. Some feature services depend on other services, and the dependent services must also be turned on at the same time.

You can enable or disable the following Unified MCP services from the Service Activation page:

- Configuration Service (page 20)
- API Service (page 20)
- Media Service (page 21)
- Call Control Service (page 21)
- Database Service (page 20)
- SM Agent (page 21)

Service Activation States

All applicable feature services are enabled in each server as provided in the Setup Summary page of your Unified MCP Post-Installation Setup wizard (see the *Feature Service Status Description* table in the Completing the Installation for the Primary Server (page 28)section for status descriptions).

Note: If a service remains in the Error or Disabled state, these service states do not apply.

Once enabled, each service can be in one of the following states at any give time:

Table 5: Possible States for Enabled Services

Possible States for Enabled Unified MCP Services	Description
In service	If a service is enabled and running without any errors, it displays the "In service" state. **Note:** The cluster details are displayed in theCluster Access (page 65) web page only if the Unfied MCP Configuration Service is in the In service state in either the primary server or the secondary server. **Caution: Even if it is already enabled, the Call Control Service will not be In service until the Unified CM information is configured. See Configuring the Call Control Service Connection (page 41).**
Shutdown	A service displays the shutdown state if one of the following situations apply: • The service is enabled but has been manually stopped. • The service failed and shut down automatically. **Caution: For any reason, if the primary Unified MCP server is shutdown or in a failed state, and the secondary Unified MCP server continues to function in the normal state, and if you launch the RTMT client at this time, then it is possible for the Unified MCP tab in the Alert Central window to remain blank and display the `HTTP request failed. Web Server`**

Possible States for Enabled Unified MCP Services	Description
	`unreachable.` **message in the status pane. See Configuring Cisco AMC Service in Unified CM (page 77) for more information.**
Shutting down	This is the interim state of the service after it was enabled and then shut down.
Initializing	This is the interim state of the service after it was started.
Not configured	The service remains in this state if a new server was added and one or more services were not configured in this server.
Unknown	This state is displayed if any of the above states do not apply.

Enabling or Disabling Feature Services

To enable or disable Unified MCP feature services, follow this procedure.

Step 1 From the Unified MCP Serviceability menu bar, click **Tools** and select **Service Activation**.

Services that display in the Service Activation window do not start until you enable them.

The Service Activation web page displays the configurable Unified MCP services along with its activation status for the default server (the primary server in the cluster).

To view the feature service activation status for another server in the cluster, select the required server from the server drop-down list box and click **Go**.

Step 2 Select **Enable** or **Disable** from the drop-down list box next to the service name.

A progress message displays in the Status section (below the tool bar) to indicate the task completion or corresponding error message as applicable.

The list of services will differ based on the server--the primary and secondary servers display all feature services while the remaining expansion servers only contain the Media Service (page 21), Call Control Service (page 21), and SM Agent (page 21).

Step 3 Click **Apply** to save your changes.

A progress message displays in the Status section to indicate that your configuration changes are being applied.

Click **Reset** changes all enabled services to the disabled state.

Note: At any time, click **Refresh** to update the screen and the deployment with the latest status of the services.

Control Center - Network Services

Unified MCP network services are installed automatically (see Understanding Unified MCP Services (page 19) for more details). Because these services are required for basic functionality you cannot enable or disable them in the Service Activation window. After the installation, network services start automatically in each server in the cluster. You can stop the network services if a necessity arises to perform this function.

Note: The local server time is displayed in the Administration Interface. This time cannot be configured.

Starting and Stopping Unified MCP Network Services

To start, stop, and restart network services, follow this procedure.

Step 1 From the Unified MCP Serviceability menu bar, click **Tools** and select **Control Center - Network Services**.

Services that display in the Control Center - Network Services window do not start until you start each service.

The Control Center - Network Services web page displays the configurable Unified MCP services along with its service status for the default server (the primary server in the cluster).

To view the network service status for another server in the cluster, select the required server from the server drop-down list box and click **Go**.

Step 2 To start, stop, or restart services, check the check box preceding the required Service Name.

A check mark appears in the check box to indicate your selection.

Step 3 Click the **Start**, **Stop**, or **Restart** button to perform the required operation.

A progress message displays in the Status section (below the tool bar) to indicate the task completion or corresponding error message as applicable.

Note: At any time, click **Refresh** to update the screen and the deployment with the latest status of the services.

Control Center - Feature Services

Unified MCP Serviceability provides several options to control feature services (see Understanding Unified MCP Services (page 19) for more details).

By enabling a service, you are essentially starting the service. Once you enable the service, you do not need to explicitly start the service--unless the service does not start automatically for any

reason. See Enabling and Disabling Feature Services (page 62) for detailed instructions on enabling feature services.

Starting and Stopping Unified MCP Feature Services

To start, stop, or restart Unified MCP feature services, follow this procedure.

Step 1 From the Unified MCP Serviceability menu bar, click **Tools** and select **Control Center - Feature Services**.

Services that display in the Control Center - Feature Services window do not start until you start each service.

The Control Center - Feature Services web page displays the configurable Unified MCP services along with its service status for the default server (the primary server in the cluster).

Step 2 To start, stop, or restart services, check the check box preceding the required Service Name.

A check mark appears in the check box to indicate your selection.

The list of services will differ based on the server--the first and second servers display all feature services while the remaining servers only display the Call Control Service (page 21) and Media Service (page 21).

Step 3 Click the **Start**, **Stop**, or **Restart** button to perform the required operation.

A progress message displays in the Status section (below the tool bar) to indicate the task completion or corresponding error message as applicable.

Note: At any time, click **Refresh** to update the screen and the deployment with the latest status of the services.

Reactivating the Media Service, Call Control Service, or Database Service

Reactivating the Media Service, the Call Control Service, or the Database Service results in the following consequences:

- The existing recordings before the restart will not be available after the reactivation.
- You can only record new calls after the service is reactivated.

Note: Reactivate/restart Call Control, Database, and Media Services during off-peak hours to ensure minimum disruption to recordings in progress.

Accessing the Serviceability UI for Other Servers in a Cluster

To access the Serviceability UI for any of the other servers in a Unified MCP cluster, follow this procedure.

Note: The Unified MCP Configuration Service must be in the *In service* state in either the primary server or the secondary server so the cluster details can be displayed in the Cluster Access web page.

Step 1 From the Unified MCP Serviceability menu bar, click **Tools** and select **Unified MCP Cluster Access**.

The Unified MCP Cluster Access web page displays the available links for each server in this cluster. Each server is identified as a primary server, a secondary server, or an expansion server in this page. The corresponding link takes you to the Unified MCP Serviceability Administration for this server. You must sign in to this server to continue.

Step 2 In the Unified MCP Serviceability Administration authentication window, enter the User ID and password for this server. Click **Sign in**.

You can now access the Serviceability UI for the applicable server in this cluster.

Chapter 5

Using the Disaster Recovery System Administration

The Unified Communications platform is the underlying platform used by Unified MCP.

This section acts as a companion to the following guides:

- *Cisco Unified Communications Operating System Administration Guide*
- *Disaster Recovery System Administration Guide*
- *Cisco Unified Real-Time Monitoring Tool Administration Guide*
- Cisco Unified Serviceability services are described in the **Cisco Unified Serviceability Administration Guide** (http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html).

These four guides provide detailed conceptual information about the Unified Communications platform and its components.

These guides are available in two ways:

- Online help files: From the corresponding Unified Communications Administration for Unified MCP.
- Cisco.com (CDC): HTML or PDF files available at .html**http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html**

While Unified MCP uses the underlying Unified Communications platform, certain features, settings, and fields need to be changed to work with Unified MCP.

This section identifies those details for the DRS Administration and also provides a list of features which do not work with Unified MCP.

This chapter contains the following topics:

About Unified Communications DRS

The Disaster Recovery System (DRS) can be invoked from Unified MCP Administration and provides full data backup and restore capabilities for all servers in a Unified MCP cluster. The DRS allows you to perform regularly scheduled automatic or user-invoked data backups. In case of high availability, the DRS performs a cluster-level backup, which means that it collects backups for all servers in a Unified MCP cluster to a central location and archives the backup data to a physical storage device. The DRS restores its own settings (backup device settings and schedule settings) as part of the platform backup/restore. DRS backs up and restores drfDevice.xml and drfSchedule.xml files. When the server is restored with these files, you do not need to reconfigure the DRS backup device and schedule.

Note: You need to follow the Unified CM authentication procedure to access the Disaster Recovery System Administration.

Supported Features and Components

Unified Communications DRS automatically backs up and restores the following components.

- Cluster configurations and applications profile in the data repository
- Recording files
- Platform information
- Trace collection information

Additionally, the DRS also backs up and restores the following Unified MCP-specific components

- Unified MCP Call Control Service
- Unified MCP API Service
- Unified MCP Database Service (includes both config database and meta database information)
- Unified MCP Media Service
- Unified MCP Configuration Service
- Unified MCP Storage Management Agent (SM Agent)
- Unified MCP Administration
- Unified MCP Serviceability Administration

All components are backed up and restored from/to the appropriate level within the /opt/cisco/ora/conf folder.

Caution: When performing the restore, be sure to indicate the exact version used for the backup. If you indicate a different version, the restore operation may not work.

Other than the database scenarios, there is no replication across servers in this release of Unified MCP. Non-database components are backed up/restored on a per-server basis and are not replicated across the Unified MCP cluster. The Database component restored on the primary server is automatically replicated to other servers in the Unified MCP cluster. The other Unified MCP components are individually backed up and restored by the DRS application for each server.

Note: When performing backup and restore, be sure to add a backup device and provide the storage location details for the SFTP server. If the IP address/hostname information does not change for the SFTP server between the backup and restore time frame, you can access the backup files stored on the SFTP server.

Chapter 6

Using the Unified Communications RTMT Administration

The Unified Communications platform is the underlying platform used by Unified MCP.

This section acts as a companion to the following guides:

- *Cisco Unified Communications Operating System Administration Guide*
- *Disaster Recovery System Administration Guide*
- *Cisco Unified Real-Time Monitoring Tool Administration Guide*
- The Cisco Unified Serviceability services are described in the **Cisco Unified Serviceability Administration Guide** (http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html).

These four guides provide detailed conceptual information about the Unified Communications platform and its components.

These guides are available in two ways:

- Online help files: From the corresponding Unified Communications Administration for Unified MCP.
- Cisco.com (CDC): HTML or PDF files available at .html**http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html**

While Unified MCP uses the underlying Unified Communications platform, certain features, settings, and fields need to be changed to work with Unified MCP.

This section identifies those details for the Unified Communications RTMT Administration and also provides a list of features which do not work with Unified MCP. For all other details refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide* .

This chapter contains the following topics:

About Unified Communications RTMT Administration

This section provides details specific to Unified MCP for the Real-Time Monitoring Tool (RTMT). The RTMT tool, which runs as a client-side application, uses HTTPS and TCP to monitor system performance and device (page 94) status for Unified MCP. RTMT can connect directly to devices (page 94) via HTTPS to troubleshoot system problems.

Note: Even when RTMT is not running as an application on your desktop, tasks such as alarm and performance monitoring updates continue to take place on the server in the background.

Caution: The VLT Plugin is not available in Unified MCP. This is because Cisco VLT does not support message files involving Session Initiation Protocol (SIP) calls.

Warning: The Maximum Number of Processes and Threads field is required by Unified CM in the Unified OS. This field specifies the number of Processes and Threads running on the server. It the total number of processes and threads exceed the maximum number (3000), an alarm and corresponding alert are generated. Because of this Unified OS restriction, you cannot monitor more than 3000 process and threads in a Unified MCP system. Unified MCP regularly creates more than 3000 processes and threads. Because of this limitation, you will not be able to monitor all processes generated by Unified MCP. See the Unified CM documentation (http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html)for more information on the Maximum Number of Processes and Threads.

Installing and Configuring RTMT

You can install RTMT on a computer that is compatible with the Unified MCP software. To install the RTMT plug-in from The Unified MCP Administration, see the Downloading the RTMT Plugin (page 73) section in this guide.

Note: See *Hardware & System Software Specification (Bill of Materials) for Cisco Unified Contact Center Enterprise Guide* available at the following website: **http://www.cisco.com/**

en/US/products/sw/custcosw/ps1844/products_user_guide_list.html to obtain a complete list of supported hardware and software information for Unified MCP.

Downloading the RTMT Plugin

To download the RTMT Plugin, follow this procedure.

Step 1 From the Unified MCP Serviceability menu bar, click **Tools** and select **RTMT Plugin Download**.

The RTMT Plugin Download web page displays.

Step 2 To download the RTMT Plugin executable to the preferred location on the client machine, click **Download**.

Follow the download procedure to install RTMT on your client

Step 3 After the RTMT welcome window displays, click **Next**.

Step 4 To accept the license agreement, check the button next to **I accept the terms of the license agreement**; then, click **Next**.

Step 5 Choose the location where you want to install RTMT. If you do not want to use the default location, click **Browse** and navigate to a different location. Click **Next.**

Step 6 To begin the installation, click **Next**.

The Setup Status window displays. Do not click Cancel.

Step 7 To complete the installation, click **Finish.**

Upgrading RTMT

When you use the tool (RTMT), it saves user preferences and downloaded module jar files locally on the client server. The system saves user-created profiles in the database, so you can access these items in RTMT after you upgrade the tool.

Note: To ensure compatibility, Cisco recommends that you upgrade RTMT after you complete the Unified MCP Administration upgrade on all servers in the cluster (page 94).

Installing Multiple Copies of RTMT

A single version of RTMT can only monitor one cluster for one product (based on compatibility with the product).

To monitor a product on a server or node in a different cluster, you must first log off the server or node before you can log on to the other server.

Monitoring Server Status

The Systems tab lists all critical services related to the system and the Unified MCP tab defines all critical services related to the Unified MCP. These critical services are enabled when VOS starts.

Understanding Performance Monitoring

Cisco Unified Communications provides counters for application performance monitoring. These counters are frequently referred to as *perfmon counters*. Perfmon counters allow to track application performance in real time. You can monitor the performance of various system components by choosing the counters for any object in RTMT. The counters for each object display when you expand the folder. Refer to **Cisco Unified Real-Time Monitoring Tool Administration Guide** (http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html) for detailed information on the interface and logs.

Unified MCP directly updates perfmon counters.The counters contain simple, useful information on the system and devices (page 94) on the system, such as the number of Unified MCP perfmon counters.

Single object contains most of the Unified MCP performance counters, and these counters have only one instance. The instance-based counters that belong to the other objects can have zero or more instances.

Using RTMT for Perfmon

RTMT integrates with the administration and serviceability software for Unified MCP. RTMT displays performance information for all Unified MCP components. RTMT provides alert notification for troubleshooting performance. It also periodically polls performance counter to display data for that counter.

Perfmon allows you to perform the following tasks:

- Monitor performance counters including all the Unified MCP nodes in a cluster.
- Monitor Unified MCP servers.
- Continuously monitor a set of preconfigured objects and receive notification in the form of an e-mail message.
- Associate counter threshold settings to alert notification. An e-mail or popup message provides notification to the administrator.
- Save and restore settings, such as counters being monitored, threshold settings, and alert notifications, for customized troubleshooting tasks.
- Display up to six Perfmon counters in one chart for performance comparisons.

Displaying System Condition and Perfmon Counter Alerts

RTMT displays both preconfigured alerts and custom alerts in Alert Central. RTMT organizes the alerts under different tabs—System, Custom, and Unified MCP. While the System and Custom tabs are the same as those available in Unified CM, the Unified MCP tab is specific to the Unified MCP application.

In Unified MCP, system conditions are used to interpret the working state of the system. Whenever a error/critical situation arises which prevents the system from functioning at its maximum capacity, a system condition is raised to indicate the problem. When the problem is resolved the system condition is cleared and the system returns to normal state. The system condition contains information about the problem and possible corrective actions to address the problem. System Conditions are associated with log messages. Log messages can raise and clear a set of system conditions. The various Unified MCP log messages can have a system condition which can be raised and cleared based on the log message.

All system conditions and perfmon counter alerts for the Unified MCP application are visible as individual RTMT alerts in the Alert Central tool in RTMT under the Unified MCP tab. Each alert description explains the system condition and possible resolution actions.

Items in red indicate that an alert has been raised. If the alert is cleared, the timestamp is updated by the alert (continues to remain red so that it is visible when the administrator signs in). In the Safe region, the *Yes* indicates that the alert was raised under normal conditions, and the *NA* indicates that the safe range field is not applicable to the system condition.

The following table lists the preconfigured system condition (preceded by SC_) and perfmon counter (preceded by PC_) alerts and its corresponding description within each Unified MCP service class object.

Table 6: Unified MCP RTMT Alert Descriptions

Service	**Alert** **SC_ = System condition alert** **PC_ = Perfmon counter alert**	**Description**	**Recommended Action**
Cisco Tomcat (Config Service)	SC_ConfigLostContactWithDB	The Configuration Service lost contact with its database service.	Check the Unified MCP Database Service. Restart this service if necessary.
	SC_ConfigurationOOS	The Configuration Service is out of service.	Check the Unified MCP Configuration Service. Restart this service if necessary.
	SC_ConfigurationLostContactWithAXL	The Configuration Service lost contact with its Unified CM AXL server.	Check the Unified CM AXL configuration. Modify or restart if necessary.
Cisco Tomcat	SC_AdministrationOOS	The Administration Service is out of service.	Check the Unified MCP Administration Service. Restart if necessary.

Service	Alert SC_ = System condition alert PC_ = Perfmon counter alert	Description	Recommended Action
(Admin Service)			
Unified MCP Call Control Service	SC_CallControlLoadWarning	Recording start latency exceeds warning threshold.	Check the Media server. Restart if necessary.
	SC_CallControlOOS	Call Control Service is out of service.	Check the Call Control server. Restart if necessary.
	SC_CallControlLostContactWithAPI	Call Control Service lost contact with API Service.	Check the API server. Restart if necessary.
	SC_CallControlLostContactWithMedia	Call Control Service lost contact with Media Service.	Check the Media server. Restart if necessary.
	SC_CallControlLoadCritical	Call load exceeds critical threshold.	Reduce the load (by decreasing the number of phones, that are configured for recording in a given cluster) or install an additional Unified MCP server.
	PC_CallControlMaximumHeapMemory ThresholdReached	Safeguards the Unified MCP system from running out of memory. Once this counter crosses the 128 MB memory threshold, then the system triggers an alert.	Reduce the load (by decreasing the number of phones, that are configured for recording in a given cluster) or install an additional Unified MCP server.
Cisco Tomcat API Service	SC_APILostContactWithDatabase	API Service lost contact with its database service.	Check the Unified MCP Database Service. Restart this service if necessary.
	SC_APIServiceOOS	API Service is out of service.	Check if SC_ORA_API_LOST_ CONTACT_WITH_ DATABASE has also been raised. If yes, then check the Unified MCP Database Service. Restart this service if necessary. If that does not work restart Cisco Tomcat (API Service). If SC_ORA_API_LOST_ CONTACT_WITH_ DATABASE has not been raised, then restart Cisco Tomcat (API Service).
Cisco Tomcat ORA Service	SC_ServiceabilityOOS	The Serviceability Administration Service is out of service.	The resolution string must be replaced.

Service	Alert SC_ = System condition alert PC_ = Perfmon counter alert	Description	Recommended Action
Unified MCP System Service	SC_SystemServiceOOS	The Unified MCP System Service is out of service	Check System Service. Restart this service if necessary.
Unified MCP Database Service	SC_DatabaseServiceOOS	Database Service is out of service.	Check the Database Service. Restart this service if necessary.
Unified MCP Storage Management Agent	SC_DiskSpaceWarning	Available media storage level is low.	Consider deleting old recordings.
	SC_DiskSpaceCritical	Available media storage level is critical. The system may fail to process new requests.	Delete old recordings to free up storage space.
	SC_DiskSpaceEmergency	No media storage space is available. This server is not functional.	Delete old recordings to free up storage space.

Configuring Cisco AMC Service in Unified CM

To support the RTMT client, a number of services need to be active and running on the Unified MCP server. Cisco AMC service is one such service which starts up automatically after the RTMT installation and allows the RTMT client to retrieve real-time information from the Unfied MCP server. This service, the Alert Manager, and the Collector service, allow RTMT to retrieve real-time information from the server (or from all servers in the Unified MCP cluster).

To view the state of the Cisco AMC service, navigate to the Unified CM Administration on Unified MCP server, choose **System** > **Service Parameters** to view the state of the CiscoAMC service. Then, choose the required server and select the **Cisco AMC service**. For more information on the Cisco AMC Service, see the **Cisco Unified Real-Time Monitoring Tool Administration Guide:** (http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html)

Caution: For any reason, if the primary Unified MCP server is shutdown or in a failed state, and the secondary Unified MCP server continues to function in the normal state, and if you launch the RTMT client at this time, then it is possible for the Unified MCP tab in the Alert Central window to remain blank and display the `Error polling alert \ status. AMC service is down.` message in the status pane. Similarly, it is possible for the System Summary pane to display the `HTTP request failed. Web Server unreachable.` error message for the same issue. To work around this issue, be sure to configure the secondary Cisco AMC Service in in the primary Unified MCP server.

Note: Be sure to make the following change in the **primary Unified MCP server.**

Navigate to Unified CM Administration (in **the primary Unified MCP server.**). Choose **System** > **Service Parameters**. Then, select the secondary Unified MCP server from the drop-down

list, and finally select **Cisco AMC Service**. In the resulting Service Parameter Configuration web page, select the secondary Unfied MCP server from the drop down list next to the **Failover Collector** field. Once you configure the Cisco AMC Service for the secondary Unified MCP server, then the secondary takes over when the primaryUnified MCP goes down, and RTMT continues to display alerts names under Alert Central.

Note: You can access the Unified CM Administration inUnified MCP server by providing the following URL format in a browser window: http://<UnifiedMCPserver-ip-address>/ccmadmin.

Configuring Trace & Log Central in RTMT

The Trace & Log Central feature in RTMT allows you to configure on-demand trace collection for a specific date range or an absolute time. You can collect trace files that contain search criteria that you specify and save the trace collection criteria for later use, schedule one recurring trace collection and download the tracefiles to a SFTP or FTP server on your network, or collect a crash dumpfile. After you collect thefiles, you can view them in the appropriate viewer within RTMT. You can also view traces on the server without downloading the trace files by using the remote browse feature. You can open the trace files by either selecting the internal viewer that is provided with RTMT or choosing an appropriate application as an external viewer.

Note: To use the Trace & Log Central feature in RTMT, make sure that RTMT can access all of the nodes in the cluster (page 94) directly without Network Access Translation (NAT).

Collecting Files

Caution: In Unified MCP, throttling is turned on by default, and cannot be configured.

The Collect Files tool allows you to specify the required Unified MCP services and application in the Select MCP Services/Application tab which is part of the Collect Files wizard. Once you specify the required Unified MCP services, continue to proceed as you would for the System Service/Application. You can collect trace files that contain search criteria that you specify and save the trace collection criteria for later use.

Collecting a Crash Dump

Cisco Unified Serviceability stores the logs for the version of application that you are logged in to in the active partition and stores the logs for the other version (if installed) in the inactive folder.

Using Remote Browse

For .log and/or .out files—Use one of the following methods: –

- Right-click the required file and select **Open** to view it in the Cisco Default Viewer.
- Alternately, you can also right-click on the required file and select **Open** with to view all available applications with which to open these files.

Caution: The Cisco QRT Viewer application is not supported by Unified MCP as an option to view files.

The log and trace file folder name for each Unified MCP service is identified in the following table.

Table 7: Unified MCP Trace File Folder Name for Each Service

Service	Remote Browse Folder Name
Unified MCP Call Control Service (page 21)	callcontrol
Unified MCP Media Service (page 21)	media
Unified MCP API Service (page 20)	ora
Unified MCP Configuration Service (page 20)	oraconfiguration
Unified MCP Database Service (page 20)	oradb
SM Agent (page 21)	storagemanagementagent
Unified MCP Administration (page 37)	oraadmin
Unified MCP Serviceability Administration (page 55)	oraservice
Unified MCP System Service	systemservice
Unified MCP Perfmon Agent	perfmonagent

Some files may use the ZIP format and in these cases, you will need to use the .zip file viewer to view these files

Caution: Unified MCP provides some log files in a ZIP format. The Trace & Log Central Remote Browse feature in Cisco Unified Communications RTMT does not display .zip files by default. You can choose to add the appropriate application or download/save the .zip file and view it directly from the downloaded location.

Unified MCP Perfmon Counters

This section provides information on system-related objects and counters. All Unified MCP's perfmon counters are logged in RTMT by default.

Note: For the latest performance monitoring counters, objects, and counter descriptions that are available for system monitoring, access the performance monitoring counters in RTMT.

The Unified MCP Perfmon Agent controls the performance monitoring infrastructure. It does not have a separate UI and operates seamlessly within the Unified MCP Serviceability Administration. Like other network services, the Perfmon Agent is operational at start up. The Java Management Extensions (JMX) technology which allows you to manage and monitor

applications and other system objects are represented by objects called ManagedBeans (MBeans). The Perfmon Agent retrieves the counter values from the JMX MBeans and writes it to the Unified CM database.

The class object provides information on different process or time usage in percentages. The following table contains information on processor counters.

Table 8: Perfmon (JMX) Counter Description

Counters	Counter Descriptions
Class: Unified MCP Call Control Service	
Recording Sessions counters	
Heap memory usage	Safeguards the Unified MCP system from running out of memory. Once this counter crosses the 128 MB memory threshold, then the system triggers an alert.
Number of active sessions	The number of active recording sessions.
Number of recorded sessions without errors	The number of recorded sessions, completed without errors.
Number of recorded sessions with errors	The number of recorded sessions, completed with errors.
Recording Setup Time	
Mean setup delay	Average delay (in milliseconds) between the initial receipt of the SIP Invite from Unified CM and the SIP response to the Unified CM. rolling window time.
Max setup delay	Maximum delay (in milliseconds) between the initial receipt of the SIP Invite from Unified CM and the SIP response to the Unified CM. rolling window time.
Class: Unified MCP Media Service	
Number of active playbacks	The number of outgoing RTSP sessions.
Number of live monitored calls	The number of ports used. A single monitored call in most cases uses two ports.
Class: Unified MCP Configuration Service	
Authentication request Processing: Average latency	The average latency for processing an authentication request.
Authentication request Processing: Max latency	The maximum latency for processing an Authentication request.
Total Requests	Total number of requests received by the Unified MCP Configuration Service
Total Failures	Total number of requests encountered by the Unified MCP Configuration Service
Class: Unified MCP API Service	
Mean query response time	The average query response time over the last one hour.
Max query response time	The maximum query response time over the last one hour.
Total number of responses	Total number of successful and unsuccessful responses.
Total number of requests	Total number of requests received and serviced by the API Service.

Counters	Counter Descriptions
Avg time per request	The average time for each request received and serviced by the Call Control Service over the last one hour.
Max time per request	The maximum time for each request received and serviced by the Call Control Service over the last one hour.
Max number of concurrent requests	The maximum number of concurrent requests received and serviced by the Call Control Service over the last one hour.
Total number of current concurrent requests in progress	The total number of current concurrent requests in progress over the last one hour.
Class: Unified MCP Database Service	
This class does not have any perfmon counters.	
Class: Unified MCP SM Agent	
This class does not have any perfmon counters.	
Class: Unified MCP System Service	
This class does not have any perfmon counters.	
Class: Unified MCP Administration	
This class does not have any perfmon counters.	
Class: Unified MCP Serviceability Administration	
This class does not have any perfmon counters.	

Chapter 7

Understanding Port Information

The section provides a list of the TCP and UDP ports used by Unified MCP, Release 8.5(x).

Note: None of these ports can be configured by the user. This table represents the values in effect when the Unified MCP system is installed.

The columns in the Port Utilization table describe the following items:

- **Server or Application Protocol**: Name of the open or private application protocol.
- **Server Protocol/Port**: An identifier for the TCP or UDP port that the Server or application is listening on, along with the IP address for incoming connection requests when acting as a server.
- **Remote Protocol/Port**: The identifier for the TCP or UDP port that the remote service or application is listening on, along with the IP address for incoming connection requests when acting as the server.
- **Remote Device**: The remote application or device making a connection to the server or service specified by the protocol; or listening on the remote protocol/port.
- **Notes**: Additional descriptions for each port.

Table 9: Unified MCP Port Utilization

Server or Application Protocol	Server Protocol/Port	Remote Protocol/Port	Remote Device	Notes
HTTPS	TCP 443, 8443			Unified MCP API Secure Port, Configuration Service Secure Port, Secure Port used by Unified MCP Administration and Unified MCP

Server or Application Protocol	Server Protocol/Port	Remote Protocol/Port	Remote Device	Notes
				Serviceability Administration.
HTTP	TCP 80, 8080			Unified MCP API Non-Secure Port, Configuration Service Non-Secure Port, Non-Secure Port used by Unified MCP Administration and Unified MCP Serviceability Administration.
SIP	TCP 5060 UDP 5060	TCP 5060 UDP 5060	Unified CM or Cisco Unified Border Element (CUBE)	SIP non-secure communication.
RTSP	TCP 554		Recording playback	RTSP port used by the Media Service.
HTTP	TCP 8085	TCP 8085	API Service and Configuration Service	HTTP Port used by the Call Control Service.
HTTP	TCP 8081	TCP 8081	API Service and CallControl Service	HTTP Port used by the Media Service.
SSL	TCP 443	TCP 443		Secure Port used by the Media Service.
HTTP	TCP 8087	TCP 8087	Unified MCP Administration and Unified MCP Serviceability Administration network services.	HTTP Port used by the Unified MCP System Service
HTTP	TCP 8084	TCP 8084	API Service and Call Control service	HTTP port used by the SM Agent (page 21).
TCP/IP	TCP 1543	Any	Peer database server(primary server or secondary server), API Service, Configuration Service, and the SQL client (for example, SQuirreL).	Used by Informix Enterprise Replication (ER) between the primary server and the secondary server. Used by the API Service or Configuration Service to make a JDBC connection with Informix

Server or Application Protocol	Server Protocol/Port	Remote Protocol/Port	Remote Device	Notes
Keep-alive heartbeats	UDP 8091	UDP 8091	Call Control Service on other servers in the cluster.	UDP port that is used by the Call Control Service to detect availability of other Call Control Services.
Call Control Service JMX port	TCP 7000	Any	Unified MCP Perfmon JMX Service	
System Service JMX port	TCP 7002	Any	Unified MCP Perfmon JMX Service	
Cisco Tomcat JMX port	TCP 7003	Any	Unified MCP Perfmon JMX Service	
SM Agent JMX port	TCP 7005	Any	Unified MCP Perfmon JMX Service	
Ephemeral port range	UDP 32768 - 61000	Any	Phone or gateway that sends RTP media streams.	Media Service can use ports from this range to receive RTP media streams.

Chapter 8

CLI Commands

The Command Line Interface (CLI) provides a set of commands applicable to Unified MCP. These commands allow basic maintenance, failure recovery, and enable basic system administration when the Unified MCP Administration is unavailable.

This chapter contains the following topics:

About CLI Commands

The Unified MCP Administration is enabled for login at the completion of the installation and is the primary interface for administering, configuring, and maintaining Unified MCP. If the Unified MCP Administration is not accessible for any reason, you can use the CLI commands specified in this chapter to perform certain tasks.

In the command syntax descriptions:

- **Bold** is used for the base command.
- *Italics* are used for mandatory parameters, when the syntax includes them.
- [brackets] are used for options, when the syntax includes them.

Unified MCP supports all Platform CLI commands supported by Unified CM. See the *Command Line Interface Reference Guides* at **http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html** for a list of supported CLI commands.

Accessing the CLI

You can access the CLI as follows:

- Directly, using the monitor and keyboard at the server console.
- Using SSH.

Step 1 At either the login prompt or the SSH client, enter the Unified MCP application administrator ID (created during the installation of the primary server).

Step 2 When prompted, enter the Unified MCP application administrator password.

You can start entering commands at the next prompt.

In addition to the CLI commands listed in the *Command Line Interface Reference Guides* and this chapter, you can also enter the following commands:

- **help**: To display the list of all supported commands. For example, to display help for a specific command, type **`help utils service list`** and press Enter.
- **quit**: to close the CLI.

Utils Commands

The section provides details on the Unified MCP-specific **utils** commands in this release.

utils media recording_sessions

This command generates a html file with a detailed list of the last 100 recording sessions processed in this Unified MCP server. The Unified MCP Call Control Service should be running for this command to execute successfully. The file is saved to the platform/cli/ folder and can be downloaded using the **`file get activelog platform/cli/fileName`** CLI command.

Command: **utils media recording_sessions** *file fileName*

Details:

- *file* is a mandatory parameter to output the information to a file.
- *fileName* is a mandatory parameter to define the name of the .html file.
- When you issue this command, you get the following response:

Unified MCP Call Control Service Recording sessions saved in platform/cli/<filename>.html You can now download it using: file get activelog platform/cli/<filename>.html

You can then retrieve the file from that directory and save it to a location of your choice.

Example:

- **utils media recording_sessions file sessions.html**

  Unified MCP Call Control Service Recording sessions saved in platform/cli/sessions.html You can now download it using: file get activelog platform/cli/sessions.html

utils service

This command starts, stops, restarts, or lists each of the Unified MCP services.

Command: **utils service** *operation service_name*

Details:

- *operation* specifies the type of operation to be performed by this command:

  The valid operations are:

  – *start*

  – *stop*

  – *restart*

  – *list*

- *service_name* specifies the name of the Unified MCP service for which you require the specified operation.

  The valid services are:

  – *Unified MCP Administration*

  – *Unified MCP Configuration Service*

  – *Unified MCP Database Service*

  – *Unified MCP Perfmon Agent*

  – *Unified MCP System Service Administration*

  – *Unified MCP API Service*

– *Unified MCP Call Control Service*

– *Unified MCP Media Service*

– *Unified MCP Storage Management Agent*

Examples:

- **`utils service list`**
- **`utils service start Unified MCP configuration service`**

Run Commands

The section provides details on the Unified MCP-specific **run** command in this release.

run db_reset_replication

This command is used to begin the process to manually reset replication for the entire Unified MCP database. Once the reset process is complete, this command returns a message with the status of the reset. You may need to use this command if the primary node fails within a multi-node cluster. See Considerations for Data Replication (page 27) for details on data replication.

Note: In a multi-server deployment, you can only run this command on the secondary server.

Command: **run db_reset_replication**

Details:

- This command does not have any options.

Example:

- **`run db_reset_replication`**

run db_synchronization

This command is used to compare the databases in the primary and secondary servers to ensure that the databases are synchronized. See Considerations for Data Replication (page 27) for details on data replication.

Note: In a multi-server deployment, you can only run this command on the secondary server.

Command: **run db_synchronization** *database_name*

Details:

- *database_name* specifies the type of operation to be performed by this command:

  The valid database names are:

  – *db_ora_config*

  – *db_ora_meta*

Example:

- **`run db_synchronization db_ora_config`**
- **`run db_synchronization db_ora_meta`**

show Commands

The section provides details on the Unified MCP-specific **show** commands in this release.

show db_synchronization status

This command monitors the status of the run db_synchronization command and displays one row for each database table and the corresponding status for that table. See Considerations for Data Replication (page 27) for details on data replication.

Note: In a multi-server deployment, you can only run this command on the secondary server.

Command: **show db_synchronization status** *database_name*

Details:

- *database_name* specifies the type of operation to be performed by this command:

  The valid database names are:

  – *db_ora_config*

  – *db_ora_meta*

- For each database table, the displayed output shows the start/end time of synchronization check, the number of rows to be checked, the number of rows already processed, and the replication check status.

  The replication check column displays the status of the replication as follows:

  – D = Defined

- R = Running
- C = Completed
- F = Completed, but inconsistent
- W = Pending Complete

Examples:

- **`show db_synchronization status db_ora_config`**
- **`show db_synchronization status db_ora_meta`**

show tech call_control_service

This command displays information on the Unified MCP Call Control Service that runs on the system. The Unified MCP Call Control Service should be running for this command to execute successfully.

Command: **show tech call_control_service** *detailed*

Details:

- When you issue this command, the Unified MCP Call Control Service details for this server are displayed in your CLI window.
- The *detailed* option specifies the type of information to download.

  Not specifying this option only provides information about the system start time, system information, recording sessions information, state of each adapter, configuration information for each adapter, and statistics for each adapter.

  Specifying this option provides all thread details, system condition details what is already provided above.

Example:

- **`show tech call_control_service`**
- **`show tech call_control_service detailed`**

Glossary

active server

An active server is a server that has one instance of each of the feature services (API Service (page 20), Configuration Service (page 20), Call Control Service (page 21), Media Service (page 21), Database Service (page 20), and SM Agent (page 21)). A Unified MCP deployment must have at least one, or at most, two active servers. Replication is available in both servers. For high availability (page 95) purposes, if one active sever goes down the other active server can handle the complete load for both servers.

API Service

Application Programming Interface (API) Service is a feature (page 95) service. Each Unified MCP cluster (page 94) can only have two instances of the API Service with only one instance in the primary server and another instance in the secondary server. Each API Service must have a corresponding Configuration Service (page 94). If a Unified MCP cluster has more than two servers, the additional servers will not have an API Service or Configuration Service. Each instance of the API Service corresponds directly to one instance of the Meta database (page 95).

call control

The Unified MCP system uses SIP for call control.A call control feature refers to any new call, transferred call, or call that is placed on hold.

Call Control Service

Call Control Service is a feature (page 95) service. It communicates with the network layer, the Media Service (page 21), and API Service (page 20) to provide key recording functions within the Unified MCP system. One instance of the Call Control Service is present in every server in a Unified MCP deployment.

cluster

Unified MCP servers are deployed in a cluster. A cluster can contain one to three Unified MCP servers. Depending on your deployment, each cluster can provide basic media recording and database storage and handle scalable recording capacity.

component

Each Unified MCP service can have one or more components.

Configuration database

The Configuration database is often referred to as the Config database. This database stores the log level and trace mask information. Each instance of the Configuration Service (page 20) corresponds directly to one instance of the Configuration database.

Configuration Service

Configuration Service is a feature (page 95) service. Each instance of the Configuration Service corresponds directly to one instance of the Configuration database (page 94). Each Unified MCP cluster can only have two instances of the Configuration Service with only one instance in the primary server and another instance in the secondary server. Each Configuration Service must have a corresponding API Service (page 20). If a Unified MCP cluster has more than two servers, the additional servers will not have an Configuration Service or API Service.

The Config database is not directly exposed to end users. You can indirectly configure functions such as service activation in the Unified MCP Serviceability web portal. All API calls are sent to the API Service.

Even if one Configuration Service does not function, the data will continue to be written to the other Configuration Service in your deployment as the Unified MCP product follows a peer-to-peer database model. As both Unified MCP servers with Configuration services are considered peers, the servers will not switch roles even if one of the two servers does not function.

database

Database refers to the two Unified MCP databases: the Config database (page 94) and the Meta database (page 95).

Database Service

Database Service is a feature (page 95) service. It contains and controls the two Unified MCP databases. Each Unified MCP cluster can only have two instances of the Database Service with only one instance in the primary server and another instance in the secondary server.

device

A *device* is a physical entity that can be an end point or a personal computer and refers to any item that can be recorded. A device is identified by a deviceRef which is a phone number or extension for each device.

Device Reference

A Device Reference (also referred to as deviceRef in the API and Device Ref in the Administration) refers to a phone number, IP address, URI/URL of each device (page 94). One or more participants (page 96) can be associated with multiple Device References.

expansion server

A Unified MCP deployment can have a maximum of three expansion servers. Each expansion server has one instance of the Call Control Service (page 21) and the Media Service (page 21). Expansion servers do not have any instances of either the API Service (page 20) or the Configuration Service (page 20).

feature service

Feature services allow you to configure and monitor all the servers in a Unified MCP deployment (see Understanding Unified MCP Services (page 19) for more details).

high availability

High availability is the term used to indicate that if one server fails, the other server can handle the complete load for both servers in a Unified MCP deployment. The data is load balanced between both servers and data replication is available in both servers.

live (Active) session

A session (page 97) can be *live* (active) or *recorded* (completed). A live session can be monitored and recorded at the same time. A recorded session can be played back at any time.

Media Service

Media Service is a feature (page 95) service. It terminates media streams (page 95) for storage on a local disk. One instance of the Media Service is present in every server in a Unified MCP deployment.

media stream

A media stream refers to the packets going through an audio channel or video channel in a live or recorded session (page 97). It refers to a live session versus a recorded session. A recorded media stream is called a track (page 97).

Meta database

The Meta database stores call history and metadata information associated with each recording. Each instance of the API Service corresponds directly to one instance of the Meta database (page 95).

network services

Network services allow you to configure and monitor overall system functions. Once you have installed the Unified MCP application and rebooted your server, the network services are enabled by default on all servers in a cluster.

participant

A participant refers to people or end points involved in a session (page 97). The participants use a device (page 94) to conduct a session. Participants are identified by the Device Reference (page 95) (phone number, IP address, or URL). Each track is associated with one participant generating the media for that track, Each track can also have one or more participants associated with different sessions.

Perfmon Agent

This network service controls the performance monitoring infrastructure. It does not have a separate UI and operates seamlessly within the Unified MCP Serviceability Administration.

primary database

The Configuration Service in the first main server in any deployment is called the primary database. Likewise, the Configuration Service in the second main server in any deployment is called the secondary database (page 96).

In a Unified MCP deployment, configuration requests are sent to both the primary database and secondary database. If the primary database is functional, data is written to the primary database and then replicated to the secondary database. If the primary database is not functional, data is not written to ensure data integrity. If the primary database is not functional for a substantial period of time, you can manually promote the secondary database to be the new primary database so the configuration data can continue to be written.When the original primary database begins functioning again, its role will be reversed as to being the new secondary database.

primary server

The primary server in a Unified MCP deployment refers to the first *node* (server) in the deployment. Once you install the Unified MCP application and reboot your server, all feature services are *enabled by default on the primary server* in a cluster. This server automatically becomes the primary server in the cluster.

recorded (completed) session

A session (page 97) can be *live* (active) or *recorded* (completed). A live session can be monitored and recorded at the same time. A recorded session can be played back at any time.

recording types

Two types of recordings are possible using Unified MCP:

- Forked media from a Cisco IP phone. This recording has two audio channels.

- Direct call to/from Unified MCP to any phone. This recording has one audio channel and one optional video channel. These recordings are referred to as blog recordings in this document.

secondary database

The Config database in the second main server in any deployment is called the secondary database. Likewise, the Config database in the first main server in any deployment is called the primary database (page 96).

secondary server

Once you access the Unified MCP Administration (page 37), and enable all feature services in that server, this server automatically becomes the secondary server.

session

A session is a recorded monologue, dialog, or conference which can involve one or more participants. A session in Unified MCP has the same meaning as a recording session in Unfied CM. See the **Cisco Unified Communications Manager Features and Services Guide** (http://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/prod_maintenance_guides_list.html) for more information on recording sessions. A session (page 97) is identified by a sessionID (or Session ID) and contains one or more tracks (page 97).

session ID

The unique identifier for a session (page 97).

SM Agent

SM Agent is a feature (page 95) service. This service monitors the overall storage in each server in the Unified MCP cluster and generates threshold events based on disk usage. This service is available in all servers in the cluster.

System Service

This network service controls service operations. It does not have a separate UI and operates seamlessly within the Unified MCPAdministration and the Unified MCP Serviceability Administration.

track

A track identifies each media stream (page 95) and quantifies it with additional data such as participants, duration, startDate, and a trackNumber.

Each track is specific to one audio stream or one video stream, and is idenfied by a trackNumber.

Each track can be associated with multiple Device References (page 95)

Each session contains one or more tracks.

Track ID

The unique identifier for a track.